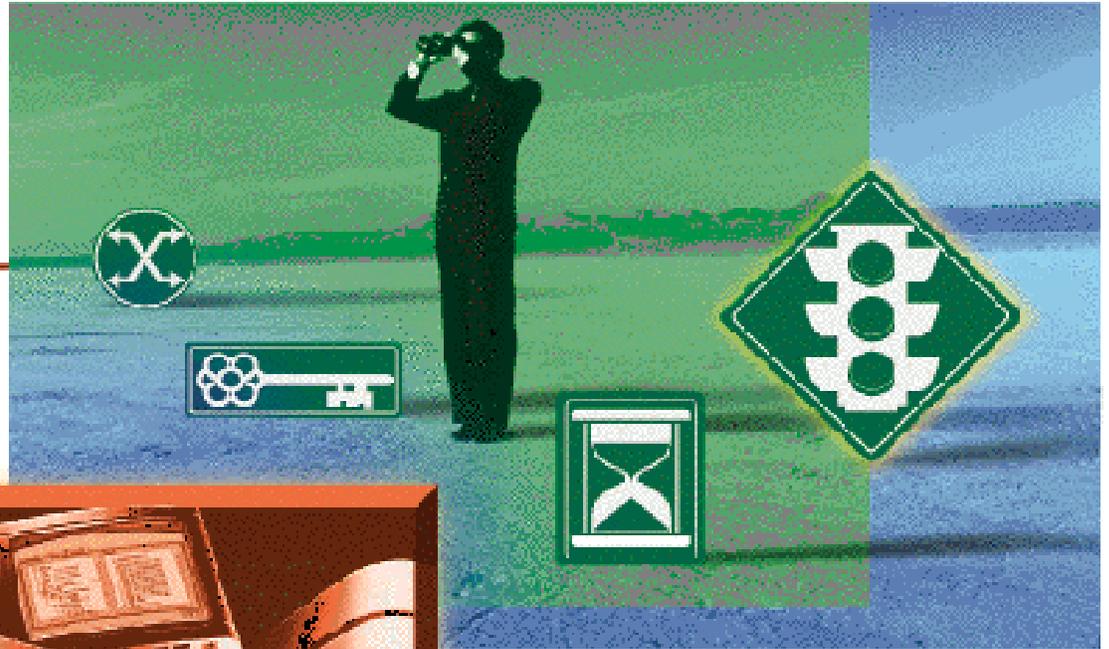
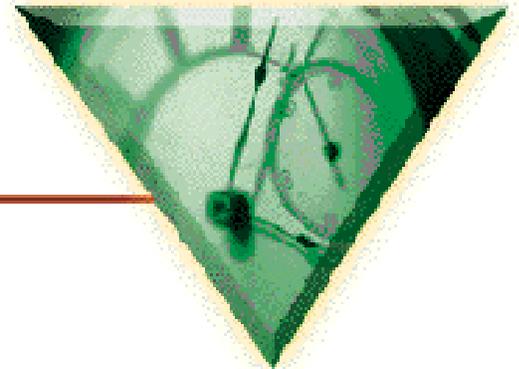


SPECTRUM



VLAN Manager



User's Guide

CABLETRON
SYSTEMS

Notice

Cabletron Systems reserves the right to make changes in specifications and other information contained in this document without prior notice. The reader should in all cases consult Cabletron Systems to determine whether any such changes have been made.

The hardware, firmware, or software described in this manual is subject to change without notice.

IN NO EVENT SHALL CABLETRON SYSTEMS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS MANUAL OR THE INFORMATION CONTAINED IN IT, EVEN IF CABLETRON SYSTEMS HAS BEEN ADVISED OF, KNOWN, OR SHOULD HAVE KNOWN, THE POSSIBILITY OF SUCH DAMAGES.

Virus Disclaimer

Cabletron has tested its software with current virus checking technologies. However, because no anti-virus system is 100% reliable, we strongly caution you to write protect and then verify that the Licensed Software, prior to installing it, is virus-free with an anti-virus system in which you have confidence.

Cabletron Systems makes no representations or warranties to the effect that the Licensed Software is virus-free.

Copyright © November 2000, by Cabletron Systems, Inc. All rights reserved.

Printed in the United States of America.

Order Number: 9032000-09

Cabletron Systems, Inc.
P.O. Box 5005
Rochester, NH 03866-5005

SPECTRUM, **SPECTRUM IMT/VNM** logo, **DCM**, **IMT** and **VNM** are registered trademarks, and **SpectroGRAPH**, **SpectroSERVER**, **Device Communications Manager**, **Inductive Modeling Technology**, **Device Communications Manager**, **SecureFast**, and **Virtual Network Machine** are trademarks of Cabletron Systems, Inc.

Acrobat is a trademark of Adobe Systems, Inc.

C++ is a trademark of American Telephone and Telegraph, Inc.

UNIX is a trademark of UNIX System Laboratories, Inc.

OSF/Motif and **Motif** are trademarks of the Open Software Foundation, Inc.

X Window System is a trademark of X Consortium, Inc.

Ethernet is a trademark of Xerox Corporation.

Restricted Rights Notice

(Applicable to licenses to the United States Government only.)

1. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Cabletron Systems, Inc., 35 Industrial Way, Rochester, New Hampshire 03867.

2. (a) This computer software is submitted with restricted rights. It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this Notice or as otherwise expressly stated in the contract.
 - (b) This computer software may be:
 - (1) Used or copied for use in or with the computer or computers for which it was acquired, including use at any Government installation to which such computer or computers may be transferred;
 - (2) Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;
 - (3) Reproduced for safekeeping (archives) or backup purposes;
 - (4) Modified, adapted, or combined with other computer software, provided that the modified, combined, or adapted portions of the derivative software incorporating restricted computer software are made subject to the same restricted rights;
 - (5) Disclosed to and reproduced for use by support service contractors in accordance with subparagraphs (b) (1) through (4) of this clause, provided the Government makes such disclosure or reproduction subject to these restricted rights; and
 - (6) Used or copied for use in or transferred to a replacement computer.
 - (c) Notwithstanding the foregoing, if this computer software is published copyrighted computer software, it is licensed to the Government, without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.
 - (d) Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the contract.
 - (e) This Notice shall be marked on any reproduction of this computer software, in whole or in part.



Contents

Preface

Year 2000 Compliance	xv
Who Should Read This Guide	xv
Using This Manual	xvi
SPECTRUM VLAN Manager Documentation	xvii
Viewing and Printing this Document	xviii
Questions about Documentation.....	xix

Chapter 1 Introducing SPECTRUM VLAN Manager

VLANs	1-1
What are VLANs?	1-1
What are the Advantages of VLANs?.....	1-2
Moves and Changes	1-2
Broadcast Traffic.....	1-3
Open/Secure VLANs	1-3
SPECTRUM VLAN Manager.....	1-4
SPECTRUM VLAN Manager Features	1-4
New and Improved for This Release.....	1-7
SPECTRUM VLAN Manager Components	1-7
SecureFast Switches.....	1-8
SPECTRUM VLAN Manager Software.....	1-9
VLAN Manager Client.....	1-9
VLANServer	1-10
Where Do I Go From Here?	1-10

Chapter 2 Managing the VLAN Manager Client and the VLANServer

Overview	2-1
Starting the SPECTRUM VLAN Manager Control Panel	2-1
Starting SPECTRUM VLAN Manager	2-2
Starting VLANServer from the Control Panel	2-3
Starting VLANServer Using the Autostart Feature	2-3
Starting the VLAN Manager Client from the Control Panel.....	2-4
Starting the VLAN Manager Client Using the Autostart Feature	2-6
Exiting SPECTRUM VLAN Manager	2-8
Ending a VLAN Manager Client Session	2-8

Shutting Down VLANServer From the VLAN Manager Control Panel	2-9
Exiting the SPECTRUM VLAN Manager Control Panel.....	2-9
The SPECTRUM VLAN Manager Control Panel.....	2-9
Pull-Down Menus.....	2-10
File Menu	2-10
Control Menu	2-11
Configure Menu	2-12
Fast Buttons	2-12
VLANServer Message Window	2-13
Status Field	2-14
Exit Button.....	2-14
Saving the VLANServer Database	2-15
Saving the Database (Models and Catalog).....	2-15
The Select File to Save Database... Dialog Box.....	2-16
Saving the Database (Models Only).....	2-17
Restoring the VLANServer Database.....	2-18
Restoring from a Saved Database (Current Release)	2-18
Restoring from a Saved Database (Previous Release)	2-20
Initializing to the Legacy Database	2-20
Configuring the VLANServer	2-21
Performance Tuning	2-21
Communications.....	2-22
VLANServer Configuration	2-22
Processd	2-23
Reinitializing processd	2-23

Chapter 3 Exploring VLAN Manager

VLAN Manager Windows.....	3-1
Main Window	3-1
Information Windows.....	3-3
Dialog Boxes	3-4
Views	3-5
VLAN Manager Menus	3-6
Pull-Down Menus.....	3-6
Pop-Up Menus.....	3-6
Menu Descriptions.....	3-6
File Menu	3-6
Edit Menu	3-8
View Menu	3-11
Tools Menu.....	3-13
Help Menu.....	3-14
Choosing Menu Items.....	3-14
VLAN Manager Tool Bar.....	3-15
Tool Descriptions.....	3-15
Working with Dialog Boxes	3-16
Entering Information Text Fields.....	3-17
Closing Windows.....	3-17
VLAN Manager Main Window Panes.....	3-17

Logical Window Pane	3-18
VLANs	3-19
AMR VLANs	3-19
IP Multicast Groups	3-19
Graphical Icons	3-20
Physical Window Pane	3-21
Graphical Icons	3-22
Scroll Bars	3-24
Working With Icons	3-24
Selecting Icons	3-25
Expanding and Collapsing Icons	3-26
Dragging and Dropping Icons	3-27
Status Bar	3-28
Operational Status	3-29

Chapter 4 Managing Security

Overview	4-1
Configuring Security	4-1
Adding a User	4-2
Adding a Host	4-3
Deleting a User or Host	4-3

Chapter 5 Managing Preferences

Overview	5-1
Global Preferences	5-1
Main Preferences	5-3
Topology View Preferences	5-4
Path Trace Preferences	5-5
Connection Table Preferences	5-6

Chapter 6 Managing Domains

Overview	6-1
VLAN Manager Domain Discovery Wizard	6-1
Discovering and Creating VLAN Domains	6-11
Discovery	6-12
Opening Domains	6-14
Creating Domains	6-16
Deleting Domains	6-17
Domain Properties	6-18
General Properties	6-19
AMR Properties	6-21
Services Properties	6-22
IP Address Learning Properties	6-24
User Persistence	6-26

Domain Details	6-30
Domain Details Window Column Descriptions	6-30
Launching the Source Blocker Table	6-32
Launching the Flood Suppression Table	6-32
Launching the Switch Properties Tabbed Folder.....	6-32
Launching the Violations Table.....	6-32
Rebooting All Switches in a Domain	6-33
Expanding a Domain Using Uplink Switching	6-34
Configuring Tier 1 Uplink Switching.....	6-35
Setting Up a Chassis to Run Uplink Switching.....	6-36
Setting Dynamic Uplink.....	6-37
Unsetting Dynamic Uplink.....	6-38
Protocol Control	6-38
Domain Wide Services	6-41
Using Search/Filter.....	6-43

Chapter 7 Managing Switches

Overview.....	7-1
Adding a Switch	7-2
Deleting a Switch.....	7-3
Switch Properties	7-4
General Switch Properties	7-4
Multicast View.....	7-7
VLAN Islands View	7-9
Displaying Switch Details	7-11
General Information Fields.....	7-12
Ports Fields	7-13
Using Search/Filter.....	7-15
Downloading Firmware to a Switch.....	7-15
Forcing a Switch to be Polled Immediately.....	7-16
Forcing a Switch to Reconfigure Immediately.....	7-16
Rebooting an Individual Switch	7-17
Replacing a Switch	7-18
Switch Protocol Control	7-19

Chapter 8 Managing Ports

Overview.....	8-1
Port Menus.....	8-2
Port Properties	8-3
Editing a Port Label.....	8-8
Configuring a Router Port	8-9
Flow of Events.....	8-9
Using the Router Wizard	8-10
Step 1	8-12
Step 2.....	8-13
Step 2a.....	8-14

Step 3.....	8-15
Step 4.....	8-16
Step 5.....	8-17
Step 6.....	8-18
Step 7.....	8-19
Step 8.....	8-20
Router Port Configuration Examples	8-21
Locking/Unlocking a Port	8-24
Setting/Unsetting a Router Port.....	8-24
Redundant Access	8-25
Dynamic Redundant Access Functional Overview.....	8-26
Provisioned Redundant Access Functional Overview	8-27
Configuring Dynamic Redundant Access Ports.....	8-28
Run Domain Discovery.....	8-28
Select Set/Unset Redundant Access Ports	8-28
Make Physical Connections	8-30
Unconfiguring Dynamic Redundant Access Ports.....	8-31
Configuring Provisioned Redundant Access Ports	8-32
Configuring Provisioned Redundant Access Ports	8-32
Run Domain Discovery.....	8-32
Select Set/Unset Provisioned Redundant Access Ports	8-32
Provision Redundant Access Port Neighbor Information.....	8-34
Make Physical Connections	8-36
Unconfiguring Provisioned Redundant Access Ports	8-37
Setting Redundant Port Properties	8-37
Configure Redundant Access Port Frequency and Priority Properties	8-38
Redirecting a Port	8-39
Launching Port Redirecting from the VLAN Manager	8-41
Adding a Port Mapping.....	8-41
Deleting a Port Mapping.....	8-42
Restricting a Port	8-42
Using Port Restrictions to Restrict a Port.....	8-43
Enabling OSPF Multicast	8-45
Enabling VRRP Multicast.....	8-47

Chapter 9 Managing SecureFast VLANs

Overview	9-1
Creating VLANs.....	9-2
Deleting VLANs.....	9-4
Removing a User from a VLAN	9-5
VLAN Properties.....	9-6
VLAN Port Properties	9-8
Displaying VLAN Details	9-9
General Information Fields	9-9
Users List.....	9-10
Editing User Properties	9-12
Using Search/Filter.....	9-12
Toggling VLAN Status/Policy.....	9-12

Assigning Membership in VLANs	9-13
VLAN Membership Rules.....	9-13
Assigning Membership to All Users Connected to a Switch	9-14
Static Membership.....	9-14
Inherited Membership	9-14
Assigning Membership to All Users Connected to a Port.....	9-15
Static Membership.....	9-15
Inherited Membership	9-16
Assigning Membership to Selected Users Connected to a Port	9-17
Assigning a Default VLAN to Multiple Switch Ports.....	9-18
AMR VLAN Administration	9-19
Specific Behaviors of AMR Types.....	9-21
IP-Subnet.....	9-21
NetBIOS	9-21
IPX RIP/SAP	9-22
IPX RIP/SAP Example	9-22
Exception to IPX RIP/SAP Rule.....	9-24
AppleTalk	9-24
DECNet	9-25
VINES	9-25
BPDU	9-25
Enabling AMR VLANs.....	9-26
Enabling AMR VLANs Using the Discovery Wizard	9-26
Enabling AMR VLANs Using Domain Properties	9-27
Displaying AMR VLANs.....	9-28

Chapter 10 Managing Users

Overview.....	10-1
Creating a User	10-1
Removing a User from a Switch.....	10-3
Removing Users from a VLAN	10-4
Deleting a User	10-5
User Properties.....	10-6
General	10-7
VLAN Membership.....	10-9
Restrictions	10-9
Adding a User Alias.....	10-10
User Alias Properties	10-12
General	10-13
Restrictions	10-13
Viewing Connection Information	10-14
Using the Directory.....	10-14
Directory Menus.....	10-15
Users List.....	10-16
Creating a User	10-16
Deleting a User	10-17
Editing User Properties	10-17
Removing Users from a Switch.....	10-17

Adding/Removing a User Alias	10-18
Directory Pop-up Menu.....	10-18
Using the Search/Filter Options	10-19
Finding Duplicate Network Addresses.....	10-19
Save	10-20
Space Delimited	10-20
Comma Delimited	10-21
Using Save	10-21
Import.....	10-23
Using Import	10-24
User Restrictions	10-25
Types of User Restrictions	10-26
Restricted Alias	10-26
Restricted Mobility	10-27
Not Restricted	10-27
Using User Restrictions to Restrict a User.....	10-28
Violations.....	10-32
Violation Notification.....	10-32
Identifying the Cause of a Violation	10-33
Violation Window Fields	10-33
Violation Window Buttons.....	10-33
Opening the Violations Window	10-34
Remediating a Violation.....	10-35
Remediating User and Port Restrictions	10-35
Example #1 (Restricted Port Violation).....	10-38
Example #2 (Restricted Mobility Violation)	10-39
Example #3 (Restricted User Violation).....	10-42
Invalid IP Violations	10-44
Example (Invalid IP - IP Not Learned).....	10-45
Disabled Protocol Violation.....	10-47
Example (Disabled Protocol Violation).....	10-47

Chapter 11 Managing Connections

Overview	11-1
Launching the Connection Table.....	11-1
Complete Connection Table Query	11-2
Partial Connection Table Query	11-3
Selecting a Source User, Destination User, or MAC Address	11-4
Elements of the Connection Table.....	11-5
Connection Table Menu Bar	11-5
File Menu	11-5
Edit Menu.....	11-6
View Menu	11-6
Connection Table Update Button.....	11-7
General Information Fields	11-7
Connection Table Fields.....	11-7
Sorting the Connection Table	11-9

Tapping a Connection	11-9
Adding a Call Tap.....	11-10
Releasing a Call Tap.....	11-11
Modifying a Call Tap.....	11-12
Tracing a Connection.....	11-12
Path Trace Menu Bar	11-13
Path Trace Display Area.....	11-14
Path Trace Status Bar.....	11-14
Releasing a Connection	11-14
Aging Connections	11-14
Configuring Call Aging.....	11-16
Aging Configuration Attributes	11-17
Aging Configuration Buttons.....	11-17
Editing Aging Configuration Attributes.....	11-18
Provisioning Calls.....	11-18
Tapped Connections.....	11-22

Chapter 12 Managing IP Multicast Groups

Overview.....	12-1
Displaying IP Multicast Groups	12-2
Editing Multicast Properties	12-3
Enabling and Disabling Multicast for an Entire Domain	12-4
Enabling or Disabling Multicast for a Router	12-4
Controlling Access to Multicast Groups	12-4
IP Multicast Group Properties.....	12-4
Switch Properties.....	12-5
Editing IP Multicast Port Properties.....	12-7
Deleting a Multicast Group	12-8

Chapter 13 Viewing Domain Topologies and Managing Switch Links

Viewing Domain Topologies	13-1
Topology View Menu Bar	13-2
Topology View File Menu.....	13-3
Topology View View Menu	13-3
Filter	13-4
Layout	13-5
Zoom	13-9
Topology Display Area.....	13-9
Switch Icons	13-9
Switch Icon Pop-up Menu.....	13-10
Managing Switch Links	13-11
Pipes	13-11
Link Status Pop-up Menu	13-12
Shared Links.....	13-12

Chapter 14 Managing VLANs Over ATM Networks

Overview	14-1
Managing VLANs Over ATM Networks Using Permanent Virtual Circuits	14-2
Creating PVC/VCC Connections	14-2
Creating an End-to-end PVC.....	14-4
Using the ATM Administrator Management SPMA to Create PVCs.....	14-5
Accessing the ATM Administrator Management SPMA	14-5
Current Connections	14-6
Editing Current Connections Entries	14-9
Using AMI to Create VCCs	14-11
Using Local Management to Create PVCs	14-12
Managing VLANs Over ATM Networks Using Switched Virtual Circuits	14-17
Initialization and Configuration	14-17
Backup ELANs	14-19
ATM-Attached Endpoints	14-20
Using SVCs to Manage VLANs Over ATM Networks	14-20
Sample SVC Network.....	14-21
Configure ELANs/LECs	14-22
Run Discovery.....	14-23
Network Scalability	14-25
Option 1.....	14-25
Option 2.....	14-26
Option 3.....	14-27
Option 4.....	14-28
Creating Additional ELANs.....	14-28
Discovery ELAN Configuration.....	14-31
Overview	14-31
Using the VLAN Manager to Edit the Discovery ELAN	14-32
Discovery ELAN Configuration Menus	14-33
File Menu	14-33
Edit Menu	14-33
Discovery ELAN Configuration Fields	14-33
Editing a Discovery ELAN Name	14-34
Changing the Operational Mode of an HSI.....	14-34
Changing the Operational Status of an HSI.....	14-35

Chapter 15 Advanced VLAN Policy

Overview	15-1
Launching Advanced VLAN Policy	15-2
Advanced VLAN Policy Dependencies	15-3
Using Advanced VLAN Policy.....	15-3
Advanced VLAN Policy Main Window Menus	15-4
File Menu	15-4
Edit Menu.....	15-6
View Menu	15-7
Help Menu.....	15-7

Advanced VLAN Policy Main Window Policy Table	15-7
Initial Settings	15-8
Selecting Parts of the Policy Table.....	15-9
Advanced VLAN Policy Main Window Buttons	15-10
Setting Advanced VLAN Policy	15-11
Sorting the Advanced VLAN Policy Main Window	15-13
Viewing Reverse Policy	15-14
Setting Flood Defaults.....	15-15
Advanced VLAN Policy Network Example.....	15-16
Setup.....	15-16
Requirement	15-18
Solution	15-18
Managing the Advanced VLAN Policy Table.....	15-20
Saving an Advanced VLAN Policy Table.....	15-21
Saving a Policy Table Using Save Policy Table.....	15-21
Saving a Policy Table Using Save Policy Table As	15-21
Restoring an Advanced VLAN Policy Table	15-22
Printing an Advanced VLAN Policy Table to a Text File.....	15-23

Chapter 16 Managing Your Database

VLAN Manager Database Backup	16-1
On-Line Backup	16-1
Backup File Maintenance.....	16-2
Configuring On-Line Backup.....	16-2

Appendix A Glossary

Acronyms.....	A-1
Terms	A-4

Appendix B SecureFast DHCP Relay Agent

Overview.....	B-1
DHCP Configuration	B-2
Defining Scopes.....	B-3
Mapping Scopes to VLANs.....	B-4
DHCP Operation.....	B-4
DHCP When More Than Eight Scopes are Serviced by a Single DHCP Server	B-6
Define Address Scopes.....	B-7
Map Scopes to VLANs.....	B-9
Configure Advanced VLAN Policy	B-9

Index

This book is a guide to using SPECTRUM VLAN Manager. It provides an overview of VLANs and VLAN Manager, discusses VLAN Manager's graphical user interface, provides startup instructions, and provides task related information pertaining to the administration of VLANs using VLAN Manager.

VLAN Manager can be installed as a stand-alone application or as an integrated SPECTRUM application. Refer to the *SecureFast VLAN Installation Guide* for information about how to install VLAN Manager as a stand-alone application or the *SPECTRUM -Integrated VLAN Manager Application Guide* for information about how to install VLAN Manager as an integrated SPECTRUM application. Management of your VLAN network using VLAN Manager is the same regardless of whether VLAN Manager is running as a stand-alone application or as an integrated SPECTRUM application.

Year 2000 Compliance

SPECTRUM VLAN Manager is designed to be "Year 2000 Compliant". This means that it is able to accurately process date data (e.g., sequencing, comparing, calculating) from, into, and between the twentieth and twenty-first centuries.

Who Should Read This Guide

This guide is intended for use by network administrators and technicians responsible for day-to-day administration of switched networks. It is also intended for use by network administrators and technicians who are considering implementing virtual LANs as the first step towards virtualizing their traditional networks.

This guide presumes you are familiar with the terms and principles associated with traditional network devices such as hubs, routers, and bridges as well as with the terms and principles associated with LAN Emulation (LANE), Asynchronous Transfer Protocol (ATM), and switching devices. It also presumes that you are familiar with traditional networking models and standards, (i.e., the Open Systems Interconnection (OSI) model, and the 802.1d, 802.3, and 802.5 standards). Familiarization with network management systems such as SPECTRUM also would be helpful.

This manual is written from a Motif windowing environment perspective. If you are using another interface (i.e. OpenLook), screens and mouse functionality will vary according to the interface being used.



If you have Motif and Open Windows installed on your system, you can switch between windowing systems using the `OIT_LOOK <environment variable>`. Windowing environment variables are: `MOTIF` or `OPENWIN`. The command used for the `cs`h is `setenv OIT_LOOK <environment variable>`. The command for the `ksh` is `export OIT_LOOK=<environment variable>`.

Using This Manual

This manual is divided into the following chapters and appendices:

- **Chapter 1, Introducing SPECTRUM VLAN Manager** - This chapter provides an overview of VLANs and SPECTRUM VLAN Manager.
- **Chapter 2, Managing the VLAN Manager Client and the VLANServer** - This chapter provides step-by-step instructions for starting VLAN Manager and detailed information about the SPECTRUM VLAN Manager Control Panel.
- **Chapter 3, Exploring VLAN Manager** - This chapter introduces VLAN Manager's graphical user interface. It provides detailed information about VLAN Manager's Main and ancillary windows, the tasks that can be launched from these windows, and the user-friendly features of the user interface that make it so easy for you to manage your network.
- **Chapter 4, Customizing VLAN Manager** - This chapter provides step-by-step instructions for setting preferences using VLAN Manager's graphical user interface.
- **Chapter 5, Configuring VLAN Manager Security** - This chapter provides step-by-step instructions for security administration tasks, using VLAN Manager's graphical user interface.
- **Chapter 6, Managing Domains** - This chapter provides step-by-step instructions for performing domain administration tasks, using the VLAN Manager's graphical user interface.
- **Chapter 7, Managing Switches** - This chapter provides step-by-step instructions for performing switch and port administration tasks, using the VLAN Manager's graphical user interface.
- **Chapter 8, Managing Ports** - This chapter provides step-by-step instructions for performing switch and port administration tasks, using the VLAN Manager's graphical user interface.
- **Chapter 9, Managing VLANs** - This chapter provides step-by-step instructions for performing VLAN and AMR VLAN administration tasks, using the VLAN Manager's graphical user interface.

- **Chapter 10, Managing Users** - This chapter provides step-by-step instructions for performing user administration tasks, using the VLAN Manager's graphical user interface.
- **Chapter 11, Managing Connections** - This chapter provides step-by-step instructions for performing connection administration tasks, using the VLAN Manager's graphical user interface.
- **Chapter 12, Managing IP Multicast Groups**- This chapter contains information about creating and administering IP Multicast groups.
- **Chapter 13, Viewing Domain Topologies and Managing Switch Links** - This chapter provides step-by-step instructions for performing link administration tasks, using the VLAN Manager's graphical user interface.
- **Chapter 14, Managing VLANs Over ATM Networks** - This chapter provides an overview of managing VLANs over ATM networks, presents information about current VLAN over ATM models, and describes how to create and manage VLANs over ATM using SPECTRUM VLAN Manager.
- **Chapter 15, Advanced VLAN Policy** - This chapter provides information about how to fine tune VLAN policy using the Advanced VLAN Policy application.
- **Chapter 16, Managing Your Database** - This chapter provides information about using on-line backup to automatically backup your VLANServer database.
- **Appendix A, Glossary** - This appendix contains a list of VLAN-related acronyms and terms.
- **Appendix B, SecureFast DHCP relay Agent** - This appendix contains configuration and operational information about the DHCP (Dynamic Host Configuration Protocol) Relay Agent.

SPECTRUM VLAN Manager Documentation

The following documentation is shipped on the SPECTRUM VLAN Manager CD-ROM:

- ***SPECTRUM VLAN Release Notes*** (*relnotes.pdf*) - a guide to the features of the SPECTRUM VLAN Manager product; lists hardware, software, and firmware requirements for the current version; explains the documentation and support available for the SPECTRUM VLAN Manager product, and identifies known anomalies in this release.
- ***SPECTRUM VLAN Manager Installation Guide*** (*installg.pdf*) - a guide to installing either version of SPECTRUM VLAN Manager (standalone or Spectrum-integrated) on your Windows NT or Solaris platform. It also provides procedures for downloading the SecureFast VLAN firmware to your switches. Users of both versions of the VLAN Manager will find this guide helpful.

- ***SPECTRUM VLAN Manager User's Guide*** (`userg.pdf`) - an administrator's guide to the windows, menus, and functions of the SPECTRUM VLAN Manager user interface, including the type and format of all possible entries. Users of both versions of the VLAN Manager will find this guide helpful.
- ***SPECTRUM -Integrated VLAN Manager Application Guide*** (`specintg.pdf`) - a guide to using the SPECTRUM portion of the SPECTRUM-integrated version of VLAN Manager. Users of the SPECTRUM-integrated version of VLAN Manager will find this guide helpful.
- ***SPECTRUM VLAN Manager Command Line Interface Guide*** (`command.pdf`) - The VLAN Command Line Interface (CLI) is a collection of independent Java™ applications that provide access to VLAN Server functions from the command line.
- ***SPECTRUM VLAN Diagnostic Tools Guide*** (`diag.pdf`) - Describes seven shell script executables used for troubleshooting and extracting key information out of a network in VLAN mode. These executables include `das`, `dirgrep`, `dirstat`, `getTable`, `mibPoller`, `showvst`, and `tracecnx`. There is also a new java-based application called the VLAN Diagnostic Toolbox that launches these executables from an easy to use GUI, described in this document.
- ***SecureFast Tools Guide*** (`tools.pdf`) - a guide that covers a set of diagnostic and monitoring tools that are available from the **Tools>SecureFast Tools** menu in VLAN Manager.

The VLAN Capacity Monitor provides Source Blocker and Flood Suppression table information and six bar graphs that provide performance data about the SecureFast Switches in your network.

Element Management Tools are a set of applications that let you retrieve and, in some cases, modify table information (MIB objects) in the switches in your SecureFast network.

The SecureFast Trap Manager lets you set the traps on the SecureFast VLAN switches in your VLAN Manager domain(s)

- ***Local Management Network Tools Guide*** (`lmn.pdf`) - Describes the commands that are available in the Local Management of a switch that is in SecureFast VLAN mode.

Viewing and Printing this Document

To view and print the SPECTRUM VLAN Manager User's Guide, you need Adobe™ Acrobat™ Reader 3.0. For your convenience, a copy of Adobe Acrobat Reader 3.0 is included on the SPECTRUM VLAN Manager CD. The startup file for Adobe Acrobat Reader 3.0, `acread`, is located in the `Acrobat/bin` subdirectory of your installation area.

With Adobe Acrobat Reader 3.0 on your system, you can access this User's Guide:

- From the docs directory on the CD-ROM by starting up Adobe Acrobat Reader 3.0 and selecting **File >Open** from the menu. (If you are a SPECTRUM user, Adobe Acrobat Reader 3.0 is installed during the SPECTRUM installation process.)
- From the VLAN Manager Help menu, since this guide is installed as an integral part of VLAN Manager.

The documents are also available in PDF format on Cabletron's Virtual Networking web site at <http://www.ctrn.com>.

You will find information specific to Cabletron switches used in VLAN configurations in the hardware guides for the switches.

Questions about Documentation



Send your questions, comments or suggestions regarding documentation to the Technical Communications Department directly via the following internet address:

`spectrum-techdocs@ctrn.com`

Introducing SPECTRUM VLAN Manager

This chapter provides an overview of VLANs and SPECTRUM VLAN Manager for SecureFast networks.

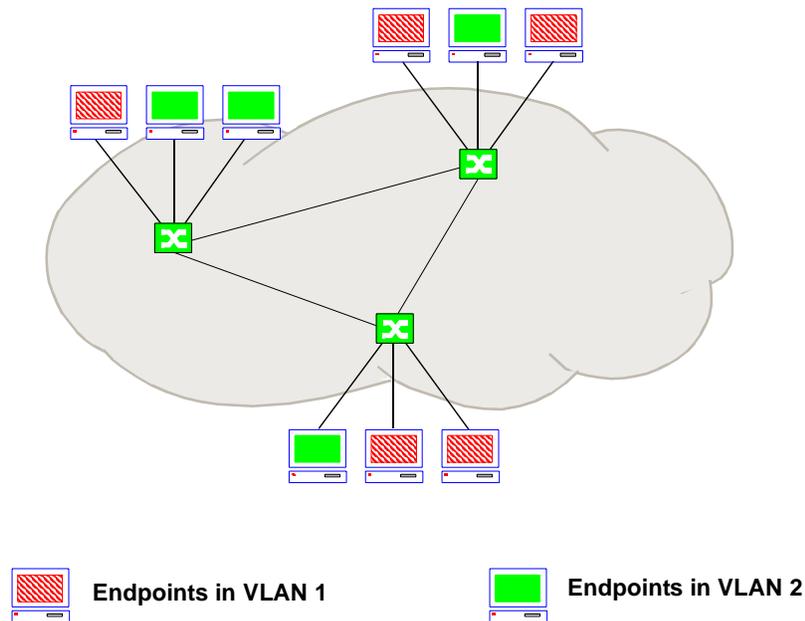
VLANs

VLANs are rapidly becoming an integral part of virtual switched networks. They offer solutions to concerns network managers have about managing a network. This section provides a brief overview of VLANs and their advantages.

What are VLANs?

A VLAN is a logical grouping of switch ports or endpoints which define a layer 2 broadcast domain. A VLAN is independent of any particular physical or geographical location. In other words, endpoints that share a virtual LAN appear to be on a single LAN segment, regardless of their actual location.

VLANs extend direct communication between users beyond the constraints of a physical LAN segment by allowing users on multiple physical LAN segments to be administratively grouped. In [Figure 1-1](#), for example, VLAN 1 is composed of endpoints on different LAN segments. In a traditional routed network, *direct* communication between these endpoints would not be possible, because the users are not all physically located on the same LAN segment. In a VLAN environment, the physical boundaries imposed by traditional solutions are removed and direct communication is possible.

Figure 1-1. VLAN-based Network

What are the Advantages of VLANs?

As a network administrator, you are concerned about potential network problems such as adds, moves and changes, broadcast traffic, and security. VLANs, and in particular Cabletron's implementation of VLANs, offer solutions to all these concerns.

Moves and Changes

VLANs greatly increase your ability to manage your network dynamically, without frequent trips to the wiring closet or manual workstation reconfigurations. In an IP network, for example, when a user moves from one subnet to another, a trip to the closet is usually required, and the user's IP address must be manually updated. VLANs eliminate both requirements because VLAN membership is not dependent on a user's physical location in the network. Users retain their original IP addresses and subnet membership.

Members of a functional group, no matter how disparate, can appear as though they are on the same LAN segment, with most network broadcast traffic staying within that group's VLAN. These functional groups can be thought of as virtual workgroups. Since physical location is not a concern in the VLAN environment, a group member who moves to

another physical location causes no particular problem to the network and no changes have to be made to the user's workstation. If that same member is transferred to another group, you can assign the user membership in the new group (or both groups) by simply "dragging" the user's icon from one VLAN and dropping it into another.

Broadcast Traffic

In Cabletron's implementation of VLANs, the amount of broadcast traffic is significantly reduced.

SecureFast VLAN switches do this by resolving broadcast packets to unicast. This is accomplished by each switch being able to resolve broadcast packets at the switch access ports, rather than just tagging and flooding the broadcast packets.

To resolve, the switch does a look-up in its local directory and/or the virtual directory (via interswitch resolve requests) for the MAC address bound to the network address (alias address). Thus, rather than flooding an ARP broadcast, the access switch resolves it to the true MAC destination and then establishes a connection from the ingress and egress switch for the source MAC address to the destination MAC address.

If the destination cannot be resolved to the true MAC address, packets are forwarded out ports associated with the source VLAN.

VLANs behave in much the same manner as routers do, by restricting broadcast traffic to only those users within the same VLAN. This also greatly reduces broadcast traffic by limiting broadcasts only to switch ports connected to endpoints belonging to a particular VLAN.

Open/Secure VLANs

Secure VLANs provide network security by only allowing members of the same VLAN to communicate. Security is also maintained by not allowing users to join other VLANs without the approval of the network administrator.

Cabletron's VLAN implementation is much more flexible than many other VLAN implementations, where inter-VLAN communication requires the services of a router. Two modes of operation are possible: open and secure. In open mode, direct communication between VLANs is allowed. In secure mode, communication is only allowed between members of the same VLAN. This flexibility allows you to secure or open communications between VLANs as required in order to maintain network security, while providing increased network performance.



For even more flexibility, VLAN Manager offers Advanced VLAN Policy which allows you to fine-tune existing VLAN connectivity and flooding policy on a per VLAN pair basis.

If the VLAN membership of either the source or destination user is configured in secure mode, inter-VLAN communication will not be possible without the services of a router. Routers configured for the purpose of inter-VLAN communication must be a member of all VLANs for which inter-VLAN communication is desired.

SPECTRUM VLAN Manager

SPECTRUM VLAN Manager provides critical management services for all the switches in your VLAN switched network. You can even manage your VLANs across ATM networks. SPECTRUM VLAN Manager's advanced graphical user interface makes VLAN administration easy. Domains, VLANs, switches, and users can be created and managed using VLAN Manager's menus, toolbar, and drag-and-drop capability. Using VLAN Manager, you can precisely control access to your VLAN network by applying rules to VLANs and switch ports. You can also monitor the VLANs, switches, ports, users, connections, and topologies in your network, using the detailed views provided.

SPECTRUM VLAN Manager is compatible with all SecureFast Packet switches for Cabletron products.

SPECTRUM VLAN Manager Features

In addition to an advanced user interface, the SPECTRUM VLAN Manager product model has many inherent features including:

- **Plug and play ease of use** - Communication between endpoints is possible even before VLAN Manager is installed. Before any VLAN membership administration, each VLAN switch domain emulates a single bridged LAN, where all directly attached endpoints in effect are members of a common VLAN.
- **Automation of user adds, moves, and changes** - Software support for dynamic user adds, moves, and changes.
- **Capability of sustaining high throughput** - Once a call is set up, processing proceeds at near wire speed.
- **Control of broadcast traffic** - Tag-based flooding of non-resolvable broadcasts.
- **Switching or Routing Between VLANs** - Layer 3 switching for open host communication or layer 3 routing to support host access control.
- **Automatic call re-routing** - A specialized VLSP (Virtual Link State Protocol) provides active redundant paths. Call re-routing is done on the fly.
- **Multiple active network links with load balancing** - The aggregate connections for each SecureFast switch is balanced over multiple high-speed links.

- **Operation independent of network protocols** - All popular protocols supported with special services for IP, IPX, DHCP, etc.
- **Operation independent of LAN technologies and topologies** - All popular LAN technologies such as Ethernet and FDDI are supported.
- **Full compatibility with existing network adapters, hubs, routers and switches** - Protects your current hardware investment.
- **Flexible VLAN membership criteria** - Endpoint membership by Switch, Port, MAC address, Protocol, Network Address.
- **Call Tap Capability** - Unidirectional or bi-directional connections monitored to the output of an analyzer or via the physical address of an analyzer. Calls may be tapped to any port within the switch fabric by selecting either the network analyzer probe's MAC address through the VLAN Manager Application or any switch port within the switch fabric.
- **Editable Topology View** - Network connections are dynamic. The number of users connected to the switch is displayed on the switch icon. You can filter on a specific VLAN. Icons can be moved around to create a customized view.
- **Multi-domain control** - One VLAN Server can manage multiple VLAN domains.
- **Complete user mobility** - A user who is statically assigned to a VLAN will retain the mapping during the process of a move from one port to another or from one switch to another.
- **Connection Table** - Displays active end node conversations for selected users.
- **Directory Services** - Dynamic directory which provides physical location of every endpoint, layer 3 address, host name, and VLAN mapping.
- **Best Path Determination** - Optimal links are chosen to establish a connection flow based on link cost.
- **Quick Topology Convergence** - Electrical loss detection for Ethernet and fast Ethernet network links. SMT loss detection for FDDI network links.
- **VLAN Policy (Open/Secure)** - In Open mode, direct inter-VLAN communication is possible via Call Processing and address/VLAN Resolution. A router is not required. In Secure mode, inter-VLAN communication is only possible by using a router or by using Advanced VLAN Policy.
- **Advanced VLAN Policy** - Inter-VLAN policies can be set on a per VLAN pair basis rather than globally.
- **Multiple VLAN membership per user** - Users can have membership in more than one VLAN.
- **VLAN membership inheritance per port for users without any previous VLAN association** - Users are assigned to the default VLAN of the port they connect to.
- **VLAN locking per port** - Users of a locked port become members of the default VLAN for the port regardless of any static mappings.

- **Setting/Unsetting Router Port** - Disable learning of alias addresses per port.
- **Control Panel** - Provides client and server start-up, database maintenance, and host configuration.
- **VLANs over ATM** - Allows operation of SecureFast VLAN switched networks over ATM.
- **Automatic Member Registration** - Automatic Membership Registration (AMR) dynamically creates VLANs, joins endpoints to those VLANs, and floods packets to those VLANs.
- **IP Multicast** - IP Multicast groups let you set up unidirectional point-to-multipoint connections.
- **Uplink Switching** - Uplink switching uses edge (uplink) switches to connect to the core mesh fabric of switches. Uplink switches allow you to achieve a factor of scaling not possible with a single-area link state protocol. A single-area link state protocol permits a maximum of 128 switches in the core fabric. By adding uplink switches to you network, a significant increase in the number of switches and users in the SecureFast network can be achieved by implementing the uplink model. As the core fabric increases, so does the capacity to add uplink switches and the entire network scales with it.
- **Port Mirroring** - Provides the ability to redirect all data to a port for packet analysis or network troubleshooting.
- **Protocol Control** - Allows the network administrator to suppress certain protocols or protocol frame types on a switch or domain basis.
- **Restriction User/Port** - Allows users to be restricted to certain ports and ports to be restricted to certain users.
- **DHCP Relay Agent** - Supports multiple DHCP (Dynamic Host Control Protocol) scopes serviced by a single DHCP server within a domain.
- **Domain Wide Services** - Allows you to set and view Domain Wide Services; this replaces the Services Element Management Tool.
- **AppleTalk AMR Islands** - Provides network administrators with the ability to modify the AMR VLAN that AppleTalk users join when AppleTalk AMR is enabled.
- **DHCP Server Islands** - Allows you to specify the DHCP Server which services DHCP requests for clients on a per switch basis.
- **DHCP Server Single Flood** - Directs replies from the DHCP Server back to the client.
- **Virtual Router Redundancy Protocol** - Supports SSRs connected to a SecureFast switch. A Multicast group will automatically be configured when you enable this feature via the Router Wizard.

New and Improved for This Release

Among the new and improved features for this release are:

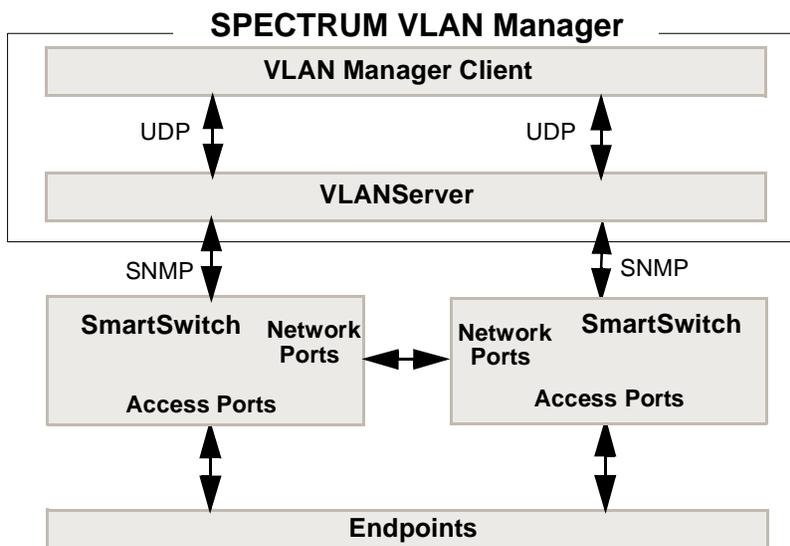
- **Wildcard VLANs** - If your firmware supports it, you can create a “wildcard” VLAN which, when dragged to a port, enables broadcasts for all VLANs to be forwarded out that port.
- **Enhanced Trap Services** - You can enable or disable the trap service via a button in the Trap Manager. In addition, more traps have been added.
- **Self ARP Packet Learning** - The ability to enable and disable this feature is available in the Port Properties and Switch Details views.
- **Persisted Alias** - The ability to persist user aliases is available in the Domain Properties and User Properties views.
- **Enable/Disable OSPF Multicast Group** - You can configure the OSPF multicast group using the Router Wizard.
- **Enhanced Uplink features** - Set/Unset Uplink per chassis is available for Tier 1 switches via the VLAN Manager **Edit >Switch** menu. An Uplink Status indicator is now available in the Switch Details and Domain Details views. You can now filter for Tier 1 and Tier 2 switches in the **Topology View**.
- **Enhanced Performance for Windows NT VLANServer clients** - The stacksize for VLANServer on NT has been enlarged for better performance.
- **Enhanced Directory View entry deletion** - You can now delete multiple entries from the Directory View.
- **Enhanced Redundant Port Properties** - Redundant Access neighbors are now shown. Limits of the Redundant Access parameters are now enforced for Send/Receive/Hello Frequencies and Priority.
- **Blockable Status indicator for users** - This can now be viewed in the User Properties view.
- **SFS Version Number** - This is now available in the Switch Details and Domain Details views.
- **General and Advanced Port Properties** - The information on the Port Properties General tab has been separated into a General tab and an Advanced tab.

SPECTRUM VLAN Manager Components

SPECTRUM VLAN Manager consists of the VLAN Manager software and Cabletron’s SmartSwitch switches (with VLAN firmware installed) working in conjunction with network endpoints ([Figure 1-2](#)).

- VLAN Manager software monitors and controls the configuration and maintenance of VLAN networks. It consists of the VLANServer and the VLAN Manager Client.
- SmartSwitch switches provide broadcast interception, address resolution, and call processing.
- Endpoints are devices connected to access ports in a VLAN switch domain.

Figure 1-2. SPECTRUM VLAN Manager Components



SecureFast Switches

SecureFast VLAN switches are connection-oriented internetworking devices. These devices use source address/destination address (SA/DA) pairs along with embedded Layer 3 virtual routing services to provide address interception, resolution, and call processing. In a connection-oriented network, path determination is accomplished at call setup time. Once a call is programmed, no additional software intervention is required. This type of call management operates much like a telephone network. The circuit is set up, data is transferred.

Switches forward packets at the MAC-layer and allow connectivity of endpoints via Access Ports based on VLAN mappings. The first packet is routed and the remaining packets are then switched along the same path. Each VLAN switch maintains a Local Directory of endpoint MAC and network addresses found on each switch port. The aggregation of each VLAN switch's Local Directory form a complete view of an entire VLAN domain. This information is used by the VLAN Manager for assignment and verification of VLANs.

SPECTRUM VLAN Manager Software

SPECTRUM VLAN Manager software is based on a client/server model. The client program (VLAN Manager) is VLAN Manager's graphical user interface. The server program (VLANServer) functions as VLAN Manager's knowledge base. The VLANServer and VLAN Manager graphical user interface are launched from the SecureFast VLAN Control Panel or from the VLANSERVER icon in SPECTRUM.

By taking advantage of this client/server relationship, multiple user interfaces can be attached to a single VLANServer. You can run the user interface locally on the same machine that is running the VLANServer and/or run it remotely across a network.

VLAN Manager Client

VLAN Manager is your gateway to the administration of VLANs. With the VLAN Manager client, you can initiate all VLAN network management tasks. For example, you can:

- Create, remove, open, configure, and discover domains, and view domain details.
- Create and delete VLANs, view VLAN details, enable or disable VLANs, and apply VLAN policy.
- Apply Advanced VLAN Policy.
- Add and remove user aliases.
- Add and delete switches, and view switch details.
- Create new users and view the directory of all users.
- Change the status of and lock or unlock access ports.
- Perform administrative and download tasks.
- View the topology of a VLAN domain.
- View active calls per user.
- Establish a Call Tap to analyze calls.
- Release calls.
- Provision calls.
- Create Permanent Virtual Circuits (PVCs).
- Configure router parameters.
- Create and manage AMR VLANs.
- Create and manage IP Multicast groups.
- Configure uplink switching on a per chassis basis.
- Restrict users to certain ports or ports to certain users.
- Redirect data from one port to another port for packet analysis.
- Configure redundant access ports.
- Set and view Domain Wide Services.

VLAN Manager uses SNMP protocol commands to configure and control all VLAN switches within a VLAN domain. A VLAN domain consists of a group of VLAN switches bounded by a routing device. All endpoint information is discovered by the VLAN switches and used during call setup. The VLAN Manager collects this information periodically, using SNMP.

VLANServer

The VLANServer provides VLAN Manager's intelligence. It contains models of the actual network devices and their interactions. These models are continuously collecting data about the objects they represent. As a result of this polling process, the VLANServer database gains extensive knowledge about any network that it manages. By analyzing this information, you can maximize your system's performance while minimizing cost.

Where Do I Go From Here?

If you are familiar with VLAN Manager's graphical user interface, proceed to those chapters in this guide that provide task oriented instructions for launching and managing your VLAN network, such as [Chapter 2, *Managing the VLAN Manager Client and the VLANServer*](#). Refer to [Page xvi](#) of the Preface for chapter descriptions.

If you are not familiar with VLAN Manager's graphical user interface, proceed to [Chapter 3, *Exploring VLAN Manager*](#). It walks you through the interface and provides information about how to use the interface's features.

Managing the VLAN Manager Client and the VLANServer

This chapter provides step-by-step instructions about how to start and stop the VLAN Manager client and VLANServer programs . Additionally, it provides detailed information about the SPECTRUM VLAN Manager Control Panel, which is used to perform all VLANServer administrative tasks.

Overview



This section describes how to start and stop VLAN Manager when VLAN Manager is installed as a stand-alone application. For information about how to start and stop VLAN Manager from SPECTRUM, refer to the *SPECTRUM -Integrated VLAN Manager Application Guide*.

Before you can start SPECTRUM VLAN Manager, you must log onto your workstation and start your window manager. Verify that VLAN Manager is installed (refer to the *SPECTRUM VLAN Installation Guide*). You can start VLAN Manager from the SPECTRUM VLAN Manager Control Panel or from the command line, using the Autostart feature.

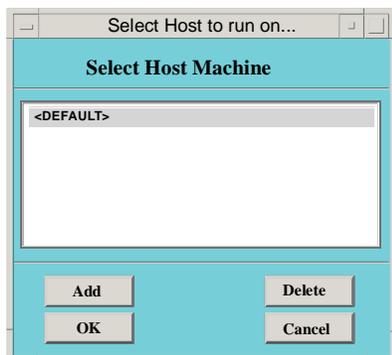
Starting the SPECTRUM VLAN Manager Control Panel

1. (UNIX) At the system prompt, enter the following: **vlanmgr**. The command can be typed from any directory.

(NT) Click the **Start** button and then navigate out to and click on **VLANPanel** by way of the **Programs** and then **VLAN Manager** pop-ups.

2. The **Select Host to run on** dialog box is displayed (Figure 2-1). Select a workstation running the VLANServer from the list, and then click **OK**. DEFAULT refers to your local workstation.

Figure 2-1. Select Host



1. If the workstation from which you want to start the VLAN Server is not listed, click **Add** to display the Enter VLANServer... dialog box, and then type in the name of the workstation or the network address and click **OK** to add that workstation to the list.
2. Click **Delete** to remove the highlighted workstation name from the list or **Cancel** to abort the operation.
3. If you inadvertently delete the DEFAULT entry from Select Host Machine dialog box, you can re-enter it by using the Add button.

Starting SPECTRUM VLAN Manager

In order to use SPECTRUM VLAN Manager, both the VLANServer and the VLAN Manager client must be running. Both can be run on the same workstation, or you can start the VLAN Manager client on your local workstation and connect to VLANServer running on another workstation. Either way, VLANServer must be running and ready to accept connections before you start the VLAN Manager client.



There is no backward compatibility between the VLAN Manager client and the VLANServer. Both components must be at the same version level.

Starting VLANServer from the Control Panel



You can use the appropriate command for your workstation (normally `ps -el` on Solaris and `ps` in the VLAN shell on NT workstations) to verify that no other programs that require database access are running.

To start VLANServer:

1. Click the  button.
2. During VLANServer's startup process, the Control Panel displays several messages, including:

```
Please wait... VLANServer loading landscape...  
Number of model types initialized: 686...  
Name Service Agent is running.
```

If you attempt to start the VLAN Manager client while the VLANServer is coming up, an error message appears, telling you that there is "No VLANServer to talk to."

3. The VLANServer is ready when the VLANServer Message Window displays:

```
VLANServer is now ready..
```

and the Status field shows RUNNING.

Starting VLANServer Using the Autostart Feature

On UNIX machines, you can save time by using the VLANServer autostart feature.

To invoke VLANServer autostart:

1. Type **vs** at the system prompt.
2. The program displays a dialog box listing the workstations on which you can start the VLANServer (Figure 2-2). Select a workstation, and then click **OK**. DEFAULT refers to your local workstation.

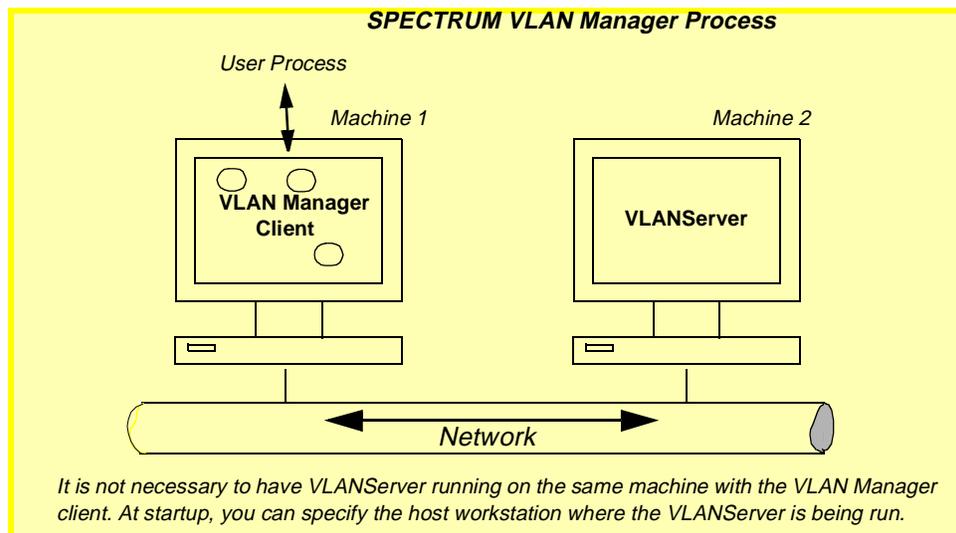
Figure 2-2. Select Host



Starting the VLAN Manager Client from the Control Panel

The VLAN Manager allows the Network Administrator to view or interact with the information contained in the VLANServer database. See Figure 2-3. If you are using one machine for VLANServer (host machine) and another for the VLAN Manager client (client machine), be sure that the VLANServer machine name is listed in the VLANServer Host Table in the SPECTRUM VLAN Manager Control Panel. You can open multiple clients, which can be useful if you want to open views from multiple domains.

Figure 2-3. User Interface Process



The first time you start SPECTRUM VLAN Manager, the user specified during the install process is the only user model in the VLANServer database. This means you must log in and start the VLAN Manager client the first time as the user who was specified during the install. Once you have started the client program, you should create a user model for your User ID. If you want to limit access to your User ID, you should destroy the user model

for install user. The network administrator must have the least restricted access. Then you can use your own User ID to start the VLAN Manager client program.

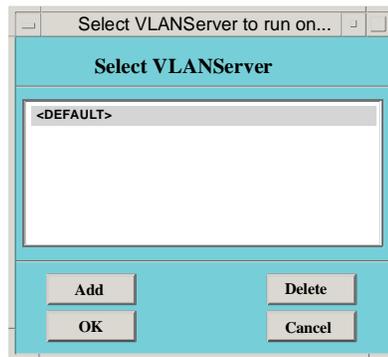
To start the VLAN Manager client from the Control Panel:

1. Click the  button.
2. The Select VLANServer dialog box ([Figure 2-4](#)) is displayed. Select the VLANServer workstation to which you want to connect the VLAN Manager client from the list, and then click **OK**. DEFAULT refers to the VLANServer on your local workstation.



1. If the VLANServer to which you want to connect the VLAN Manager client is not listed, click **Add** to display the Select VLANServer dialog box, and then type in the name of the workstation running VLANServer and click **OK** to add that workstation to the list of available VLANServers.
2. Click **Delete** to remove the highlighted VLANServer from the list or **Cancel** to abort the operation.

Figure 2-4. Select VLANServer



If you specify an incorrect name for the VLANServer to which you want to connect, or if the VLANServer you have chosen to connect to is not running, an error box appears, displaying the following message:

ERROR: VLANServer not running.

If you see this prompt, click **Close** in the error box and re-enter the command, using the correct VLANServer name.

Once the VLAN Manager client loads, and the VLAN Manager has successfully connected to the selected VLANServer, the following message is displayed in the status bar at the bottom of the VLAN Manager's Main window.

Connection to VLANServer Established

3. At this point, the Discovery Wizard is launched and Step 1 (Figure 2-5) is displayed providing that domains have not been previously discovered. Using the wizard, you can add or remove domains from a list of domains to be configured or discovered. You cannot remove previously discovered domains, but you can rediscover or configure a domain. A series of steps walks you through the discovery process, each step solicits information required by the wizard.

At this point, you can choose to enter the name of a new domain and continue the wizard process, or you can terminate the process and display the SPECTRUM VLAN Manager Main window.

Figure 2-5. VLAN Manager Wizard



In most cases, you will probably want to create and/or discover at least one domain using the wizard, however, if you decide to perform another task first, such as setting up security, you can terminate the wizard by clicking **Cancel**.

You can always restart the wizard by selecting **Wizard** from the **File>Domain** menu. Refer to [Chapter 3](#), for detailed information about using the VLAN Manager Discovery wizard.

Starting the VLAN Manager Client Using the Autostart Feature

You can save time by starting the VLAN Manager client on UNIX machines using the autostart feature.

To invoke autostart:

1. At the system prompt, type:

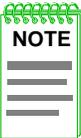
```
vm
```

2. The Select VLANServer dialog box (Figure 2-6) is displayed listing the VLANServers to which you can connect the VLAN Manager client. Select a VLANServer and then click **OK**. DEFAULT refers to your local VLANServer.



1. If the VLANServer to which you want to connect the VLAN Manager client is not listed, click **Add** to display the Select VLANServer dialog box, and then type in the name of the workstation running VLANServer and click **OK** to add that workstation to the list of available VLANServers.
2. Click **Delete** to remove the highlighted VLANServer from the list, or click **Cancel** to abort the operation.

Figure 2-6. Select VLANServer



If you specify an incorrect name for the VLANServer to which you want to connect, or if the VLANServer you have chosen to connect to is not running, an error box appears, displaying the following message:

ERROR: VLANServer not running.

If you see this prompt, click **Close** in the error box and re-enter the command, using the correct VLANServer name.

3. Once the VLAN Manager client loads, and the VLAN Manager has successfully connected to the selected VLANServer, the following message is displayed in the status bar at the bottom of the VLAN Manager's Main window.

Connection to VLANServer Established

At this point, the Discovery Wizard is launched and Step 1 is displayed providing that domains have not been previously discovered.

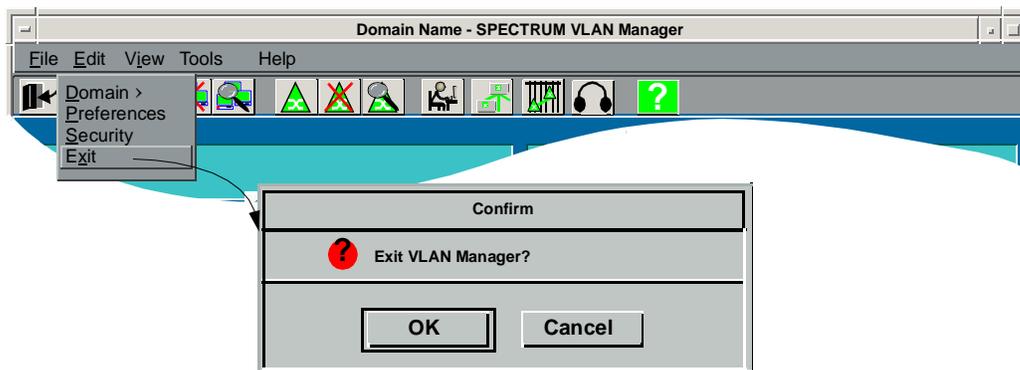
Exiting SPECTRUM VLAN Manager

Both exit processes, exiting SPECTRUM VLAN Manager client or shutting down the VLANServer, can be done independently. If you are shutting down the VLANServer, use the SPECTRUM VLAN Manager Control Panel. It is not necessary to bring the VLANServer down unless you have maintenance to perform.

Ending a VLAN Manager Client Session

1. Select **Exit** from the SPECTRUM VLAN Manager **File** menu to display the Confirm dialog box (Figure 2-7).

Figure 2-7. Confirm Dialog Box



2. Click **OK** to exit VLAN Manager client, or click **Cancel** to abort the operation and return to the previous screen.



For a controlled shutdown of the VLAN Manager client, use the **Exit** menu option. Shutting down the VLAN Manager client other than from the **Exit** menu option may cause unpredictable results.



When you exit the VLAN manager client, all windows will close except for those which run as separate processes (e.g., Element Management Tools).

Shutting Down VLANServer From the VLAN Manager Control Panel

1. Click the **Stop VLANServer** button. A confirmation box is displayed. Click **OK** to shut down the VLANServer. If you click **Cancel**, the VLANServer is not shut down. The VLANServer is not shut down until the VLANServer Message Window displays:

VLANServer has successfully shut down

and the Status field shows INACTIVE.

Exiting the SPECTRUM VLAN Manager Control Panel

To exit the Control Panel:

Click the  button. A confirmation box is displayed. Click **OK** to exit from the Control Panel. If you click **Cancel**, the program does not exit from the Control Panel.

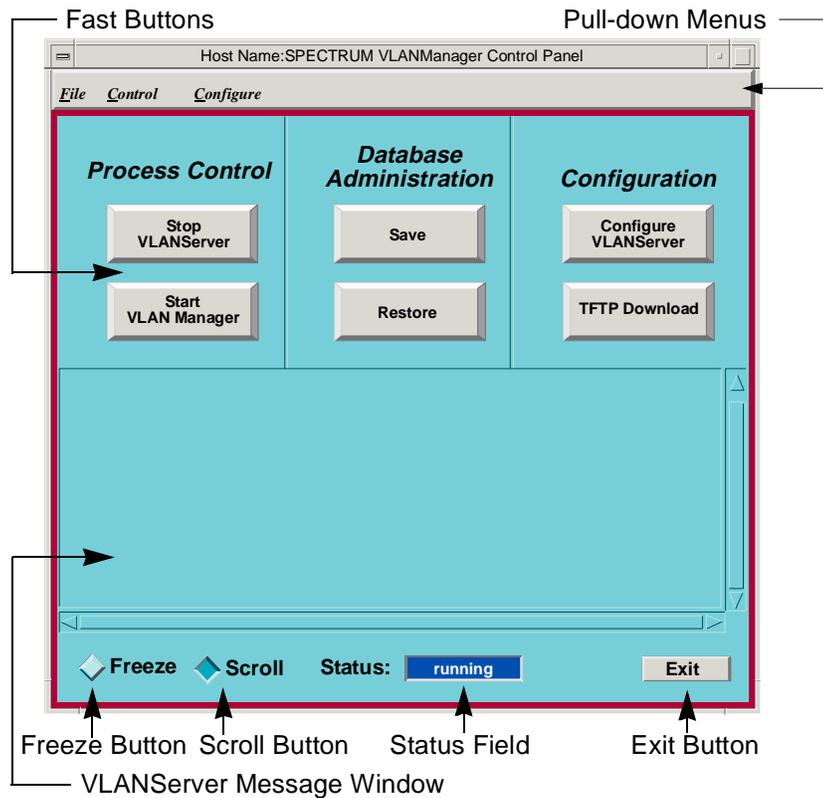


1. Processes you started from the Control Panel (e.g. VLANServer, VLAN client) continue after you exit the Control Panel. To regain control of these processes at any time, restart the Control Panel.
2. If you stop the VLANServer, the VLAN client will loose its connection to the VLANServer and exit automatically.

The SPECTRUM VLAN Manager Control Panel

The SPECTRUM VLAN Manager Control Panel, shown in [Figure 2-8](#), is divided into several functional areas: pull-down menus, fast buttons, VLANServer message window, **Freeze** button, **Scroll** button, **Status** field, and **Exit** button. The Control Panel can be used to start, stop, and administer VLAN Manager.

Figure 2-8. SPECTRUM VLAN Manager Control Panel

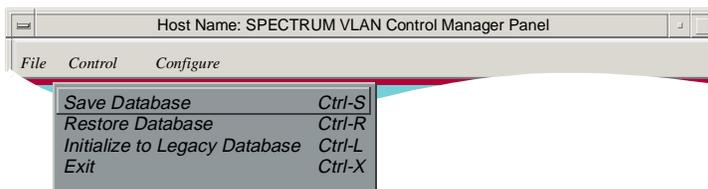


Pull-Down Menus

Pull-down menus provide an alternative means of activating control panel functions controlled by buttons. In some instances such as with the Initialize to Legacy Database function, the menus are the only way to activate functions.

File Menu

The **File** menu (Figure 2-9) combines functions from Database Administration buttons with the ability to exit from the SPECTRUM VLAN Manager Control Panel. Click on **File** to pull down and access selections from the **File** menu.

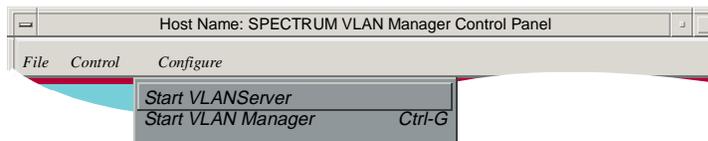
Figure 2-9. SPECTRUM VLAN Manager Control Panel File Menu

- **Save Database** - opens the File Selection dialog box letting you create a database save file. It serves the same function as the **Save** button.
- **Restore Database** - lets you load a previously saved database. It serves the same function as the **Restore** button.
- **Initialize to Legacy Database** - lets you initialize your database (restore it to the state that existed following your most recent install with no models of switches or VLANs created).
- **Exit** - closes the SPECTRUM VLAN Manager Control Panel. It serves the same function as the **Exit** button.

Keyboard shortcuts (keystroke combinations) for menu functions are shown to the right of each selection.

Control Menu

The **Control** menu (Figure 2-10) provides access to the same functions as the buttons in the **Process Control** area.

Figure 2-10. SPECTRUM VLAN Manager Control Panel Control Menu

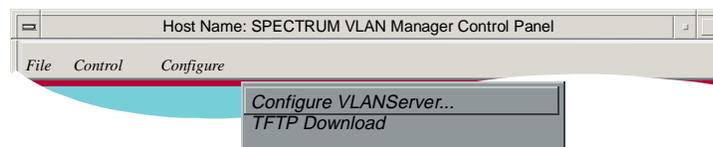
- **Start VLANServer** - Controls the operation of VLANServer. When the server is running, the button and the menu selection both are labeled **Stop VLANServer**. For information about starting and stopping VLANServer, refer to [Chapter 1, Introducing SPECTRUM VLAN Manager](#).
- **Start VLAN Manager** - Launches the VLAN Manager client. For information about starting the VLAN Manager client, refer to [Chapter 1, Introducing SPECTRUM VLAN Manager](#).

The text on some buttons turns red while VLANServer is running, to indicate that these functions will interrupt VLANServer operation.

Configure Menu

The **Configure** menu (Figure 2-11) provides access to the same functions that are available from the **Configuration** area. Selections from this menu let you configure certain VLANServer settings and download firmware.

Figure 2-11. SPECTRUM VLAN Manager Control Panel Configure Menu



Configure VLANServer - Lets you set VLANServer performance and communications settings.

TFTP Download - Lets you download firmware using the TFTP utility. For information about downloading firmware using this utility, refer to the *SPECTRUM VLAN Installation Guide*.

Fast Buttons

Three groups of buttons (Figure 2-12) control VLAN Manager tasks: **Process Control**, **Database Administration**, and **Configuration**.

- Start and stop VLANServer and start the VLAN Manager client.
- Save and restore the VLANServer database.
- Configure performance tuning parameters and download firmware to VLAN switches.



Pull-down menus provide an alternative means of activating Control Panel functions controlled by buttons. In some instances, such as the **Initialize to Legacy Database** option, these menu selections are the only way to activate functions.

VLANServer Message Window

Displays terminal dialog from operations affecting the VLANServer database.

Freeze Button

Stops VLANServer messages from scrolling.

Scroll Button

Resumes VLANServer messages scrolling.

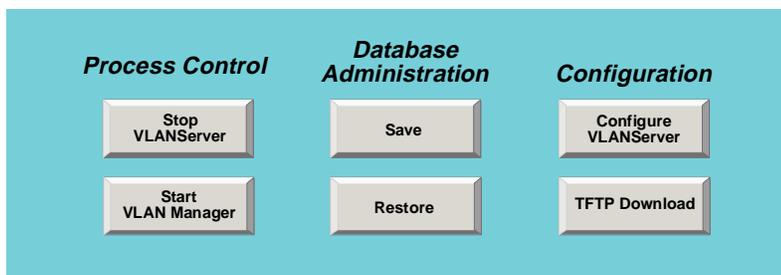
Status Field

Shows the current status for the VLANServer and database operations.

Exit Button

Closes the Control Panel. Processes you started from the Control Panel remain active; you can restart the Control Panel to regain control at any time.

Figure 2-12.

SPECTRUM VLAN Manager Control Panel Fast Buttons

VLANServer Message Window

This window displays output and errors for the VLANServer process. It indicates the server's progress during loading and shutdown and reports any internal errors. The message window can be controlled by the **Freeze** and **Scroll** buttons.

-  **Freeze** - stops messages from scrolling
-  **Scroll** - resumes message scrolling

Status Field

The **Status** field shows the current status for the VLANServer and database operations. As shown in the following table, both the text and background color of the field provide an indication of status. Status field background color is only used in the Motif windowing environment, not the OPEN Windows environment.

Table 2-1. VLANServer Status Field

Field Text/Color	Background Color	VLANServer Status
INACTIVE (White)	Blue	The server has not been started.
STARTING (Black)	Yellow	The server is starting. Clients cannot yet attach to the server.
RUNNING (Black)	Green	The server is up and running. Clients can attach in this state.
STOPPING (Black)	Yellow	The server is being administratively shut down.
TERMINATED (Red)	Blue	The server has abnormally terminated. This should not occur during normal operation.
SAVING (Black)	Yellow	The server database is being backed-up. The server is in an inactive state.
RESTORING (Black)	Yellow	The server database is being restored from a backup. The server is an inactive state.

Exit Button

 Closes the SPECTRUM VLAN Manager Control Panel. Processes you started from the Control Panel remain active, and you can restart the Control Panel to regain control at any time. The control panel automatically synchronizes with the VLANServer and displays the current status.

Saving the VLANServer Database

There are three methods of saving the VLANServer database:

- Online Backup - This is the simplest, and preferred method. See *On-Line Backup on Page 16-1*.
- Complete save (models and catalog) - See *Saving the Database (Models and Catalog)*, below.
- Models only - See *Saving the Database (Models Only) on Page 2-17*.

Saving the Database (Models and Catalog)

This procedure initiates a complete save of the VLANServer database models and catalog. You can select a file name from a list of previous backups (overwrites the previous backup file), or you can enter a new file name. If the VLANServer is running when you initiate a save, it is shut down for the duration of the save operation and restarted when the save is completed.

To do a complete save of the VLANServer database:

1. On the Control Panel, select the **Save** button or **Save Database** from the **File** menu. The Select File to Save Database... dialog box ([Figure 2-13](#)) is displayed. Refer to [The Select File to Save Database... Dialog Box](#), for information about how to use this dialog box.
2. Type the path and filename for your database save file in the Selection text box.



If you are saving the VLANServer Database in preparation for upgrading to a newer version of VLAN Manager, choose a path that is NOT within the VLAN Manager install area to avoid accidentally removing the saved database during the upgrade.

3. Click **OK**. If VLANServer is running, a confirmation dialog box is displayed.
4. Click **OK** to begin the save. Click **Cancel** to terminate save without disturbing existing files.

Once the save is started, the Control Panel **Status** changes to **Saving**. When the save is finished, the VLANServer is restarted and the Control Panel **Status** message changes to **Running**.



You can also save your database using **Online Backup** which is available from the VLAN Manager's **File** menu. See *On-Line Backup on Page 16-1*.

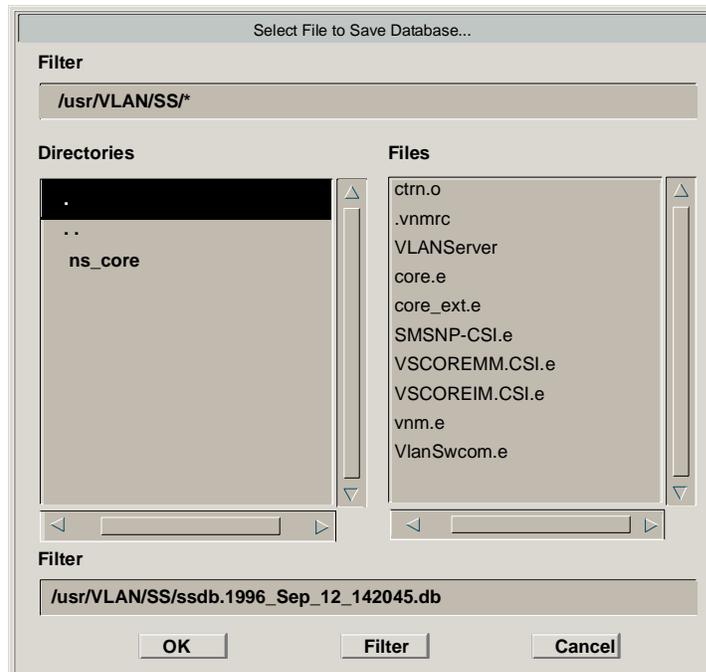
The Select File to Save Database... Dialog Box

The Select File to Save Database dialog box (Figure 2-13) is frequently used to define the path and filename for a file to be saved or opened.

The **Filter** field allows you to set a path and file filter. A filter sets the path for the files displayed in the **Files** window and, with the use of standard wildcards, limits the filenames that appear in the **Files** window.

To use the filter feature, enter a path in the **Filter** field and press the **Filter** button to activate the filter. The **Directories** scroll field lists directories within the directory defined by your filter. The **Files** scroll field lists files within the directory defined by your path filter. The selection is the file path and filename for the file you are saving or restoring. If you specify an existing file, that file will be overwritten.

Figure 2-13. Select File to Save Database... Dialog Box



Saving the Database (Models Only)

This procedure saves your existing database models, without saving the catalog.

To save your database models only:

1. From a VLAN Shell or Unix terminal session navigate to the `<install root>/VLAN/server` directory.
2. Create a saved file of the models in your database using the following command:

```
../../../../SS-Tools/SSdbsave -m <filename>
```

3. Copy the newly saved database file `<filename>.db` to an area other than the VLAN Manager install area and make note of its location.

Restoring the VLANServer Database

There are three methods of restoring a VLANServer database. The method you use depends on your circumstances.

- **Restoring from a saved database (current release):** This method loads models from a VLANServer database saved with the *currently installed* release of VLAN Manager, into your existing database. You would use this method if, for example, your existing database were corrupted, or if your VLANServer machine failed, and your backup database had been saved with the currently installed release of VLAN Manager. To use this method, refer to [Restoring from a Saved Database \(Current Release\)](#), below.
- **Restoring from a saved database (previous release):** This method loads models from a VLANServer database saved with a *previous* release of VLAN Manager, into your existing database. You would use this method if, for example, your existing database were corrupted, or if your VLANServer machine failed, and your backup database had been saved with a previous release of VLAN Manager. To use this method, refer to [Restoring from a Saved Database \(Previous Release\)](#) on [Page 20](#).
- **Initializing to the legacy database:** This method clears all the models from your existing database. You might use this method if your existing database were corrupted, and you did not have a backup. You might also use it if you have changed the IP address of the VLANServer machine. To use this method, refer to [Initializing to the Legacy Database](#) on [Page 2-20](#).

Restoring from a Saved Database (Current Release)



After you use the **Restore** button or **File >Restore Database** menu option to restore a VLANServer database, run Discovery to ensure that the information maintained by the VLANServer database is synchronized with the information maintained by the network switches.

To restore the models from a VLANServer database saved with the current version of VLAN Manager:

1. In the Control Panel, click the **Restore** button or select **Restore Database** from the **File** menu. A dialog box appears, asking if you wish to initialize your database.
2. Click **No** to restore both the model and catalog information from the database file you specify into your current database. The Select File to Restore Database... Dialog box is displayed ([Figure 2-14](#)).

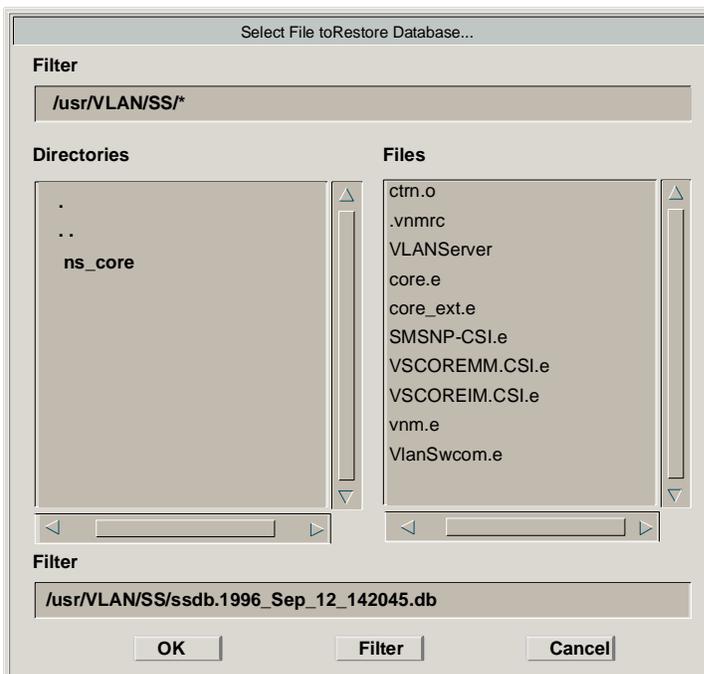


If you answer **Yes** to the question asking if you want to initialize the VLANServer's database also, you will replace your current database with the catalog from the database file you specify. All models will be deleted.

3. Set the path, select a previously-saved database file using the **Select File to Save Database** option, and then click **OK**. If the VLANServer is running, a confirmation box is displayed.
4. Click **OK** to begin the restore. Click **Cancel** to terminate the restore without disturbing the current database.

Once the restore has begun, the Control Panel **Status** message changes to **Restore**. When the Restore is complete and the VLANServer starts up again, the **Status** field changes to **Running**.

Figure 2-14. Select File to Restore Database... Dialog Box



Restoring from a Saved Database (Previous Release)



After you use the the SSdbload command-line tool to restore a database, run Discovery to ensure that the information maintained by the VLANServer database is synchronized with the information maintained by the network switches.

- a. From a VLAN Shell or Unix terminal session, copy the saved database file into the `<install root>/VLAN/server` directory.
- b. Navigate to the `<install root>/VLAN/server` directory.
- c. Restore the models to your database using the following command:

```
../../../../SS-Tools/SSdbload -m <filename>
```

Initializing to the Legacy Database

Initializing to the legacy database clears all the models from your existing database, leaving a database structure consisting of the modeling catalog and a limited number of hidden internal models. You might use this procedure if your existing database were corrupted, and you did not have a backup. You might also initialize if you have changed the IP address of the VLANServer machine.

If the VLANServer is running, it will be shut down during the initialization operation and restarted when it is completed. You cannot initialize the database when save or restore operations are in progress.



Do not initialize your database without first making a backup copy of it. All models specific to your network are removed during initialization.

To initialize your VLANServer database:

1. In the Control Panel, select **Initialize to Legacy Database** from the **File** menu. An information dialog box is displayed, warning you of the consequences of initializing.
2. If you understand the consequences and still want to initialize your database, click **OK**. If you want to retain your existing database, click **Cancel**.

3. If the VLANServer is running when you start to initialize your database, a second information dialog box is displayed. Click **OK** to start the initialization.

Configuring the VLANServer

You can configure VLANServer performance and communications settings (Figure 2-15). By changing the defaults for these settings, you can improve the performance of the VLANServer and ensure optimal communication between the VLANServer, VLAN Manager client, or other network management applications.

Figure 2-15. SecureFast VLANServer Configuration Window

Performance Tuning

- **Max. Number of Request Threads** - This number represents the number of requests sent to the VLANServer by the models (e.g., switches, ports, and users) in the VLANServer database. The default is 256. If the number of models being managed by the VLANServer does not exceed 4000, the default setting provides maximum software performance. If the number of models being managed exceeds 4000, increasing **Max. Number of Request Threads** could provide a slight increase in software performance. To calculate the **Max. Number of Request Threads**, divide

the total number of models in the VLANServer database by 16. For example, if the number of models is 6000, the **Max. Number of Request Threads** should be set to approximately 375 (6000/16).

- **Max. Total Work Threads** - This number represents the total number of threads used by all VLANServer subsystems. The default is 512. It should be set to 256 more than **Max. Number of Request Threads**. If you change the **Max. Number of Request Threads** value from the default setting of 256, you should change **Max. Total Work Threads** accordingly.
- **Max. Total Polling Threads** - This number represents the total number of threads used by the VLANServer to poll switches. The default is 20. If the information displayed in VLAN Manager windows is out of sync (does not match) the information contained in the switches being managed by the VLANServer, you should consider incrementally increasing the **Max. Number of Polling Threads** value.
- **Mail Queue Size** - Number of slots reserved by the VLAN Manager client for solicited communication with the VLANServer. Each slot is approximately 64 bytes. This value must be larger than the number of models in the database.
- **Unsolicited Queue Size** - Number of slots reserved by the VLAN Manager client for unsolicited communication with the VLANServer.

Communications

- **Communications Port Number** - Port that the VLAN Manager client uses to communicate with the VLANServer. The default port number is 0xd741.
- **SNMP Comm. Port Number** - Port that the VLAN Manager client uses to communicate with SNMP compliant network management applications.

VLANServer Configuration

To configure the VLANServer:

1. Click the **Configure VLANServer** button or select **Configure VLANServer** from the **Configure** menu. The SecureFast VLANServer Configuration window ([Figure 2-15](#)) is displayed.
2. To change the information in any text box, highlight the information in the box and then type in the new information.

3. Click **OK** to accept the changes or **Cancel** to dismiss the SecureFast VLANServer window without making changes.



In order for changes to take effect, the VLANServer must be stopped and then re-started.

Processd

'Processd' is a process launching and tracking daemon that provides the Control Panel with the ability to control various processes (e.g., database saves and restores) that are run on various servers and clients in a distributed VLANServer environment. 'Processd' starts processes when requested by an application such as the SPECTRUM VLAN Manager Control Panel. It can also start processes on system boot if configured by the user and can automatically restart critical processes in the event they terminate unexpectedly.

Processes are launched and tracked via processd only when an application requests such actions. Under normal circumstances, processd operates in the background and is invisible to the user. However, there are two reasons users may need to reconfigure processd data:

- Something in the 'processd' database has become corrupted. When this occurs, the message, "Process Daemon cannot be contacted to run external application" is displayed on the screen, and 'processd' must be stopped, reinitialized, and restarted.
- A machine has been dedicated to maintain a VLANServer process and would like it to start at system boot time using the '.autostartc' file.

'Processd' is automatically started during the VLANServer installation. The install makes the necessary changes so that when the system is started up the 'processd' will also start. 'Processd' must be run as root. This requirement is handled by system startup, as most processes executed during this time run as root.

Reinitializing processd

If 'processd' fails and the message "Process Daemon cannot be contacted to run external application" is presented, it's likely that the processd database has been corrupted and will need to be reinitialized. To reinitialize processd on supported Solaris or NT operating systems, do the following:

1. Become root or Administrator.
2. Change directories to the <VLAN install area/SDPM>.
3. Make sure that all VLANServer processes that can be shutdown are, otherwise this can cause problems with the VLANServer.

4. Type `processd.sh stop`. This stops 'processd'.
5. Type `makeinstdb -dir /<directory location of VLAN Install Root>`.
6. Type `readinstdb` to read the install database.
7. Remove the `CsProcDb.k` file by typing `rm CsProcDb.k`.



Even though the database is already corrupted, removing the `CsProcDb.k` file alerts the `processd` daemon that there is a problem and allows it to proceed with reinitialization.

8. Type `processd.sh start`. This will put `processd` back in a running state.

Exploring VLAN Manager

This chapter introduces VLAN Manager's client user interface. It provides detailed information about VLAN Manager's Main window, the tasks that can be launched from this and other windows, and the user-friendly features of the user interface that make it easy to use.

VLAN Manager Windows

VLAN Manager windows are grouped into four types: Main, Information, Dialog, and Views.

- **Main** - This window is your gateway to all VLAN Manager tasks and appears whenever you start the VLAN Manager application.
- **Information** - The primary purpose of this type of window is to present information. Information windows are not normally editable and usually do not require user input. The Directory is an example of this type of window.
- **Dialog** - The primary purpose of this type of window is to provide information required before an operation can be performed. Dialog windows can also present a limited amount of data. The Create VLAN dialog box is an example of this type of window. Properties windows and tabbed folders are also forms of the dialog box.
- **Views** - This type of window presents topological information. The Topology view is an example of this type of window.

This section describes each of the four types of VLAN Manager windows.

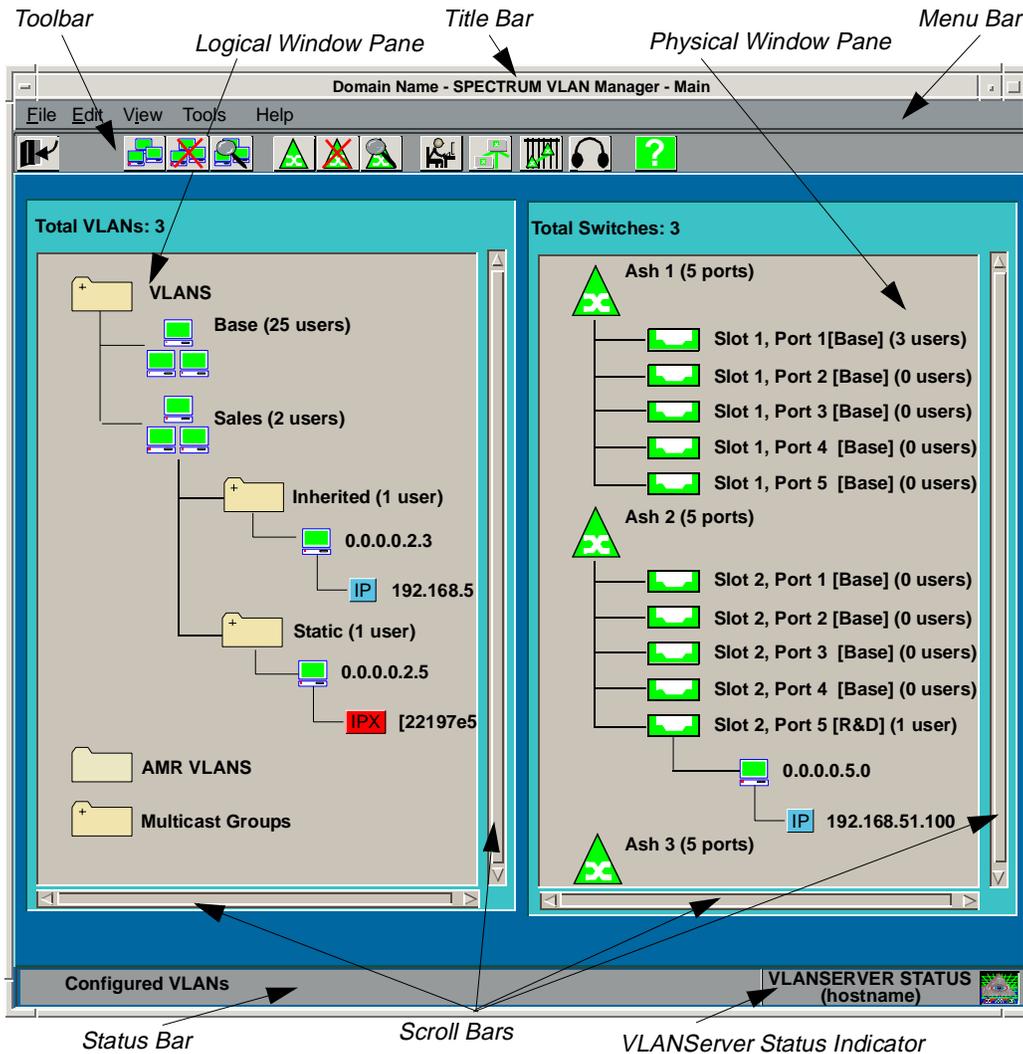
Main Window

The VLAN Manager Main window ([Figure 3-1](#)) consists of the following parts:

- **Title Bar** - Displays the name of the window and the name of the current domain.
- **Menu Bar** - Lists the names of the available menus. Select a menu to display a list of items.

- **Tool Bar** - Displays available graphical command buttons.
- **Logical Window Pane** - Uses a tree structure to display information about configured VLANs, AMR VLANs and IP Multicast Groups. Many VLAN management tasks can be initiated from this pane.
- **Physical Window Pane** - Uses a tree structure to display information about discovered switches, ports, and users. Many switch management tasks can be initiated from this pane.
- **Scroll Bars** - Move part of the VLAN or Switch window pane contents into view when the entire contents will not fit in the pane.
- **Status Bar** - Displays VLAN Manager generated error and cursor location information. Error messages not related to the Main window are displayed in dialog boxes.
- **VLANServer STATUS Indicator** - Displays color-coded information about VLANServer's operational condition.

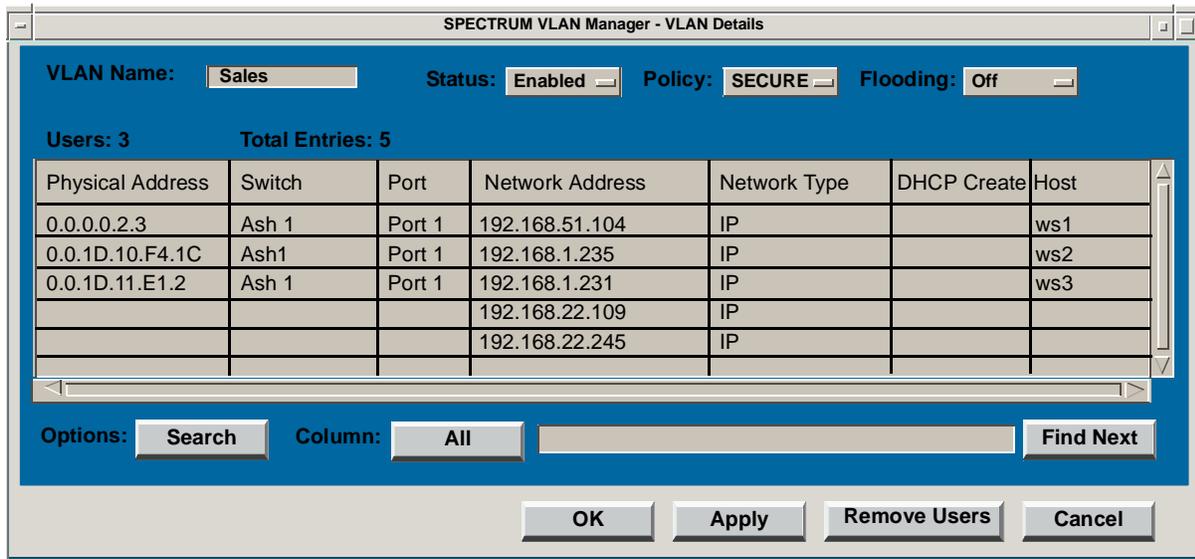
Figure 3-1. VLAN Manager Main Window



Information Windows

VLAN Manager information windows show data using various formats. For instance, an information window designed to present information about VLANs will display data such as Physical Address, Switch, and Port, whereas a window designed to present information about connections will display data such as Source Alias, Destination Alias, and Duration. VLAN management operations may be initiated from information windows. [Figure 3-2](#) shows an example of an information window.

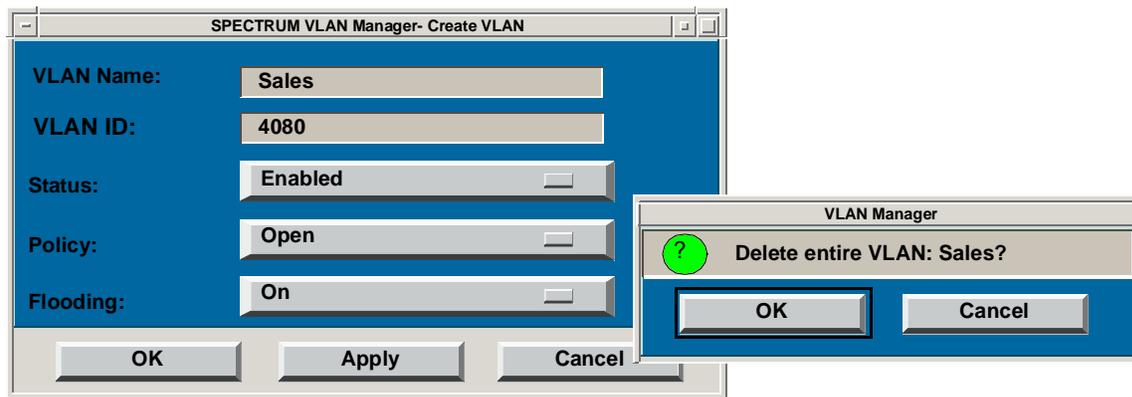
Figure 3-2. Information Window



Dialog Boxes

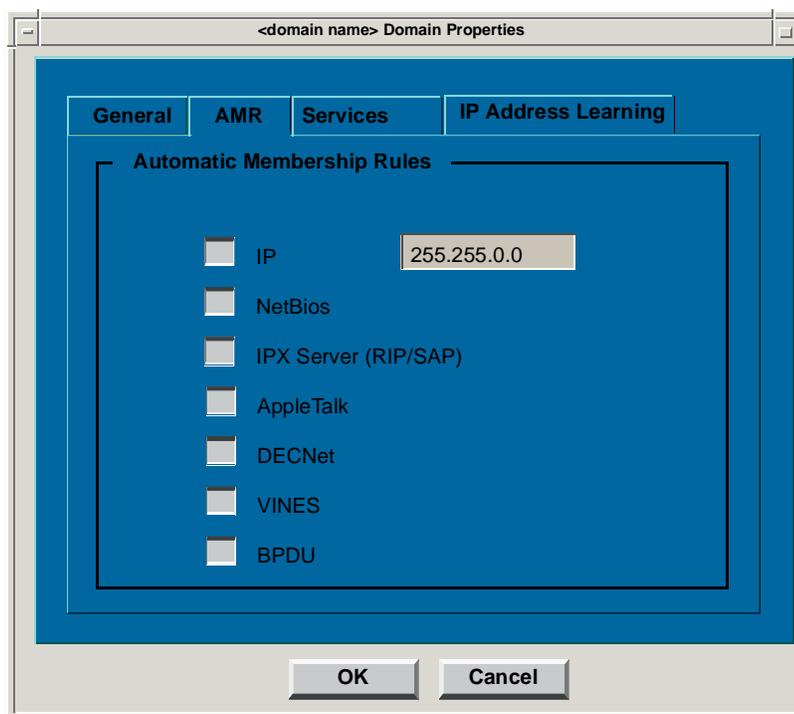
Dialog boxes may be displayed while performing operations. They usually ask you for additional information, such as entering text or selecting options, however, a dialog box can provide information which does not require more information or a response (e.g., a dialog box containing error information). Examples of two dialog boxes are shown in [Figure 3-3](#).

Figure 3-3. Dialog Boxes



Another type of dialog box is called a tabbed folder. Tabbed folders consist of tabbed pages. Each page displays information about a set of related properties. Properties on a tabbed page are presented in one of two modes: read-only or read-write. Read-only properties cannot be edited. Read-write properties can be edited. Changes to a property are applied when you click **OK**. If a change is made outside a tabbed page while the tabbed page is open, the change will not be displayed until the dialog box is closed and then reopened. An example of a tabbed folder is shown in [Figure 3-4](#).

Figure 3-4. Tabbed Folder



Views

VLAN Manager views show graphical topological information. The Topology view shows the switches and links associated with a particular domain. The Path view shows end-to-end connectivity of a particular call. Both views use color to represent the condition of a given switch or link.

VLAN Manager Menus

VLAN Manager provides several main menus from which you can choose VLAN administration functions. Menu names appear in the menu bar across the top of a window. When you select a main menu, its corresponding pull-down menu is displayed.

Pull-Down Menus

Pull-down menus are located in the menu bar across the top of the main VLAN Manager window. You open a pull-down menu by clicking on a menu title with the left mouse button. To make a selection within an open pull-down menu, click on the item. To close a pull-down menu without making a selection, move the pointer off the menu and click the left mouse button. If your menu item cannot be initiated, an error message will be displayed in the status bar indicating the problem and a beep will sound.

Some main menus present submenus. The existence of a right arrow (>) character to the right of a menu selection indicates the existence of a submenu. Placing the mouse pointer on such an item and clicking the left mouse button opens the submenu. To close the submenu, select another item from the parent menu, or move the pointer off the pull-down menu entirely and click the left mouse button.

Pop-Up Menus

Pop-up menus are available from most VLAN Manager windows. They let you perform administrative tasks without having to choose an item from a menu bar or toolbar. You execute a pop-up menu item using the right mouse button. Click and hold on a field or icon, and then drag to the item you want to execute. Release the mouse button. To close a pop-up menu without executing an item, move the pointer off the menu and release the right mouse button.

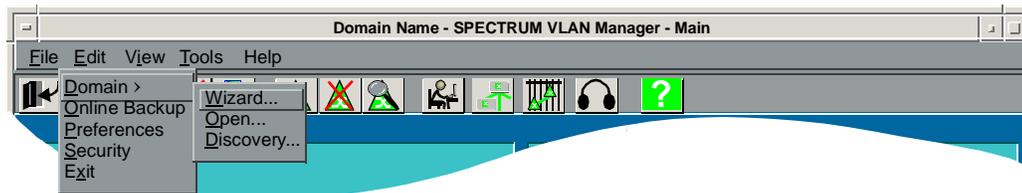
Menu Descriptions

This section describes Main window menus. Other window menus are described during the discussion of specific windows, such as the Directory.

File Menu

The **File** menu (Figure 3-5) consists of the following items: **D**omain, **O**nline Backup, **P**references, **S**ecurity, and **E**xit. The Domain item provides access to additional menu items.

Figure 3-5. File Menu

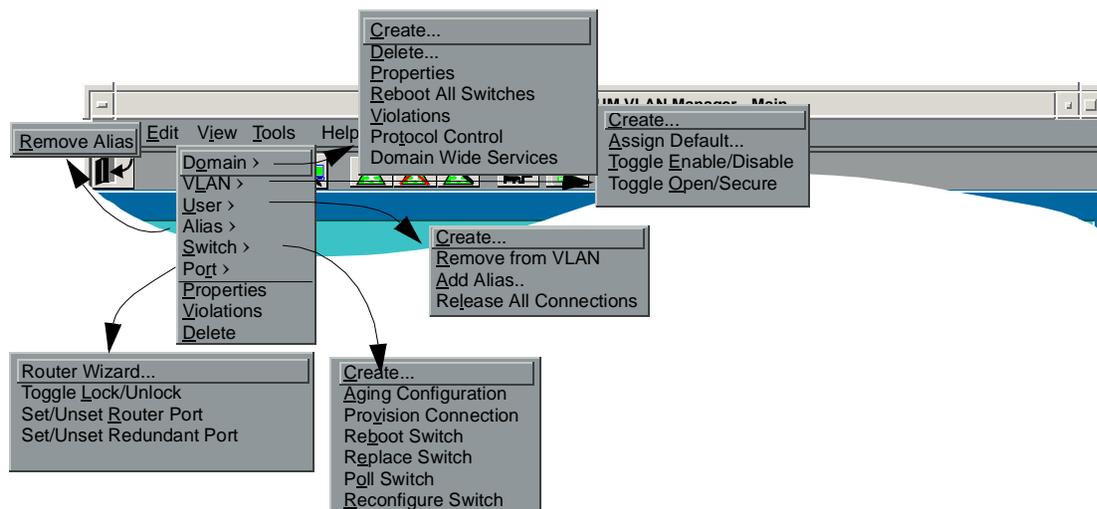


- **Domain** - opens the domain maintenance submenu allowing you to perform domain maintenance tasks. This menu consists of the following items: **W**izard, **O**pen, and **D**iscovery.
 - **Wizard** - Steps you through the process of creating, configuring, and discovering domains. Refer to *VLAN Manager Domain Discovery Wizard*, on page 6-1 for information about how to use the VLAN Discovery Wizard.
 - **Open** - Lets you open any domain known to the VLANServer. Refer to *Opening Domains*, on page 6-14, for information about how to open a domain.
 - **Discovery** - Discovers the switches, links, users, aliases, and VLANs contained in a domain. Refer to *Creating Domains*, on page 6-16, for information about how to discover a domain.
- **Online Backup** - Lets you configure VLAN Manager to automatically backup your VLANServer database on demand or at a scheduled interval without bringing the VLANServer down. Refer to [Chapter 16, Managing Your Database](#).
- **Preferences** - Lets you define Global, Main, Topology view, Path Trace, and Connection Table settings for VLAN Manager. Refer to [Chapter 5, Managing Preferences](#), for information about how to set preferences.
- **Security** - Lets you define which users have permanent connection privileges to the VLANServer, define what level of security each user is assigned, and lets you define which host systems can connect to the VLANServer. Refer to [Chapter 4, Managing Security](#) for information about how to set security.
- **Exit** - Displays the Exit VLAN Manager confirmation box. Click **OK** to exit VLAN Manager or **Cancel** to return to the VLAN Manager main window. You can also exit VLAN Manager by clicking on the  icon on the Menubar.

Edit Menu

The **Edit** menu (Figure 3-6) consists of the following items: **D**omain, **V**LAN, **U**ser, **A**lias, **S**witch, and **P**ort, all of which provide access to additional menu items and three smart menu picks, **P**roperties, **V**iolations, and **D**elete. The dialog box displayed when you click a smart menu pick and the action taken depends on what icon is currently selected (VLAN, User, Alias, Switch, Port) in the SPECTRUM VLAN Manager's Main window at the time you click the menu pick. For example, if a port is selected and you click **Properties**, the Port Properties tabbed folder is displayed. If however, a user is selected and you click **Properties**, the User Properties tabbed folder is displayed. If no action can be taken for the selected icon, a message indicating why the action cannot be taken is displayed in the Status Bar at the bottom left of the Main window.

Figure 3-6. Edit Menu



- **D**omain - Opens the Domain submenu, which lets you perform Domain maintenance tasks. This menu consists of the following items: **C**reate, **D**elete, **P**roperties, **R**eboot All Switches, **V**iolations, **P**rotocol Control, and **D**omain Wide Services.
 - **C**reate - Lets you create domains. Refer to *Creating Domains*, on page 6-16, for information about how to create a domain.
 - **D**elete - Lets you delete domains from the VLANServer database. Refer to, *Deleting Domains*, on page 6-17 for information about how to delete a domain.
 - **P**roperties - Lets you configure general domain, AMR, IP Multicast properties, and IP Address Learning. Properties consists of four tabbed pages: General, AMR, Services, and IP Address Learning. Refer to *Domain Properties*, on page 6-18, for information about how to configure general domain properties.

Refer to *AMR VLAN Administration*, on page 9-19 for information about how to configure AMR properties. Refer to *Editing Multicast Properties*, on page 12-3, for information about how to configure Multicast services.

- **Reboot All Switches** - Lets you reboot all the switches in a domain from the user interface without having to physically push the reset button on each switch. Refer to *Domain Details*, on page 6-30, for information about how to reboot all switches.
- **Violations** - Lets you view domain restriction violations. For more information about violations and how to remedy them, refer to *Violations*, on page 10-32.
- **Protocol Control** - Lets you enable and disable configured protocols and frame types. The primary purpose of implementing Protocol Control is to reduce the amount of broadcast traffic on your network by limiting the types of protocols and protocol frame types that the switches being managed by a VLANServer will process. For more information, refer to *Protocol Control*, on page 6-38.
- **Domain Wide Services** - Lets you enable or disable configured services for all switches in a domain. For more information, refer to *Domain Wide Services*, on page 6-41.
- **VLAN** - Opens the VLAN submenu, which lets you perform VLAN maintenance tasks. This menu consists of six commands: **Create**, **Assign Default**, **Toggle Enable/Disable**, and **Toggle Open/Secure**.
 - **Create** - Lets you create new VLANs in the current domain. Refer to *Creating VLANs*, on page 9-2.
 - **Assign Default** - Lets you assign a VLAN to be the default VLAN for multiple switch ports. Refer to *Assigning a Default VLAN to Multiple Switch Ports*, on page 9-18.
 - **Toggle Enable/Disable** - Lets you Enable or Disable a VLAN. Users in disabled VLANs cannot communicate. Refer to *Creating VLANs*, on page 9-2.
 - **Toggle Open/Secure** - Lets you change the policy attached to a VLAN to be OPEN or SECURE. Refer to *Creating VLANs*, on page 9-2.
- **User** - Opens the user submenu, allowing you to perform user maintenance tasks. This menu consists of the following items: **Create**, **Remove from VLAN**, **Remove from Switch**, **Add Alias**, and **Release All Connections**. If a user is selected from the Logical pane, the items are: **Create**, **Remove from VLAN**, **Add Alias**, and **Release All Connections**. If the user is selected from the Physical pane, the items are: **Create**, **Remove from Switch**, **Add Alias** and **Release All Connections**.
 - **Create** - Lets you create new users in the current domain. Refer to *Creating a User*, on page 10-1.
 - **Remove from VLAN** - Lets you remove a user from a VLAN. If the user is not a member of any other VLANs, it is returned to the default VLAN for the port. This may or may not be the Base VLAN. Refer to *Removing Users from a VLAN*, on page 10-4.

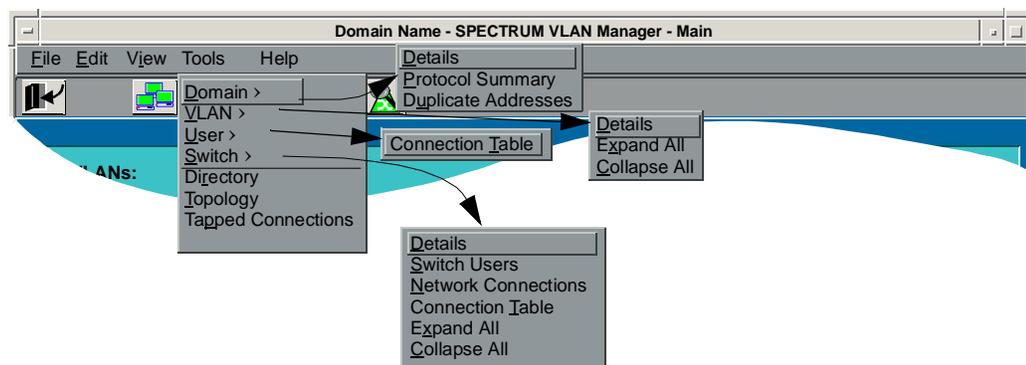
- **Remove from Switch** - Lets you remove a user from a port in anticipation of being learned on another port. The user icon is grayed out and all connections for that user are torn down. Remove allows a user to maintain VLAN memberships while physically relocating. Refer to *Removing a User from a Switch*, on page 10-3.
- **Add Alias** - Lets you add a network alias to a user that is running more than one protocol. Refer to *Adding a User Alias*, on page 10-10.
- **Release All Connections** - Releases all active calls for the selected user.
- **Alias** - Opens the alias submenu, allowing you to perform alias maintenance tasks. This menu consists of the following item: **Remove Alias**. This task can also be initiated from the Alias pop-up menu.
 - **Remove Alias** - Lets you remove a network alias to a user that is running more than one protocol.
- **Switch** - Opens the switch submenu, allowing you to perform switch maintenance tasks. This menu consists of the following items: **Create**, **Aging Configuration**, **Provision Connection**, **Reboot Switch**, **Replace Switch**, **Poll Switch**, and **Reconfigure Switch**.
 - **Create** - Lets you create new switches in the current domain. Refer to *Adding a Switch*, on page 7-2.
 - **Aging Configuration** - Lets you configure call aging parameters to optimize call aging. Refer to *Aging Connections*, on page 11-14.
 - **Provision Connection** - Lets you set up calls manually. Refer to *Provisioning Calls*, on page 11-18.
 - **Reboot Switch** - Lets you reboot an individual switch. Refer to *Rebooting an Individual Switch*, on page 7-17 for detailed information about rebooting a switch.
 - **Replace Switch** - Clears the address information of the switch that was replaced from the alias tables of all switches in a domain. Refer to *Replacing a Switch*, on page 7-18.
 - **Poll Switch** - Lets you force a switch to start a polling cycle. Refer to *Forcing a Switch to be Polled Immediately*, on page 7-16.
 - **Reconfigure Switch** - Lets you force a switch to start a synchronization cycle. Refer to *Forcing a Switch to Reconfigure Immediately*, on page 7-16.
- **Port** - Opens the port submenu, allowing you to perform port maintenance tasks. This menu consists of the following items: **Router Wizard**, **Toggle Lock/Unlock**, **Set/Unset Router Port**, and **Set/Unset Redundant Port**.
 - **Router Wizard** - Launches the router port configuration application.
 - **Toggle Lock/Unlock** - Lets you Lock or Unlock ports. Users connecting to a locked port become members of the default VLAN for the port. Refer to *Locking/Unlocking a Port*, on page 8-24.

- **Set/Unset Router Port** - Lets you set and unset access port(s) to be a router port(s). Once the port is toggled the port icon changes, depending on what type of port it is set for:  for a router port,  for a user access port. Refer to *Setting/Unsetting a Router Port*, on page 8-24.
- **Set/Unset Redundant Port** - Lets you set and unset redundancy for user(s) that have been attached to more than one port. Refer to *Redundant Access*, on page 8-25.
- **Properties** - Lets you change some attributes of the selected User, Alias, Port, Switch, or VLAN.
- **Violations** - Lets you view port and user restriction violations for the selected User, Alias, Port, or Switch. For more information about violations and how to remedy them, refer to *Violations*, on page 10-32.
- **Delete** - Lets you:
 - Delete entire VLANs from the database.
 - Delete a user permanently. Users that are deleted are removed from all ports and VLANs. They are completely removed from the VLANServer database and the switch. Refer to *Deleting a User*, on page 10-5.
 - Delete switches from the VLANServer database. Refer to *Deleting a Switch*, on page 7-3.

View Menu

The **View** menu (Figure 3-7) consists of the following items: **Domain**, **VLAN**, **User**, **Switch**, **Directory**, **Topology**, and **Tapped Connections**.

Figure 3-7. View Menu



- **Domain** - Opens the **Domain** submenu allowing you to view the details of a particular domain. This menu consists of the following items: **Details**, **Protocol Summary**, and **Duplicate Addresses**.

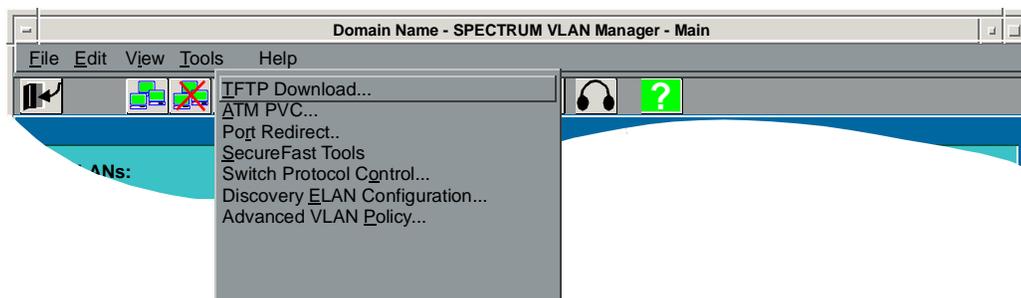
- **Details** - Lets you display detailed information about the current domain. Refer to *Domain Details*, on page 6-30.
- **Protocol Summary** - Lets you view the status (On/Off) of protocols configured on all switches in the current domain. To edit domain protocol policy, select **Protocol Control** from the **Edit>Domain** menu. Refer to *Domain Properties on Page 6-18* for information about setting switch protocols.
- **Duplicate Addresses** - Lets you view endpoints with duplicate addresses. Refer to *Finding Duplicate Network Addresses*, on page 10-19.
- **VLAN** - Opens the VLAN submenu allowing you to view the details of a particular VLAN and control the amount of information displayed in the VLANs area. This menu consists of three items: **Details**, **Expand All**, and **Collapse All**.
 - **Details** - Lets you display detailed VLAN and VLAN user information about a particular VLAN. You can also use this window to remove users from the selected VLAN. Refer to *Displaying VLAN Details*, on page 9-9.
 - **Expand All** - Displays all leafs of the VLAN hierarchy.
 - **Collapse All** - Displays only the root of the VLAN hierarchy.
- **User** - Opens the User submenu allowing you to view the details of a particular user. This menu consists of **Connection Table**.
 - **Connection Table** - Launches the Connection Table filtered for the selected user. Refer to *Launching the Connection Table*, on page 11-1.
- **Switch** - Opens the Switch submenu letting you view the details of a particular Switch and control the amount of information displayed in the Switches area. This menu consists of the following items: **Details**, **Connection Table**, **Network Connections**, **Switch Users**, **Expand All**, and **Collapse All**.
 - **Details** - Lets you display detailed switch and port information about a particular switch. Refer to *Displaying Switch Details*, on page 7-11.
 - **Switch Users** - Displays the Directory for a particular switch. Details about all users attached to the switch are shown. Refer to *Using the Directory*, on page 10-14 for more information about switch users.
 - **Network Connections** - Displays the Network Connections window. Refer to *Viewing Domain Topologies*, on page 13-1 for more information about network connections.
 - **Connection Table** - Lets you display the Connection Table, which provides detailed information about connections specific to the selected switch. Refer to *Launching the Connection Table*, on page 11-1.
 - **Expand All** - Displays all leafs of the switch hierarchy.
 - **Collapse All** - Displays only the root of the switch hierarchy.

- **Directory** - Displays detailed information about each user in the current domain. Menus let you perform related user procedures. Search and filter options help you locate a user quickly.
- **Topology** - Displays the switches and their network connections for the current domain. Refer to *Viewing Domain Topologies*, on page 13-1.
- **Tapped Connections** - Lets you view tapped connections associated with the current domain.

Tools Menu

The **Tools** menu (Figure 3-8) consists of the following items: **TFTP Download**, **ATM PVC**, **Port Redirect**, **SecureFast Tools**, **Switch Protocol Control**, **Discovery ELAN Configuration**, and **Advanced VLAN Policy**.

Figure 3-8. Tools Menu



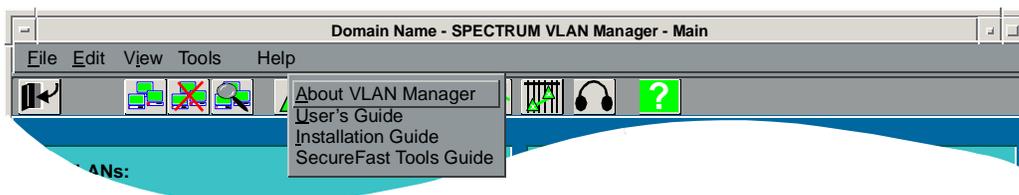
- **TFTP Download** - Lets you download switch firmware. Refer to *Downloading Firmware to a Switch*, on page 7-15.
- **ATM PVC** - Lets you create Permanent Virtual Circuits (PVCs) across ATM networks. Refer to *Managing VLANs Over ATM Networks Using Permanent Virtual Circuits*, on page 14-2.
- **Port Redirect**- Lets you redirect data from one or more interfaces directly to another interface, essentially mirroring the traffic at the “redirect” interface. Refer to *Redirecting a Port*, on page 8-39.
- **SecureFast Tools**- Brings up the SecureFast Tools submenu. From this menu you can launch the following tools: Element Management, Capacity Monitor, Connection Diagnostics, and Trap Manager. Refer to *SecureFast Tools Guide* for detailed information about SecureFast Tools.
- **Switch Protocol Control** - Lets you edit the administrative status of protocols and protocol frame types on a per switch basis. Refer to *Switch Protocol Control*, on page 7-19.

- **Discovery ELAN Configuration** - Lets you edit the administrative status of discovery ELANs.
- **Advanced VLAN Policy** - Launches the Advanced VLAN Policy application. Refer to [Chapter 15, Advanced VLAN Policy](#) for detailed information about this application.

Help Menu

The **Help** menu ([Figure 3-9](#)) consists of the following items: **About VLAN Manager**, **User's Guide**, **Installation Guide**, and **SecureFast Tools Guide**.

Figure 3-9. Help Menu



- **About SPECTRUM VLAN Manager** - Identifies the version of VLAN Manager running on the host machine.
- **User's Guide** - Displays the SPECTRUM VLAN Manager User's Guide in PDF (Portable Document Format) format using Acrobat™ Reader.
- **Installation Guide** - Displays the SPECTRUM VLAN Manager Installation Guide in PDF (Portable Document Format) format using Acrobat™ Reader.
- **SecureFast Tools Guide** - Displays the SecureFast Tools Guide in PDF (Portable Document Format) format using Acrobat™ Reader.

Choosing Menu Items

Menu items are used to perform VLAN administration tasks. Some items perform tasks as soon as you select them; others open dialog boxes which require additional input.

To execute a menu item do any one of the following:

- Select a menu and then click on the item you want to execute, or drag the cursor down the menu until the item you want to execute is highlighted.
- Click the graphical command tool that corresponds to the action you want to execute.

- Select the accelerator key for the item you want to execute. Accelerator keys let you execute a menu item without having to select a menu and then an item. You execute a item associated with an accelerator key by pressing the Alt key followed by the accelerator key for the item you want to execute. One letter in each menu item is underlined. That letter is the accelerator key for that item.

VLAN Manager Tool Bar

VLAN Manager provides a strip of graphical command tool icons. These icons are located under the menu bar and provide a convenient way to access the most common VLAN administration functions without having to select a menu and choose an item. Position the cursor over an icon to display a pop-up (fly-by, tool-tip) text box, which describes the function of that icon.

For example, when you want to create a new VLAN, you can simply click on the Create VLAN icon(), instead of selecting the **VLAN** menu and then choosing the **Create** item.

Tool Descriptions

VLAN Manager provides the following set of graphical tools. A short description (Tool Tip) of a tool is displayed when the cursor is positioned over a tool icon for one second. Tool Tips can be turned off by deselecting the Tool Tips preference. Refer to [Chapter 5, Managing Preferences](#), for information about setting preferences.



- Exit VLAN Manager



- Create a VLAN



- Delete a VLAN



- Display VLAN details



- Create a switch



- Delete a switch



- Display switch details



- Display Directory information

 - Display Topology View

 - Display Connection Table

 - Display all tapped connections

 - Launch Acrobat Reader to display the SecureFast VLAN Manager User's Guide

Working with Dialog Boxes

VLAN Manager uses dialog windows to request input that it needs before it can carry out a command, to provide status information about a request, or to display detailed information. Some dialog windows contain just text, while others may contain text, text boxes, option buttons and tabbed pages.

When you choose a command that is followed by an ellipsis (...), a dialog window appears to let you select from related options or provide further information. A command with no ellipsis will be executed immediately.

For example, if you choose **Create** from the **Edit >VLAN** menu, the SecureFast VLAN - Create VLAN dialog window is displayed. To create the new VLAN, you enter the name of the new VLAN in the **VLAN Name:** text box, choose properties for the new VLAN, and then click **OK**. In contrast, if you choose **Toggle Open/Secure** from the **Edit >VLAN** menu, the selected VLAN's policy is toggled immediately.



You can turn confirmations off by deselecting Confirmations in the Global preferences box. Refer to [Chapter 5, Managing Preferences](#).

Properties you set using tabbed pages are not applied until you click **OK**.

VLAN Manager uses confirmation boxes, a form of dialog box, to request confirmation before carrying out a request.

For example, if you choose **Exit** from the **File** menu, the VLAN Manager confirmation window is displayed. To exit VLAN Manager, click **OK**. To dismiss the confirmation window and return to the VLAN Manager Main window, click **Cancel**.

Entering Information Text Fields

Text fields may contain text, numbers, or special characters, depending on the type of information being requested. The procedure you use to enter text into a text field varies, depending on whether or not the field already contains information.

- If a text field is empty, click anywhere in the field and then enter the information into the field.
- If the text field already contains information, highlight the text in the field that you want to replace and then enter the new information.

Closing Windows

The way in which you close each type of window is described below.

- **Main** - When you close the VLAN Manager Main window, you close the VLAN Manager client. To close the window, select **Exit** from the **File** menu or click on the Close Window icon from the menu bar. A confirmation box will ask you to verify that you want to exit the VLAN Manager client if the Application Exit preference is set. If this preference is not set, the window will be closed immediately. Refer to [Chapter 5, Managing Preferences](#) for information about how to set preferences.
- **Information** - Select **Close** from the **File** menu or click the **Cancel** button.
- **Dialog** - Select **OK** to accept changes and close the window, **Apply** to accept changes and leave the window open, or **Cancel** to close the window without making changes.
- **View** - Select **Close** from the **File** menu.

VLAN Manager Main Window Panes

The VLAN Manager Main window panes contain icons that represent the logical contents (VLANs, AMR VLANs, and IP Multicast groups) and physical contents (switches, ports, and users) of the current domain that can be administered by SPECTRUM VLAN Manager. The graphical representation of elements and the drag-and-drop features of SPECTRUM VLAN Manager's user interface make VLAN, AMR VLAN, and Multicast Group administration simple.

Logical Window Pane

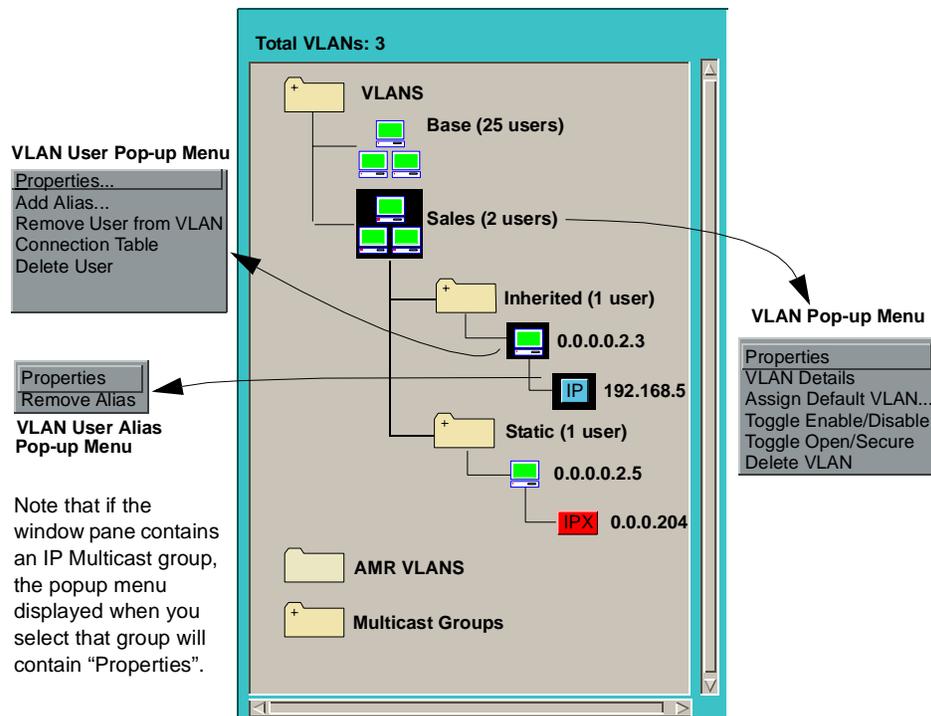
This pane (Figure 3-10) uses folders that represent logical categories of users (e.g., VLANs, AMR VLANs, and IP Multicast groups) in the current domain. Entries are sorted in ascending order.

A “+” is used to indicate whether or not a folder is empty. The presence of a “+” indicates that a folder is not empty. Double-click the folder icon to view the contents of the folder. The absence of a “+” indicates that a folder is empty. Empty folders are a lighter shade of yellow and cannot be expanded.

Folders are also used within a logical category to further define users in that category. For example, within a VLAN, users are categorized in folders according to how they gained membership in the VLAN (e.g., Inherited membership or Static membership).

The **Total VLANs** field displays the total number of configured VLANs (VLANs and AMR VLANs).

Figure 3-10. Logical Window Pane



VLANs

VLANs are sorted alphabetically. Initially, the default VLAN for all ports is the Base VLAN so all users in a domain inherit membership in the Base VLAN. You can think of the Base VLAN as a container that holds endpoints until membership criteria is defined for them. When a user acquires membership in another VLAN, it is automatically removed from the Base VLAN. Similarly, when a user is removed from all non-Base VLANs, it is automatically returned to the Default VLAN for the port. This may or may not be the “Base” VLAN.

Additional VLANs are created using **C**reate from the **E**dit > **V**LAN menu. When a VLAN is created, it is empty. You add members to it by dragging users, access ports, or switches to a VLAN (Static Membership) or by dragging the VLAN to the access port or switch (Inherited Membership). Refer to [Chapter 6, *Managing Domains*](#), for step-by-step instructions about how to create VLANs.

VLAN management tasks are initiated from the **E**dit > **V**LAN menu, the **V**iew > **V**LAN menu, or the VLAN pop-up menus. The VLAN pop-up menus ([Figure 3-10](#)), which are available from the right mouse button when a VLAN, user, or user alias is selected, lets you perform many VLAN and user management tasks. Refer to [Chapter 9, *Managing SecureFast VLANs*](#), for detailed information about managing VLANs and to [Chapter 10, *Managing Users*](#), for detailed information about managing users.

AMR VLANs

Automatic Membership Registration (AMR) dynamically creates VLANs, joins endpoints to those VLANs, and floods packets to those VLANs. Using AMR to create VLANs makes it easy to group all users of a certain type into a single VLAN without having to manually drag and drop users into a VLAN. Refer to *AMR VLAN Administration*, on page 9-19 for detailed information about AMR VLANs.

IP Multicast Groups

IP Multicast groups let you set up unidirectional point-to-multipoint connections. Multicasts are most often used when data from a given source must be distributed simultaneously to several destinations (e.g., sending video to a group or disk mirroring). Multicast packets are distributed through the switch cloud using a packet distribution tree rooted at the sender. Only switches in the tree for a particular call get involved with connection setup for that call. The packet distribution tree can add branches without changing the rest of the tree when new receivers join. Refer to [Chapter 12, *Managing IP Multicast Groups*](#) for detailed information about IP Multicast Groups.

Graphical Icons

Graphical icons identify the various logical window pane elements.

Folder Icons ( ) - Used to represent logical groups of users (e.g., VLANs, AMR VLANs, and Multicast Groups) in the current domain. Also used within a logical group to categorize users as shown below.

- **VLANs** - Inherited or Static
- **AMR VLANs** - Automatic (Learned) or Static
- **Multicast Groups** - Senders or Receivers

The “+” inside a folder icon () indicates that the folder is not empty and can be expanded. A folder icon that does not contain a “+” () is empty and cannot be expanded.

VLAN Icon () - Precedes the VLAN name. The number of users in a VLAN is shown in parentheses to the right of the VLAN name. Double-clicking on a VLAN icon alternately collapses and expands the VLAN tree. Use the right mouse button to select and execute operations that can be performed on this icon. Refer to [Operational Status](#), on page 3-29, for more information about status colors.

AMR VLAN Icon () - Precedes the AMR VLAN name. The number of users in an AMR VLAN is shown in parentheses to the right of the AMR VLAN name. Double-clicking on an AMR VLAN icon alternately collapses and expands the AMR VLAN tree. Use the right mouse button to select and execute operations that can be performed on this icon. Refer to [Operational Status](#), on page 3-29, for more information about status colors. For information about AMR VLANs, refer to [AMR VLAN Administration](#), on page 9-19.

Multicast Group Icon () - Precedes the group name. The number of users in a group is shown in parentheses to the right of the group name. Double-clicking on a group icon alternately collapses and expands the group tree. Use the right mouse button to select and execute operations that can be performed on this icon. Refer to [Operational Status](#), on page 3-29, for more information about status colors. For information about Multicast Groups, refer to [Chapter 12, Managing IP Multicast Groups](#).

User Icon () - Indicates an instance of a physical address. The user’s name is displayed to the right of the user’s MAC address, if there is one. Associated network address icons are displayed under the MAC address. Use the right mouse button to select and execute operations that can be performed on this icon. Double-clicking on a user icon alternately collapses and expands the network aliases for the user.

Network Alias Icon () - Indicates an instance of one or more network alias addresses such as IP (), IPX (), AppleTalk (), NetBios (), or () DHCP which is associated with a physical address. The network alias address is displayed to the right of the icon. If the name associated with a network address can be resolved, it will appear next to the network address.



DHCP (Dynamic Host Control Protocol) icons represent users that have acquired an IP address from a DHCP server. IP addresses acquired in this manner generally have a lease associated with them. The terms of the lease determine how long the user can keep the IP address, although a user can extend the lease.

You can remove a network alias by selecting the alias you want to delete and then clicking the right mouse button. If confirmations are ON, you will be asked to verify that you want to remove the alias before it is removed. If confirmations are OFF, no verification is requested. Refer to [Chapter 5, Managing Preferences](#), for information about setting preferences. You can also add a network alias. Refer to [Chapter 10, Managing Users](#).

Key Icon () - Indicates that the selected VLAN is running in SECURE mode. The Key Icon is displayed to the right of the VLAN icon.

Physical Window Pane

This pane ([Figure 3-10](#)) uses icons to represent the all chassis, switches, ports, and users discovered in the current domain by the VLAN Manager ([Figure 3-11](#)).

When fully collapsed, the pane displays only chassis icons. You double-click a chassis icon to view its contents. Double-clicking down through the chassis, switch, and port icons, progressively exposes more detail about the domain.

This area contains It also displays the total number of switches discovered in the **Total Switches** field.

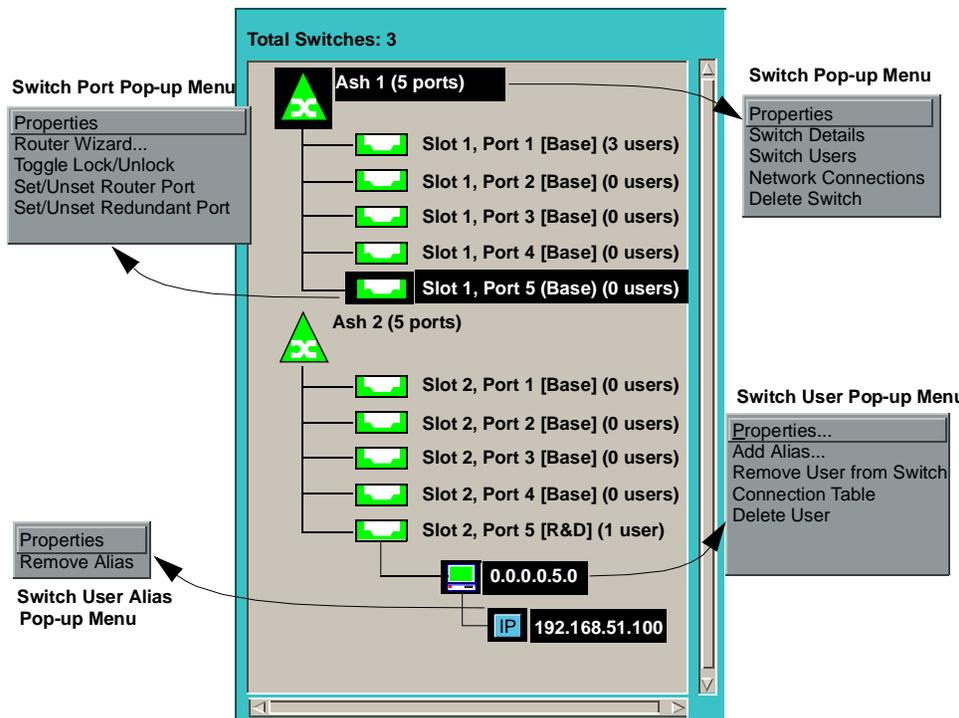
Chassis, switches, ports, and users are automatically discovered by the seed switch when you choose the **Discover** command from the **Domain** menu or when you press the **Discover** button while using the wizard. Refer to [Chapter 6, Managing Domains](#), for step-by-step instructions about how to discover switches.

The switches in the physical pane can be sorted by name or by IP address on a per chassis basis. The way in which the switches are sorted is determined by the **Switch Sort** preference. The default is sort by name. For information about how to set the **Switch Sort** preference, refer to [Chapter 5, Managing Preferences](#).

Switch management tasks are initiated from the **Edit >Switch** menu, the **View >Switch** menu, or the switches pop-up menus. The switches pop-up menus ([Figure 3-11](#)) are available from the right mouse button when a switch, port, user, or user alias is selected.

These menus let you perform many switch and user management tasks. Refer to [Chapter 7, Managing Switches](#), for detailed information about managing switches and to [Chapter 10, Managing Users](#), for detailed information about managing users.

Figure 3-11. Physical Window Pane



Graphical Icons

Graphical icons identify the various Switches window pane elements.

Chassis Icon () - Precedes the chassis name. The number of slots is displayed in parentheses to the right of the chassis name. Double-clicking a chassis icon alternately expands and collapses the chassis's switch hierarchy. Use the right mouse button to select and execute operations that can be performed on this icon.

Color is used to indicate the operational status of a chassis. Refer to [Operational Status](#), on page 3-29, for more information about status colors.

Switch Icon () - Precedes the switch name. The number of ports is displayed in parentheses to the right of the switch name. Double-clicking a switch icon alternately expands and collapses the switch's port hierarchy. Use the right mouse button to select and execute operations that can be performed on this icon.

Color is used to indicate the operational status of a switch. Refer to [Operational Status](#), on page 3-29, for more information about status colors.

Access Port Icons (  ) - Identifies the port as an access port.  is used to represent a normal access port.  and  are used to represent the mode a port is in when redundant access ports are configured for a single user. Refer to [Redundant Access](#), on page 8-25. The icon precedes the port label. You can change the label of an access port from the default label (Slot x, Port x) to any name that is meaningful to you via port properties. The default VLAN for the port is shown in square brackets to the right of the port label. Access ports are entry points into the switch network.

Double-clicking an access port icon alternately expands and collapses the port's user hierarchy. Use the right mouse button to select and execute operations that can be performed on this icon.

Color is used to indicate the status of a port. Refer to [Operational Status](#), on page 3-29, for more information about status colors.

Router Port Icon () - Identifies the port as a router port. The icon precedes the port label. Use the right mouse button to select and execute operations that can be performed on this icon. Color is used to indicate the status of a port. Refer to [Operational Status](#), on page 3-29, for more information about status colors.

Network Port Icon () - Identifies the port as a switch-to-switch link. (Network ports cannot be dragged; they belong to all VLANs.)

ATM Port Icon () - A port that has joined an ELAN. The icon precedes the port name. The name of an ATM port can be changed from the default name (ELAN) to any name that is meaningful to you. The default VLAN for the port is shown to the right of the port name. Use the right mouse button to select and execute operations that can be performed on this icon. Color is used to indicate the status of a port. Refer to [Operational Status](#), on page 3-29, for more information about status colors.

INB Port Icon () - The Internal Network Bus (INB) icon identifies the port as the connection to the backplane of a chassis. INB ports cannot be used to perform statistics and control tasks. (INB ports cannot be dragged; they belong to all VLANs since they are a type of Network port.)

Lock Icon () - Indicates that the default VLAN for the selected port is LOCKED to the port and no static membership to other VLANs will be honored. The Lock icon is displayed to the right of the Port icon.

User Icon () - Indicates an instance of a physical address. The user's name is displayed to the right of the user's MAC address, if there is one. Associated network address icons are displayed under the MAC address. Use the right mouse button to select and execute operations that can be performed on this icon.

Network Alias Icon () - Indicates an instance of one or more network alias addresses, such as IP (), IPX (), AppleTalk (), NetBios (), or (), which is associated with a physical address. The network alias address is displayed to the right of the icon. If the name associated with a network address can be resolved, it will appear next to the network address.



DHCP (Dynamic Host Control Protocol) icons represent users that have acquired an IP address from a DHCP server. IP addresses acquired in this manner generally have a lease associated with them. The terms of the lease determine how long the user can keep the IP address. Refer to [Appendix B, *SecureFast DHCP Relay Agent*](#) for more information about DHCP.

You can remove a network alias by selecting the alias you want to delete and then clicking the right mouse button. If confirmations are ON, you will be asked to verify that you want to remove the alias before it is removed. If confirmations are OFF, no verification is requested. Refer to [Chapter 5, *Managing Preferences*](#), for information about setting preferences.

Scroll Bars

Some areas of the VLAN Manager window and some dialog boxes contain more information than will fit in an area; scroll bars are provided in these instances. The scroll bar consists of a scroll box and scroll arrows. You drag the scroll box up and down or side-to-side to scroll through all the information in an area. You can also use the scroll arrows to scroll through the information.

Working With Icons

You can perform many VLAN administrative tasks by selecting icons from one side of the VLAN Manager Main window and then dragging them to and dropping them in the other side of the window. This section describes how to select icons, expand and collapse icons, and drag and drop icons.

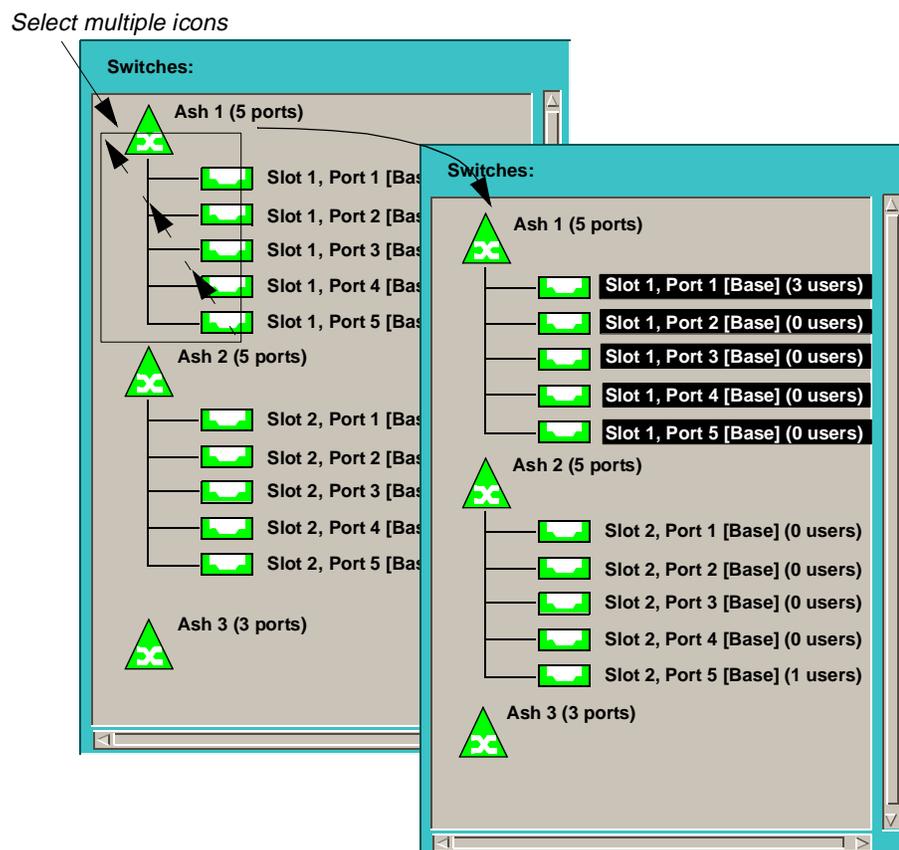
Selecting Icons

You must select the icon that represents an element (VLAN, switch, port, user, or alias) before you can perform any administrative tasks on the element. To select an icon, click on the icon or name associated with the element using the left mouse button.

To select two or more icons, press the “Control” key and click on the icons you want to select. Non-selectable icons such as INB, Host or Network will not be selected.

If the icons are adjacent, you can also use the “rubber band” technique. Place the cursor near one of the icons, click and hold the left mouse button, drag the cursor over the other icons you want to select, and then release the button (Figure 3-12).

Figure 3-12. Selecting Multiple Icons



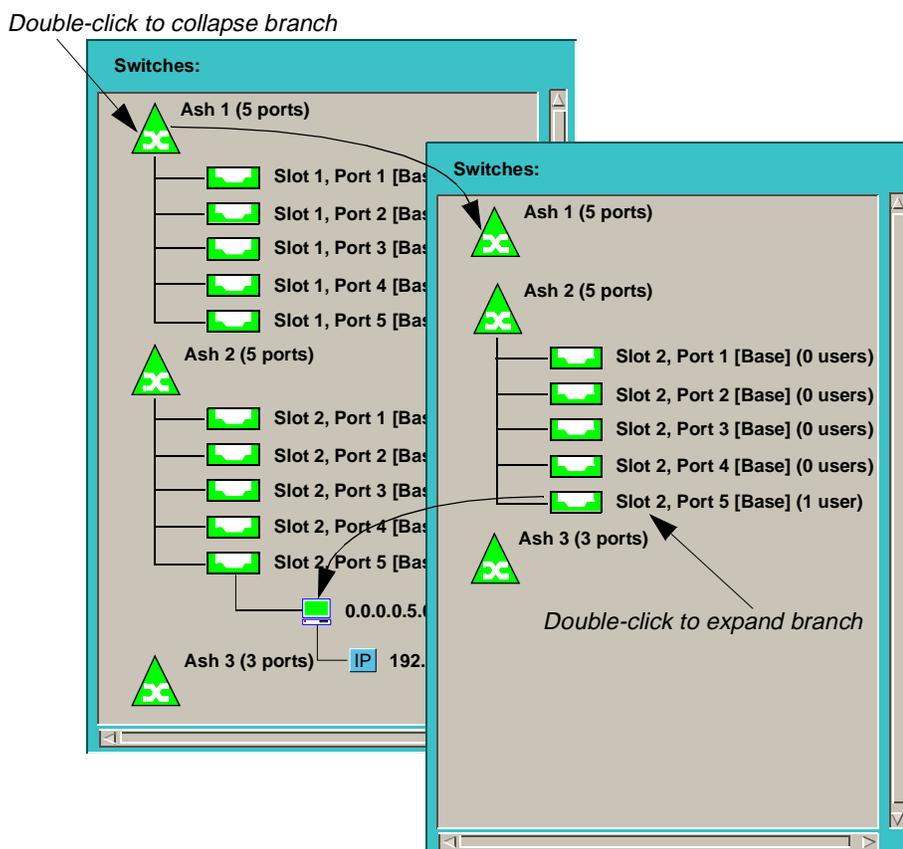
Expanding and Collapsing Icons

Expanding and collapsing icons allows you to control the level of information being displayed in the VLANs and Switches window panes. The level at which icons are displayed is controlled by expanding or collapsing the various icons (Figure 3-13). When an icon is expanded, all of its sub-icons are displayed. When collapsed, its sub-icons are not displayed.

When an icon is expanded, its sub-icons are displayed in the same state they were in the last time the icon was collapsed. For example, let's say that Ash 2 is expanded to show all of its ports with Port 5 expanded to show all of its users. If Ash 2 collapsed and then expanded, Ash 2 would still show all of its ports and Port 5 would show its users.

To expand or collapse an icon, double-click on the name or icon associated with an element.

Figure 3-13. Expanding and Collapsing Icons



Dragging and Dropping Icons

Dragging and dropping is used to establish user membership in VLANs.

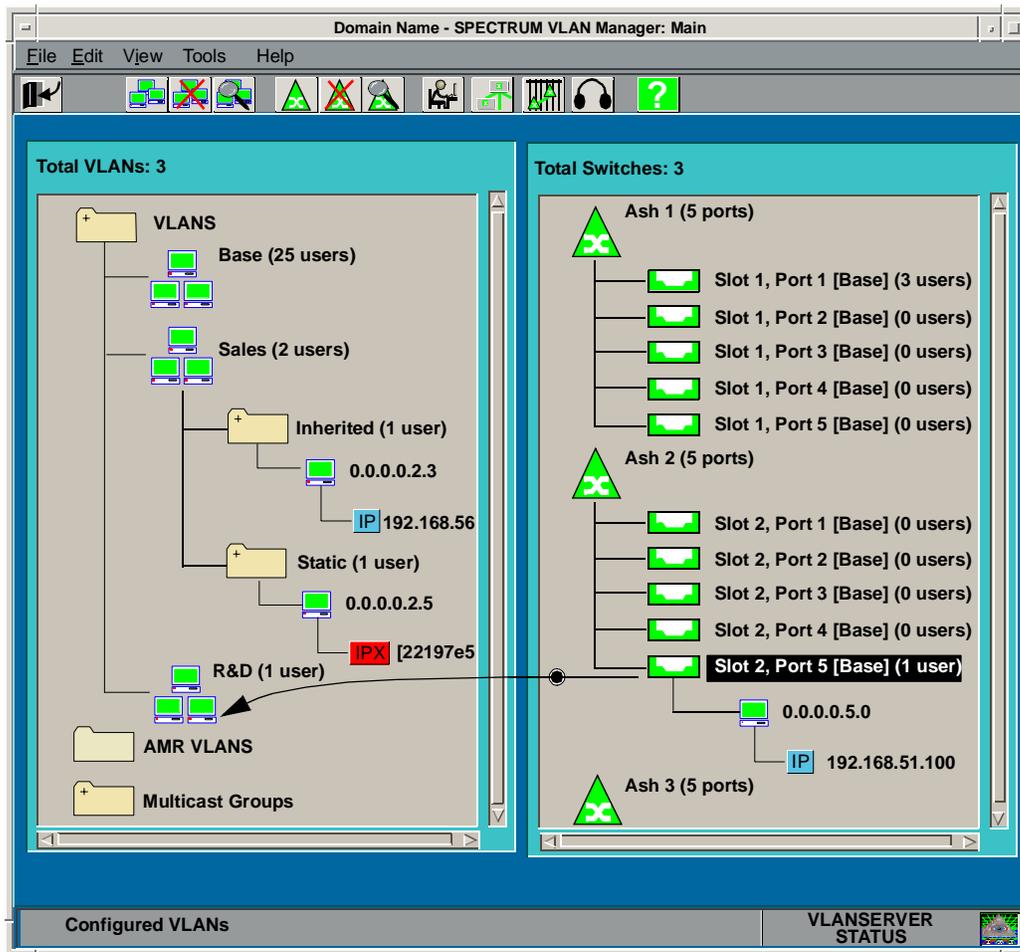
To add users to a VLAN:

1. Select the switches, ports, or users you want to have belong to a particular VLAN. (Selected icons are highlighted on the screen.)
2. Click and hold anywhere in the highlighted area, drag the cursor over the VLAN icon you want the highlighted icons to populate, and then release the mouse button (Figure 3-14). (The cursor shape changes into a  as you drag icons from one area to the other and into a  when it is located over a VLAN that can be populated.)



Network and INB ports cannot be dragged.

Figure 3-14. Dragging and Dropping



Status Bar

Error or cursor location status information is displayed in a two-line status bar located in the bottom left of the VLAN Manager Main window.

The first line displays error information. For example, the message “Network Port Cannot be Selected In This View” is displayed if you try to select a network port from the switches pane.

The second line displays cursor location information. For example, the message “Configured VLANs” is displayed if the cursor is moved into the logical pane. Likewise, “Display Network Directory” is displayed if the cursor is moved over the  tool.

Operational Status

Color is used to indicate the operational status of the VLANServer, switches, ports, users, and links. Pipes, which represent one or more links between switches, also use color to indicate operational status. Refer to [Chapter 13, Viewing Domain Topologies and Managing Switch Links](#) for information about pipe status.

Status colors and descriptions are shown below and are all inclusive unless otherwise noted.

Table 3-1. Operational Status

Color	Description
Green	(All except ports) Up - Contact has been established. (Port) A link has been detected.
Red	(Used for the VLANServer, switches, and links) Down - Contact has been lost. Not pingable.
Orange	(Used for the VLANServer and switches) Contact has been lost. Pingable but not responding to SNMP.
Gray	(Used for the VLANServer, users, switches, and links) (All except users) Unknown - Cannot be reached due to a known error condition that exists. (User) Has been deleted from switch but still exists in the VLANServer database.
Blue	(Used for the VLANServer and ports) (VLANServer) Initial - Contact has not yet been established. (Port) A link has not yet been detected.
Yellow	(Used for switches) Two or more switches have the same IP address, or two IP addresses are associated with the same switch. (Used for switch ports to indicate user or port restriction violations.)

Managing Security

This chapter provides step-by-step instructions for controlling access to the VLANServer using SPECTRUM VLAN Manager's graphical user interface.

Overview

The VLAN Manager Security feature lets you control which users have access to the VLANServer and may use the VLAN Client, from what hosts a user can connect to the VLANServer, and what level of access each user has to the VLANServer.

Access to the VLANServer is only permitted if the user is listed on the **Users** list *and* the host from which the user is connecting to the VLANServer is on the **Hosts** list.

The level of access a user has is determined by the permissions assigned to a user (Read Only or Read/Write). Users with Read/Write privileges have full privileges, including the privilege to add and delete users, configure VLANs, and stop the VLANServer. Users with Read Only privileges have limited privileges. Menu selections and Toolbar buttons not available to Read Only users are not shown. Also, if a user with Read Only privileges tries to perform an operation that is not allowed (e.g., dragging a user from a switch port to a VLAN), an error message will be displayed.



When a user with Read Only permissions displays a view containing a community name, each character in the community name is overwritten with an "*" character.

Configuring Security

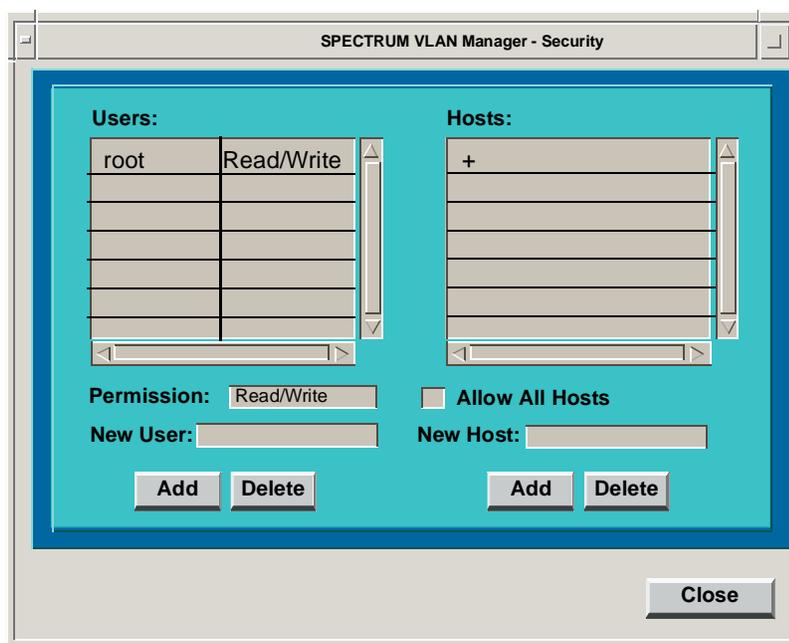
You use the Security window ([Figure 4-1](#)) to set access privileges to the VLAN Server for users and hosts. The Security window is divided into a **Users** side and a **Hosts** side. The **Users** side lets you add and delete users to the **Users** list as well as set permissions for each user in the list. It consists of a **Users** list, which shows a list of users and associated permissions, a **Permission** field, a **New User** field, and **Add** and **Delete** buttons.

The Hosts side lets you add and delete hosts to the **Hosts** list. It consists of a **Hosts** list, an **Allow All Hosts** field, a **New Host** field, and **Add** and **Delete** buttons.

Clicking the **Close** button accepts changes and then closes the window.

As shown in [Figure 4-1](#), the user specified during the installation (e.g., root or Administrator) is allowed Read/Write access to the VLANServer from any host. The **Users** area only contains one entry, “root” which limits access to only the “root” user. The **Hosts** area also contains one entry: “+”. The “+” sign is a UNIX convention which allows access by all hosts.

Figure 4-1. Security Window



Adding a User

To add a user:



Care should be taken when adding users to the Users list. All users on the list with Read/Write permissions have full privileges, including the privilege to add and delete users, configure VLANs, and stop the VLANServer.

1. Select **Security** from the **File** menu to display the SPECTRUM VLAN Manager’s Security window ([Figure 4-1](#)). You must have Read/Write permissions to display the Security window.

2. Enter the name of the user to be added into the **New User** field and then click the **Add** button associated with adding a new user. The new user is added to the **Users** list.



The default permissions for a new user is Read/Write. To change permissions for a user, you must delete the user and then add the user again with the new permissions.

Adding a Host

To add a host:

1. Select **Security** from the **File** menu to display the SPECTRUM VLAN Manager's Security window (Figure 4-1). You must have Read/Write permissions to display the Security window.
2. Enter the name of the host system to be added into the **New Host** field and then click the **Add** button associated with adding a new host. The new host is added to the **Hosts** list. To allow all hosts, click **Allow All Hosts**.



Entries in the Hosts list can be DNS/NIS hostnames or IP addresses.

Deleting a User or Host

To delete a user or host:



The user currently running the VLAN client cannot be deleted.

1. Select **Security** from the **File** menu to display the SPECTRUM VLAN Manager's Security window. You must have Read/Write permissions to display the Security window.
2. Click on the user or host you want to delete, and then click the corresponding **Delete** button to delete the user or host. You cannot delete your own user model or the last host.

Managing Preferences

This chapter provides step-by-step instructions for setting preferences using SPECTRUM VLAN Manager's graphical user interface.

Overview

Setting **Preferences** lets you customize the look and feel of VLAN Manager windows. You do this by modifying a window's display characteristics. Preferences are grouped into five types: **Global** (Figure 5-1), **Main** (Figure 5-2), **Topology View** (Figure 5-3), **Path Trace** (Figure 5-4), and **Connection Table** (Figure 5-5). You can set preferences from the VLAN Manager's Main window or from the particular window type you want to set (i.e., Topology preferences can be set from the Topology View; Connection Table preferences can be set from the Connection Table).



Preferences are unique to each workstation running the VLAN client.

Global Preferences

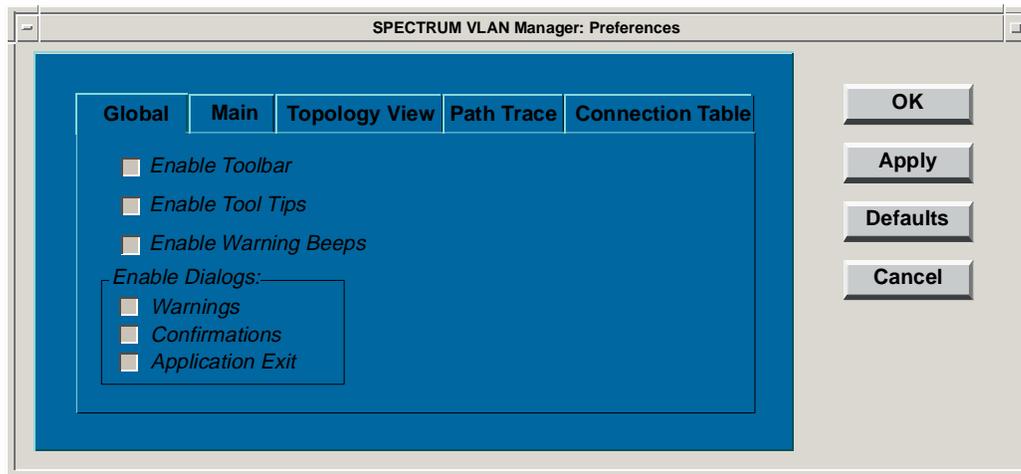
As the name implies, Global Preferences are applied to all VLAN Manager windows. These preferences allow you to enable or disable certain user aids such as the Toolbar. A preference is enabled when its corresponding preference button is recessed (down). You set Global preferences from the SPECTRUM VLAN Manager Main window.

Global Preferences are:

- **Enable Toolbar** - Display graphical toolbar.
- **Enable Tool Tips** - When the cursor is positioned over an icon for a short time, display a one or two word description of the selected toolbar icon.

- **Enable Warning Beeps** - Audible alert sounds as a reminder to look at the Status Bar at the bottom of the Main window.
- **Enable Dialogs** - Text messages are displayed for the selected type of dialog soliciting confirmation before performing an operation or indicating the successful or unsuccessful completion of an operation (e.g., warnings, confirmations, and application exit).

Figure 5-1. Global Preferences



To set global preferences:

1. Choose **Preferences** from the **File** menu in the VLAN Manager Main window.
2. Click the **Global** tab to display global preferences.
3. Click the preference button next to each preference that you want to enable. Preferences are enabled when the button is recessed, disabled when the button is raised.

Click another preference tab to set additional preferences, **OK** to set preferences and dismiss window, **Apply** to set preferences and retain the window, **Defaults** to set preferences to the default settings, or **Cancel** to dismiss the SPECTRUM VLAN Manager's Preferences window without making preference changes.

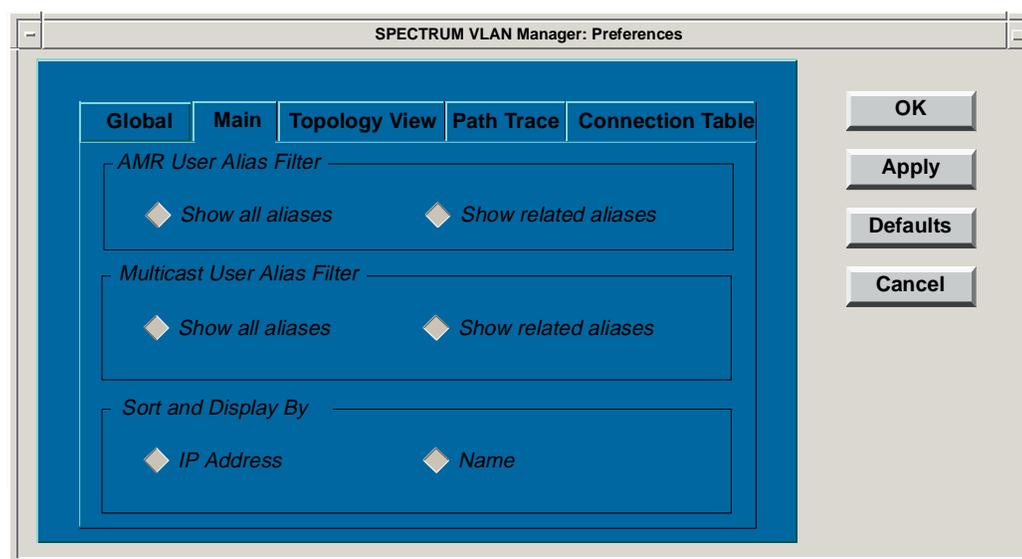
Main Preferences

Main Preferences are applied to AMR VLANs, to Multicast groups, and to the VLAN Manager Main window physical pane. A preference is enabled when its corresponding preference button is recessed (down). For detailed information about AMR VLANs, refer to *AMR VLAN Administration*, on page 9-19. For detailed information about IP Multicast, refer to [Chapter 12, *Managing IP Multicast Groups*](#). You set Main preferences from the SPECTRUM VLAN Manager Main window.

Main Preferences are:

- **AMR User Alias Filter** - Filters AMR user aliases in the Main VLAN Manager window based on AMR type, IP-Subnet, NetBIOS, or IPX RIP Only user aliases that match the criteria for the VLAN are displayed. For instance, if a user has two aliases, say NetBIOS and IPX, only the NetBIOS alias would be displayed for that user in the NetBIOS AMR VLAN. Likewise, only the IPX alias for that user would be displayed in the IPX AMR VLAN. Similarly, if a user has two IP aliases, say 192.168.107.61 and 1.1.1.1, only the 192.168.107.61 alias would be displayed for the 192.168.107.0 subnet.
- **Multicast User Alias Filter** - Filters IP Multicast user aliases in the Main VLAN Manager window. Only IP user aliases are displayed.
- **Switch Sort** - Arranges switch icons in the VLAN Manager Main window physical pane by name in alphabetical order or by IP address in ascending order.

Figure 5-2. Main Preferences



To set Main preferences:

1. Choose **Preferences** from the **File** menu in the VLAN Manager Main window.
2. Click the **Main** tab to display Main preferences.
3. Click the preference button next to each preference that you want to enable. Preferences are enabled when the button is recessed, disabled when the button is raised.
4. Click another preference tab to set additional preferences, **OK** to set preferences and dismiss window, **Apply** to set preferences and retain the window, **Defaults** to set preferences to the default settings, or **Cancel** to dismiss the SPECTRUM VLAN Manager's Preferences window without making preference changes.

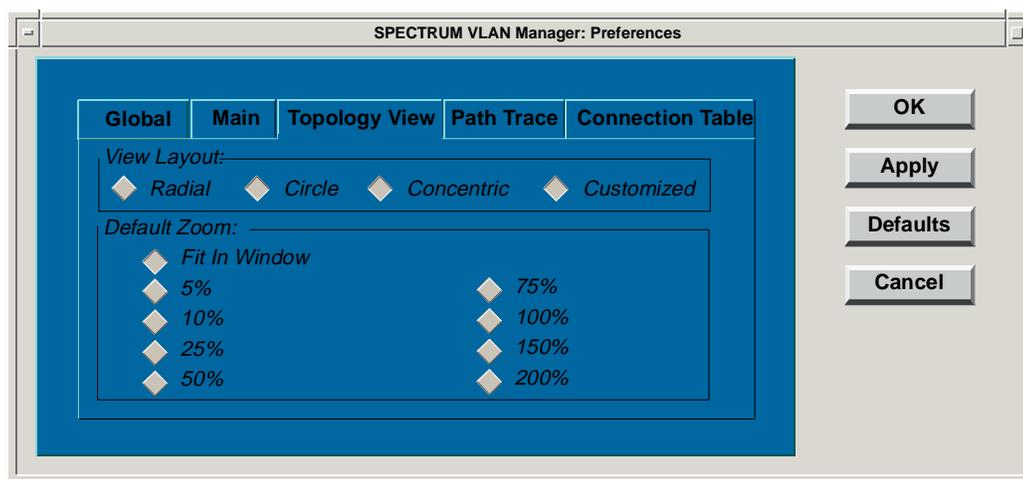
Topology View Preferences

Topology View preferences (Figure 5-3) are applied to icons present in the topology view. These preferences let you select how icons are arranged and how icon size in the view is determined. You set Topology View preferences from the SecureFast VLAN Main window or from the Topology View window.

Topology View Preferences are:

- **View Layout** - Display icons using a **Radial**, **Circle**, **Concentric**, or **Customized** arrangement. **Radial** places the switch with the greatest number of links in the center of the display with the other switches grouped around it. **Circle** (Figure 13-6) displays all switches in a circular arrangement. **Concentric** (Figure 13-7) displays all switches in a concentric arrangement. **Customized** displays all switches in the last saved customized arrangement.
- **Default Zoom** - Proportionally increase or decrease the size of the icons in the topology view to the percentage specified. **Fit in Window** will zoom the icons to the largest percentage that still allows all icons to be displayed in the view.

Figure 5-3. Topology View Preferences



To set Topology View preferences:

1. Choose **File ? Preferences** from the VLAN Manager Main window or from the Topology View window.
2. Click the **Topology View** tab to display topology view preferences.
3. Click the preference button next to each preference you want to enable. Preferences are enabled when the button is recessed, disabled when the button is raised.
4. Click **OK** to set preferences and dismiss the window, **Apply** to set preferences and retain the window, **Defaults** to set preferences to the default settings, or **Cancel** to dismiss the SPECTRUM VLAN Manager's Preferences window without making preference changes.

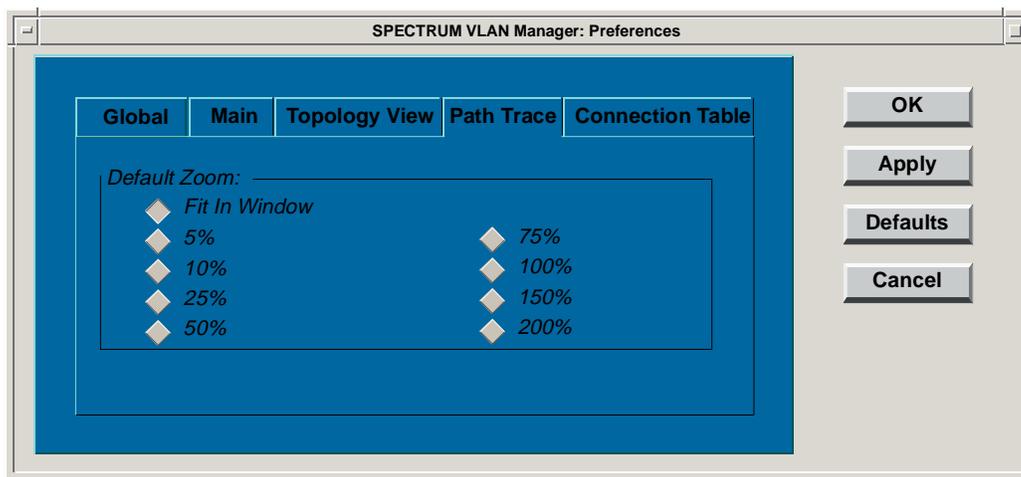
Path Trace Preferences

Path Trace preferences (Figure 5-4) are applied to icons present in the path trace view. These preferences let you select how icon size in the view is determined. You set Path Trace preferences from the SPECTRUM VLAN Manager Main window or from the Path Trace window.

Path Trace Preferences are:

- **Default Zoom** - Proportionally increase or decrease the size of the icons in the path trace view to the percentage specified. **Fit in Window** will zoom the icons to the largest percentage that still allows all icons to be displayed in the view. The default setting is 100%.

Figure 5-4. Path Trace Preferences



To set Path Trace preferences:

1. Choose **File ? Preferences** from the VLAN Manager Main window or from the Path Trace window.
2. Click the **Path Trace** tab to display topology view preferences.
3. Click the preference button next to each preference you want to enable. Preferences are enabled when the button is recessed, disabled when the button is raised.
4. Click **OK** to set preferences and dismiss the window, **Apply** to set preferences and retain the window, **Defaults** to set preferences to the default settings, or **Cancel** to dismiss the SPECTRUM VLAN Manager's Preferences window without making preference changes.

Connection Table Preferences

These preferences (Figure 5-5) let you select what type of information will be displayed in the Connection Table's Source and Destination fields and how much router connection information will be displayed in the Connection Table. You set Connection Table preferences from the VLAN Manager Main window or from the Connection Table window.

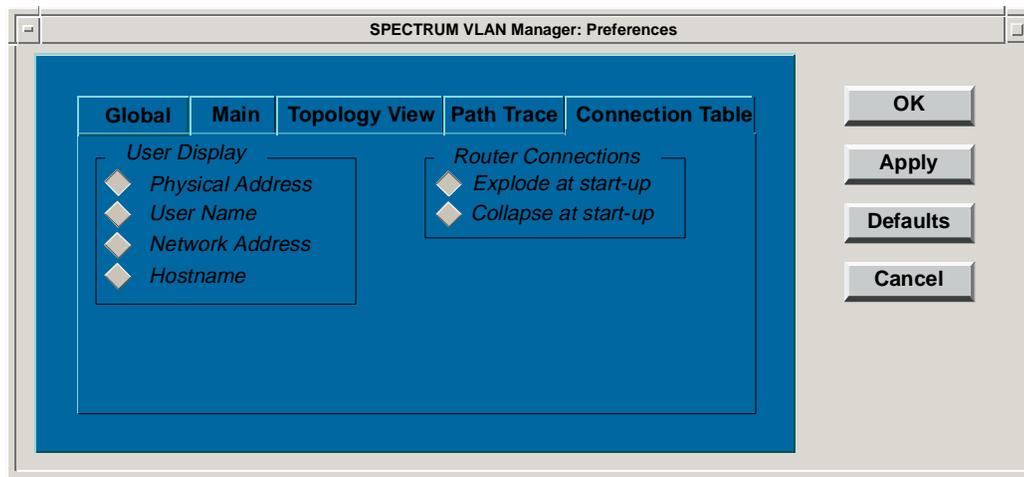
Connection Table Preferences are:

- **User Display** - Lets you select how Source and Destination information is displayed in the Connection Table. If **Physical Address** is selected, these fields contain MAC addresses. If **User Name** is selected, these fields contain user names. If **Network**

Address is selected, these fields contain network addresses. If **Hostname** is selected, these fields contain host names.

- **Router Connections** - If **Collapse at start-up** is selected, router connections will only show router information. “COLLAPSED” is displayed to indicate that information about connections other than the router are not being displayed. If **Explode at start-up** is selected, information about all connections to a router will be displayed.

Figure 5-5. Connection Table Preferences



To set connection table preferences:

1. Choose **File ? Preferences** from the VLAN Manager Main window or the Connection Table.
2. Click the **Connection Table** tab to display Connection Table preferences.
3. Click the preference button next to each preference you want to enable. Preferences are enabled when the button is recessed, disabled when the button is raised.
4. Click another preference tab to set additional preferences, **OK** to apply preferences and dismiss the window, **Apply** to apply preferences and retain the window, **Defaults** to set preferences to the default settings, or **Cancel** to dismiss the SPECTRUM VLAN Manager's Preferences window without making preference changes.

Managing Domains

This chapter provides step-by-step instructions for performing domain administration tasks using SPECTRUM VLAN Manager's graphical user interface. It also contains reference information and helpful tips to help you to perform these tasks.

Overview

VLAN domains are established on the basis of your network configuration. Each group of interconnected SecureFast VLAN switches and endpoints bounded by a router constitutes a VLAN domain. Each domain is named during the domain creation process. The seed switch for the domain is also identified during this process. A seed switch is used to discover all other switches within a particular domain.

You can use the VLAN Manager user interface to open any domain known to SPECTRUM VLAN Manager. This is particularly useful if you are managing multiple domains. In addition, you can configure, delete, and discover the topology of any domain known to VLAN Manager.

The VLAN Manager's flexibility allows you to perform many of the domain maintenance tasks using the VLAN Manager Discovery Wizard or other selections from the **Domain** menu. Ordinarily, you use the wizard the first time you start the VLAN Manager to create and discover domains. Later, you use the other **Domain** menu selections to perform domain maintenance tasks.

VLAN Manager Domain Discovery Wizard

The VLAN Manager Discovery Wizard is launched automatically the first time VLAN Manager client is started or whenever the database is empty. You can also launch it by selecting the **Wizard** selection from the **File >Domain** menu.

Using this wizard, you can discover a single domain, discover multiple domains, enable IP Multicast, create AMR (Automatic Member Registration) VLANs, and enable DHCP related services. For information about AMR VLANs, refer to *AMR VLAN Administration*, on page 9-19.

A series of steps walks you through the Discovery Wizard process. Each step solicits information required by the wizard. The last step provides you with the opportunity to add, remove, or modify domains that have been configured but not yet discovered, start the discovery process, or cancel the wizard.

Buttons located across the bottom of each wizard window allow you to cancel the wizard, return to the previous window, proceed to the next window, or skip to the last window.

Under certain circumstances, some areas of a window may not be accessible. These areas are grayed-out when such conditions exist.



For Advanced VLAN Policy users: If Advanced VLAN Policy has already been enabled in a domain, and you then delete the domain (or reinitialize the VLANServer database) and rediscover the domain, Advanced VLAN Policy is disabled. You can re-enable it from the VLAN Manager **Tools** menu after rediscovering the domain (see *Launching Advanced VLAN Policy*, on page 15-2).

The steps are as follows:

Step 1

1. Enter the name of the new domain in the text box (Figure 6-1). Domain names can be up to 16 characters in length. Spaces are not allowed in the name.



If you don't want to create a domain at this time, click **Cancel** to terminate the wizard.

Figure 6-1. Wizard - Step 1

2. Select **Next >** to go to the next wizard window, or select **Cancel** to exit the Discovery Wizard.

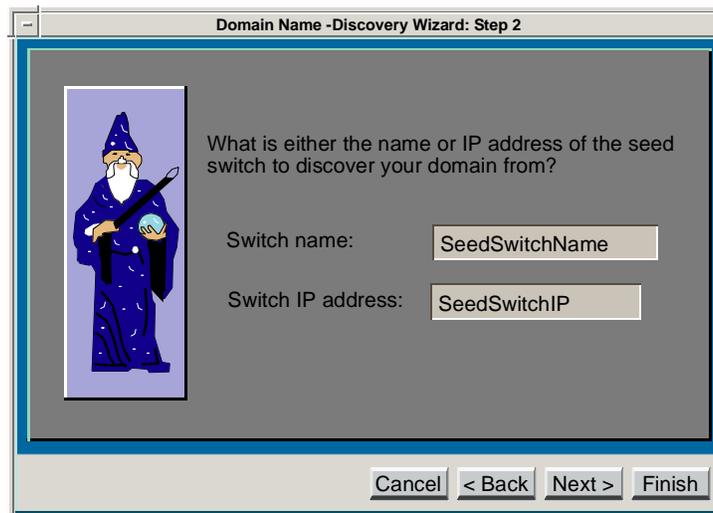
Step 2

1. Enter the name and/or the IP address of the seed switch for this domain. The seed switch is the switch that will be used as a starting point for the discovery process. During the final step of the wizard process, this information is transferred to the VLANServer. The VLANServer initiates contact with the seed switch. Topology information is learned starting with the seed switch's neighbor table and is stored in the VLANServer's database. Seed switch names can be up to 16 characters in length. Spaces are not allowed in the name



If your network does not have a Domain Name Server or there is no DNS entry for your switch, you must complete the Switch IP Address field.

Figure 6-2. Wizard - Step 2



2. Press **Next >** to continue, **< Back** to return to the previous step. Press **Cancel** or **Finish** to display the Discovery Wizard Summary window.

Step 3

1. Enter the community names for the switches in this domain. Community names define security communities to which a user is permitted access and establishes the user's edit privileges within those communities.

Press the **Return** key or click **Add** to add the community name to the list of community names. To remove a community name from the list of community names, click on the name you want to remove and then click **Remove**.

Figure 6-3. Wizard - Step 3



2. Select **Next >** to continue, **< Back** to return to the previous step. Select **Cancel** or **Finish** to display the Discovery Wizard Summary window.



In order to successfully discover and manage a SecureFast VLAN switch, the community name(s) provided in the community name list must match the ReadWrite or Super User community name configured on the SecureFast VLAN switch.

Step 4

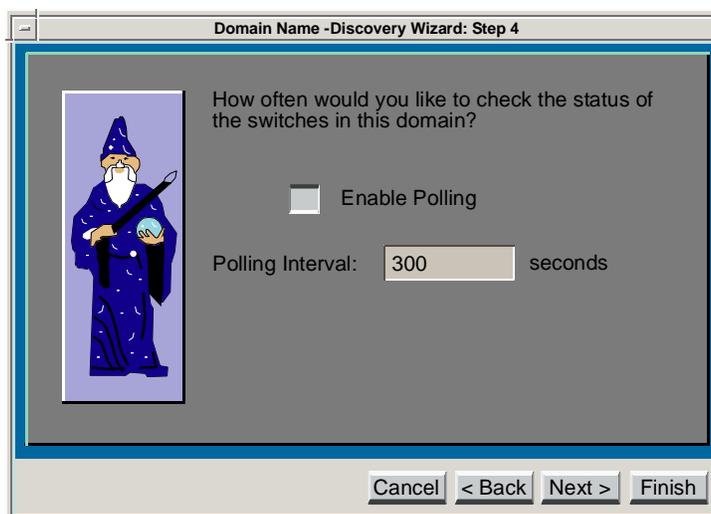
This step allows you to choose how often you want to have the status of the switches in this domain checked and new information read from the switches. If enabled (button recessed), the status of the switches will be checked periodically, based on the time you set in the **Polling Interval** text box.

1. Enter how often (in seconds) you would like the status of the switches in this domain checked in the **Polling Interval** text box. Polling is disabled when the Enable Polling button is raised (up).



The default polling interval is 300 seconds. Large networks may require longer polling intervals. If the polling interval is too small, the VLANServer will not have time to complete polling the network before the next polling cycle begins. If the polling interval is too long, important network events may not be reported in a timely manner.

Figure 6-4. Wizard - Step 4



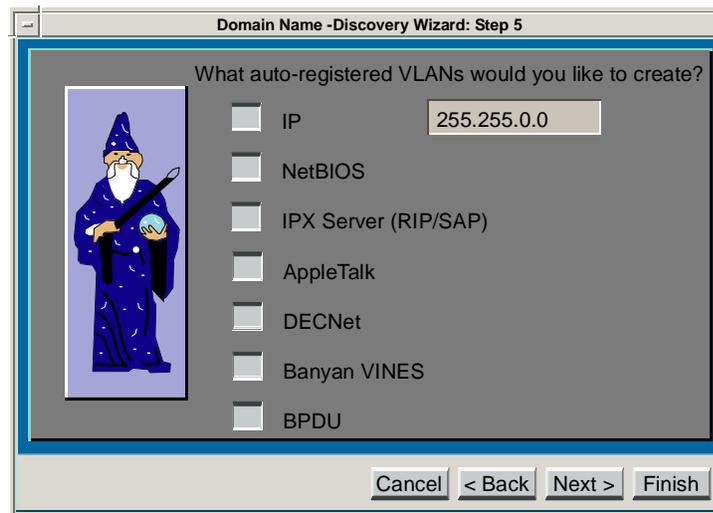
2. Select **Next >** to continue, **< Back** to return to the previous step, **Cancel** to exit the wizard and display the VLAN Manager's Main window, or **Finish** to display the Discovery Wizard's Summary window.

Step 5

This step lets you enable AMR VLANs by type. For detailed information about enabling AMR VLANs, refer to *AMR VLAN Administration*, on page 9-19.

1. Enable AMR VLANs by selecting its corresponding button.

Figure 6-5. Wizard - Step 5



2. Select **< Back** to return to the previous step, **< Next** to proceed to the next step, **Cancel** to exit the wizard and display the VLAN Manager's Main window, or **Finish** to display the Discovery Wizard's Summary window.

Step 6

This step lets you enable or disable IP Multicast for this domain. IP multicast call processing enables you to set up unidirectional point-to-multipoint connections within the domain. Multicasts are most often used when data from a given source must be distributed simultaneously to several destinations (e.g., sending video to a group or disk mirroring). For more information about IP multicast, refer to *Editing IP Multicast Port Properties*, on page 12-7.

If IP Multicast is enabled, the options to enable or disable Multicast scoping and Multicast Optimization become available.

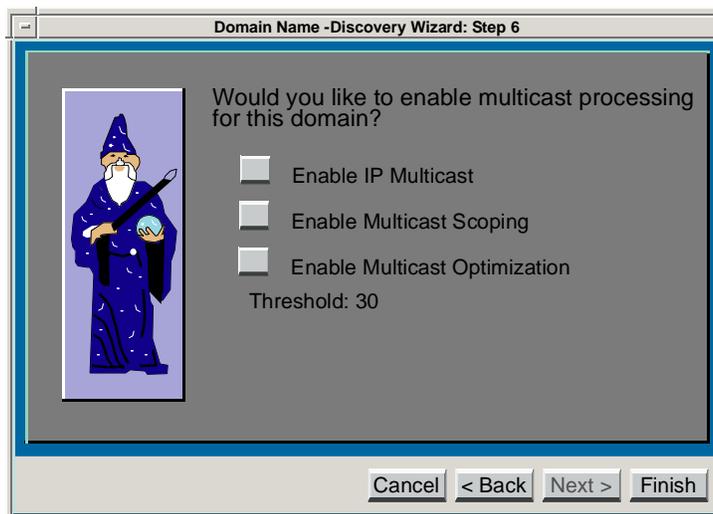
1. Enable (recessed button) or disable (raised button) IP Multicast by selecting or deselecting the corresponding button.
 - **Enable IP Multicast** - Enables or disables IP multicast call processing for this domain. If you enable this option, Enable Multicast Scoping and Multicast Optimization become available. The default is 'Disable'.
2. If you enabled IP Multicast, enable or disable Multicast Scoping and/or Multicast Optimization.
 - **Enable Multicast Scoping** - If this option is enabled, IP multicast traffic is flooded out ports with the same inherited VLAN. If it is disabled, IP multicast traffic is flooded out all ports regardless of VLAN membership. The default is 'Disabled.'

- **Enable Multicast Optimization** - If this option is enabled, you can limit the number of multicast packets by setting a Threshold value.
 - **Threshold** - Limits the number of multicast packets on any switch(es) to this number or fewer. The default is 30 packets per second, but you can change it to any integer value from 1 to 500.



You can use the IP Sender Info Base Element Manager Tool to fine-tune the IP Multicast Sender configuration. Refer to the *SecureFast Tools Guide*.

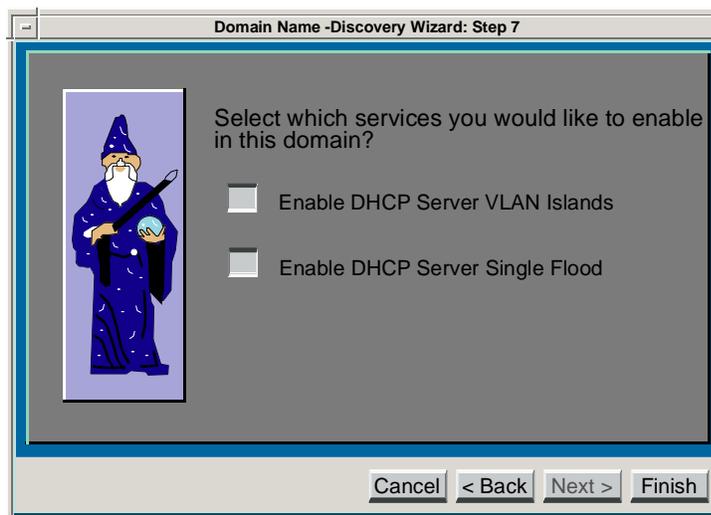
Figure 6-6. Wizard - Step 6



3. Select **< Back** to return to the previous step, **Next >** to proceed, **Cancel** to exit the wizard and display the VLAN Manager's Main window, or **Finish** to display the Summary window.

Step 7

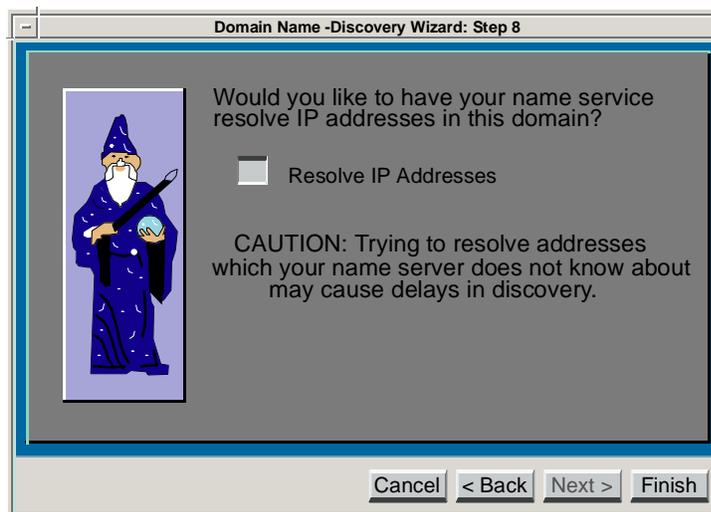
This step allows you to enable DHCP Server VLANs or DHCP Server Single Flood in the domain. See *Services Properties*, on page 6-22 for more information on DHCP Server Islands and DHCP Server Single Flood.

Figure 6-7. Wizard - Step 7

1. Enable/disable DHCP Server VLANs and DHCP Server Single Flood by selecting or deselecting the corresponding button.
2. Select < **Back** to return to the previous step, **Next** > to proceed, **Cancel** to exit the wizard and display the VLAN Manager's Main window, or **Finish** to display the Summary window.

Step 8

1. Enable or disable name service IP address resolution by selecting or deselecting the corresponding button.

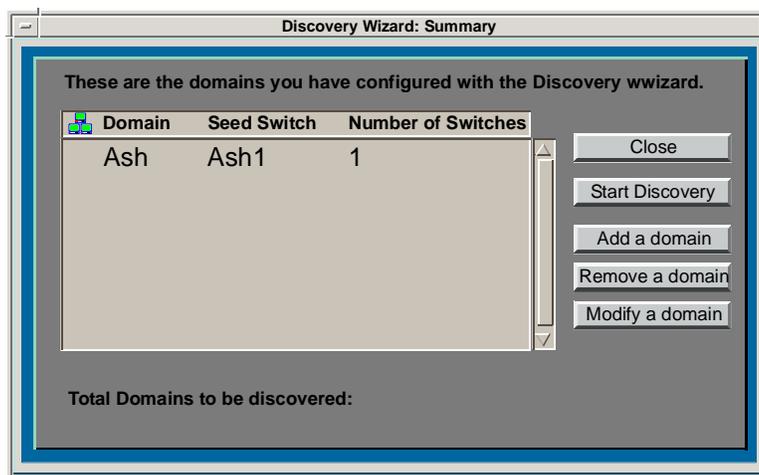
Figure 6-8. Wizard - Step 8

2. Select < **Back** to return to the previous step, **Next** > to proceed, **Cancel** to exit the wizard and display the VLAN Manager's Main window, or **Finish** to display the Summary window.

Summary Window

This window provides configuration information for all domains created during the current wizard session. The window shows the domain name, seed switch, number of switches for each domain, and the total domains to be discovered. Buttons let you add additional domains, remove domains, modify domains, start the discovery process, or cancel the wizard.

Figure 6-9. Wizard - Summary Window



To display the Discovery Error Log, double-click on a domain entry in the Wizard's Summary window. The log lists errors encountered during the discovery process. An empty log indicates that no error occurred during discovery. Refer to [Table 6-1](#) for error code information.

Table 6-1. Discovery Error Log

Error Message	Cause
No switch, check seed switch, and/or community names	Most likely, an incorrect community name. Check spelling. Check whether switch name is incorrect, or the IP address entered is not for the switch but some other device. Check switch name and IP address.
Bad switch, check community names	Incorrect community name. Check spelling.
Duplicate switch	Switch exists in another domain.
Unable to resolve switch name	Switch name is incorrect. Check spelling.

Discovering and Creating VLAN Domains

The **File >Domain >Wizard** and **Discovery**, and **Edit >Domain > Properties** and **Create**, menu selections let you discover, create, and configure VLAN domains. The following chart describes the function of each menu selection. This section provides information about how to use **Discovery**, **Create**, and **Properties**. Refer to [VLAN Manager Domain Discovery Wizard](#), on page 6-1, for information about using the **Wizard**.

Table 6-2. Creating and Discovering VLAN Domains

Menu Selection	Description
Wizard	Walks you through the VLAN domain create, configure, and discover processes. A series of views request information about the domain you want to create. A final view summarizes the domain(s) created and lets you discover, modify, or remove domains created during the current wizard session.
Discovery	Lets you create and discover VLAN domains from a single view.
Properties	Lets you configure VLAN domains after they have been created and/or discovered.
Create	Lets you create and configure VLAN domains without running discovery.

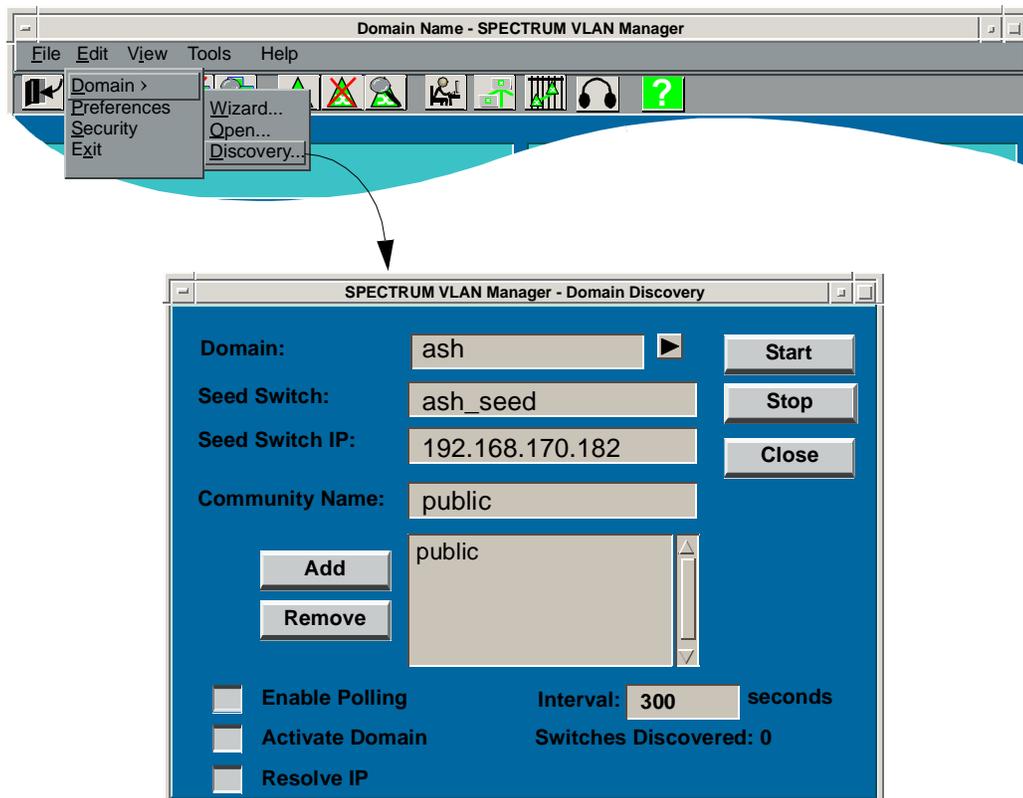
Discovery

VLAN domains can be created, configured, and discovered by running **Discovery** from the **File > Domain** menu. Normally, Discovery only has to be run once, because changes to a domain's topology are discovered automatically, based on the polling interval set in the Discovery dialog box. The only time you would have to run Discovery again would be if the seed switch were unreachable the first time you ran discovery. For example, if a switch were off-line or an incorrect community name were entered, it would be unreachable. After you put the switch on line or put in the correct community name, you would have to run Discovery again.

To use Discovery:

1. Select **Discovery** from the **File > Domain** menu to display the SPECTRUM VLAN Manager - Domain Discovery dialog box (Figure 6-10).

Figure 6-10. Discovering VLAN Domains



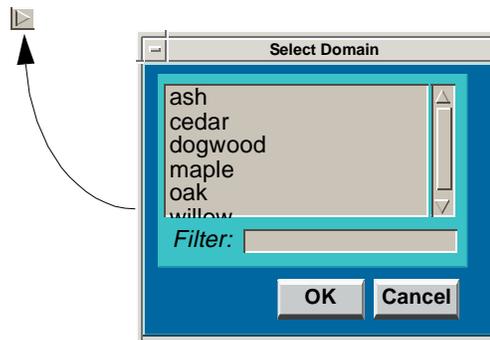
2. Enter the name of the domain you want to create or discover in the **Domain** text box. The  button offers a convenient way to find an existing domain in large networks containing multiple domains. To use this feature:

- a. Click  to display the Select Domain dialog box (Figure 6-11).



In order to successfully discover and manage a SecureFast VLAN switch, the community name(s) provided in the community name list must match the ReadWrite or Super User community name configured on the SecureFast VLAN switch.

Figure 6-11. Discover Select Domain Dialog Box



- b. Click anywhere in the **Filter** text box.
 - c. Enter the name of the domain you want to find. As you type, domain names that don't match the filter criteria will be removed from the domain list. Only the domain names that match your filter criteria will remain.
 - d. Click on the name of a domain, and then click **OK**. The selected domain name is entered into the **Domain Name** text box in the VLAN Manager's Domain Discover dialog box.
3. Enter the name of the seed switch in the **Seed Switch** text box or enter its IP address in the **Seed Switch IP** text box. The seed switch is the switch that VLAN Manager uses to start the discovery process.



If your network does not have a Domain Name Server, you must complete the Switch IP Address field.

Enter the community name(s) for the seed switch and then press return or click **Add** to add the name to the community name list. Once a name is added to the community name list, it is cleared from the **Community Name** text box. Repeat this process until the community name list contains community names for all switches in the domain. The default community name "public" can be removed if it does not apply. Click a community name and then click **Remove** to remove a community name.

Discovery tries each community name listed until it finds one that matches the seed switch's community name. Next, Discovery finds the seed switch's neighbors and tries to contact them using the same community names. If a switch cannot be reached using any of the community names listed, the switch will not be discovered.

4. VLAN Manager will automatically poll your network at a specified interval and add new VLAN switches and users it discovers to your domain. To use this feature, select **Enable Polling** (button recessed), and then enter the poll time, in seconds, in the **Interval** text box. The default setting is 300 seconds.



The default polling interval is 300 seconds. Large networks may require longer polling intervals. If the polling interval is too small, the VLANServer will not have time to complete polling the network before the next polling cycle begins. If the polling interval is too large, important network events may not be reported in a timely manner.

5. Use the **Activate Domain** button when you want to discover multiple domains. The last domain discovered with **Activate Domain** enabled will be displayed in VLAN Manager's Main window when the discovery process is finished.

For example, if your VLAN network has three domains and you discover one of them, without regard to the state of **Activate Domain** (selected/deselected), that domain is displayed in VLAN Manager's Main window. If you then discover another domain with **Activate Domain** selected (button recessed), that domain will be displayed when Discovery has finished. Finally, if you discover the third domain with **Activate Domain** deselected, the second domain discovered will remain displayed, since it was the last to be discovered with **Activate Domain** selected.

6. Use the **IP Resolve** button when you do not want VLAN Manager to perform name resolution for IP users. This expedites discovery in instances where DNS is not configured properly on an NT system.
7. Select the **Start** button. You can stop the discover process at any time by pressing the **Stop** button. Discover will stop as soon as it has finished discovering the ports and users for the switch it is currently analyzing.

Select the **Close** button to close the SPECTRUM VLAN Manager's Domain Discovery dialog box.

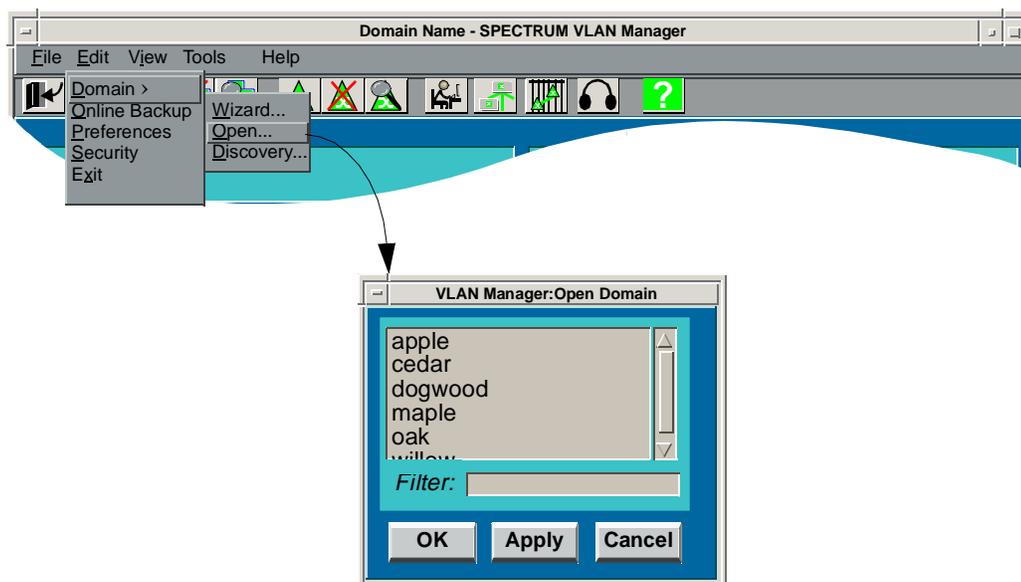
Opening Domains

Opening a domain displays all information about the domain, such as the number of VLANs and switches, and lets you manage all aspects of the domain.

To open domains:

1. Select **Open** from the **File > Domain** menu to display the VLAN Manager's Domain Open dialog box (Figure 6-12).

Figure 6-12. Opening VLAN Domains



2. Click on the name of the domain you want to open.

You can use the **Filter** feature to find a particular domain in large databases containing many domains.

To use the domain filter:

- a. Click anywhere in the **Filter** text box.
- b. Enter the name of the domain you want to find. As you type, domain names that don't match the filter criteria will be removed from the domain list. Only the domain names that match your filter criteria will remain. If the domain list contains two names "apple" and "cedar", and you type "c" in the filter text box, "apple" is removed from the list since it does not match the filter criteria.



Use the backspace key to clear the filter.

3. Click **OK** or **Apply** to open that domain in VLAN Manager's Main window.
 - **OK** opens the selected domain and then closes the Open Domain dialog box.
 - **Apply** opens the selected domain but keeps the Open Domain dialog box open.

Click **Cancel** to exit this operation and return to the SPECTRUM VLAN Manager Main window without changing domains.



If you frequently change domains, use **Apply** to leave the 'Domain Open' window open. This saves you time, since you don't have to bring up the Open Domain window every time you want to change domains.

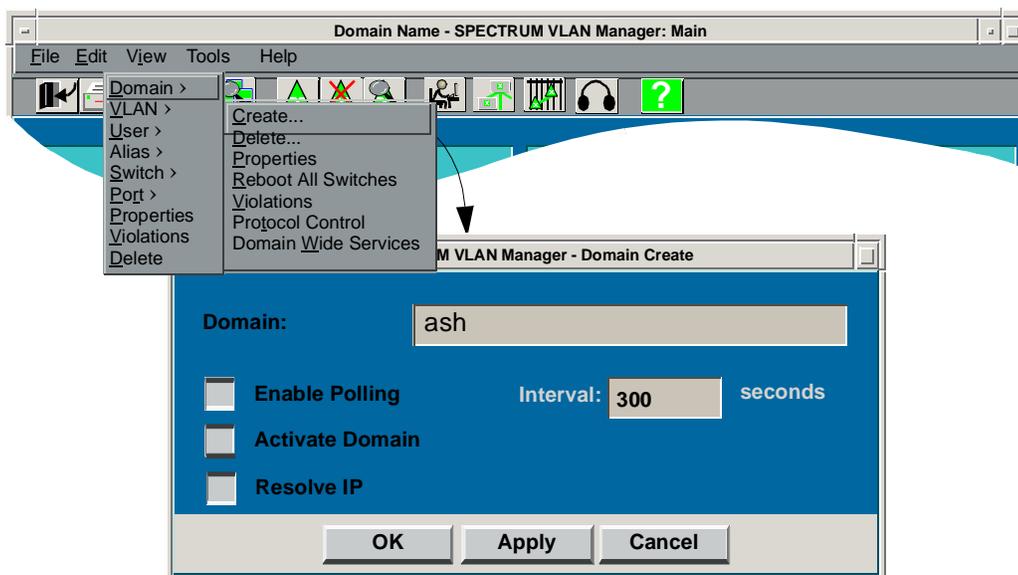
Creating Domains

Create lets you create VLAN domains without running Discovery.

To create a VLAN domain using the **Create** selection:

1. Select **Create** from the **Edit > Domain** menu to display the SPECTRUM VLAN Manager's Domain Create dialog box (Figure 6-13).

Figure 6-13. Creating VLAN Domains Using Create



2. Enter the name of the domain you want to create in the **Domain** text box.
3. VLAN Manager will automatically poll your network at a specified interval and add new VLAN switches and users discovered to your topology providing that at least one switch has been created. To use this feature, select **Enable Polling** (button recessed), and enter the poll time, in seconds, in the **Interval** text box. The default setting is 300 seconds.



The default polling interval is 300 seconds. Longer polling intervals may be required for large networks. If the polling interval is too small, the VLANServer will not have time to complete polling the network before the next polling cycle is scheduled to begin. If the polling interval is too large, important network events may not be reported in a timely manner.

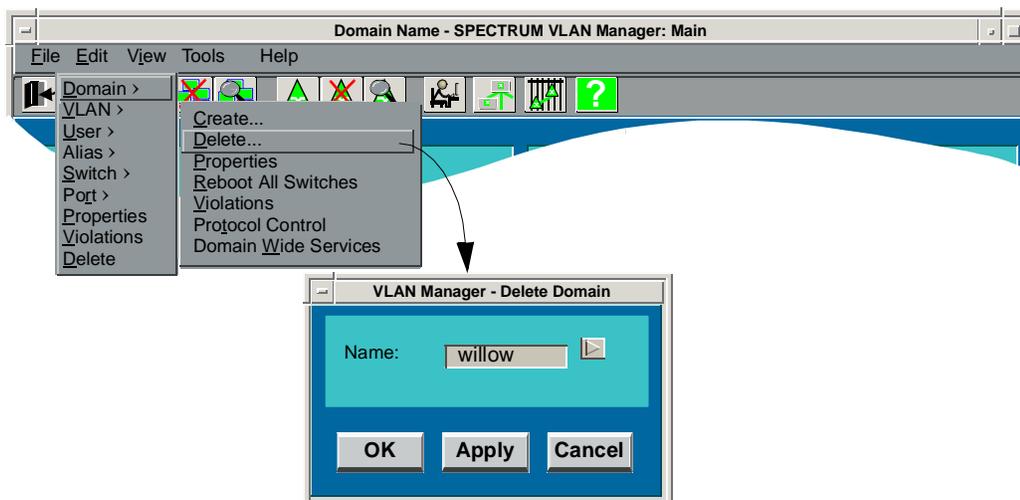
4. Use the **Activate Domain** button when you want to display the created domain immediately.
5. Use the **IP Resolve** button when you do not want VLAN Manager to perform name resolution for IP users. This expedites discovery in instances where DNS is not configured properly on an NT system.
6. Select **Apply** to create a new domain and leave the Domain Create window open, **OK** to create a new domain and close the window, or **Cancel** to close the window without creating a new domain.

Deleting Domains

To delete VLAN domains:

1. Select **Delete** from the **Edit > Domain** menu to display the VLAN Manager's Delete Domain dialog box (Figure 6-14).

Figure 6-14. Deleting VLAN Domains

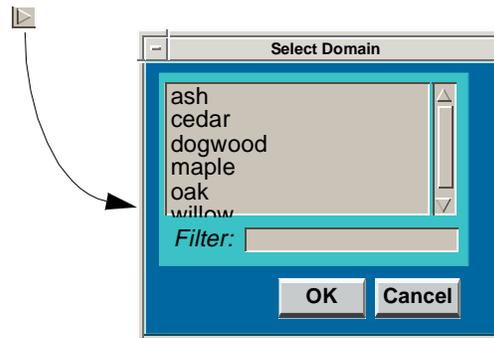


2. Enter the name of the domain to be deleted in the **Name** text box

The  button offers a convenient way to find a particular domain in large networks containing multiple domains. To use this feature:

- a. Click  to display the Select Domain dialog box (Figure 6-15).

Figure 6-15. Delete Domain - Select Domain Dialog Box



- b. Click in the **Filter** text box.
 - c. Enter the name of the domain you want to find. As you type, domain names that don't match the filter criteria will be removed from the domain list. Only the domain names that match your filter criteria will remain.
3. Click on the name of a domain, and then click **OK**. The selected domain name is entered into the **Name** text box in the VLAN Manager's Delete Domain dialog box.

Click **OK** to delete the selected domain and close the window, **Apply** to delete the selected domain and leave the window open, or **Cancel** to exit the operation and return to the SPECTRUM VLAN Manager Main window. Domains that are deleted are permanently removed from the VLANServer database.

Domain Properties

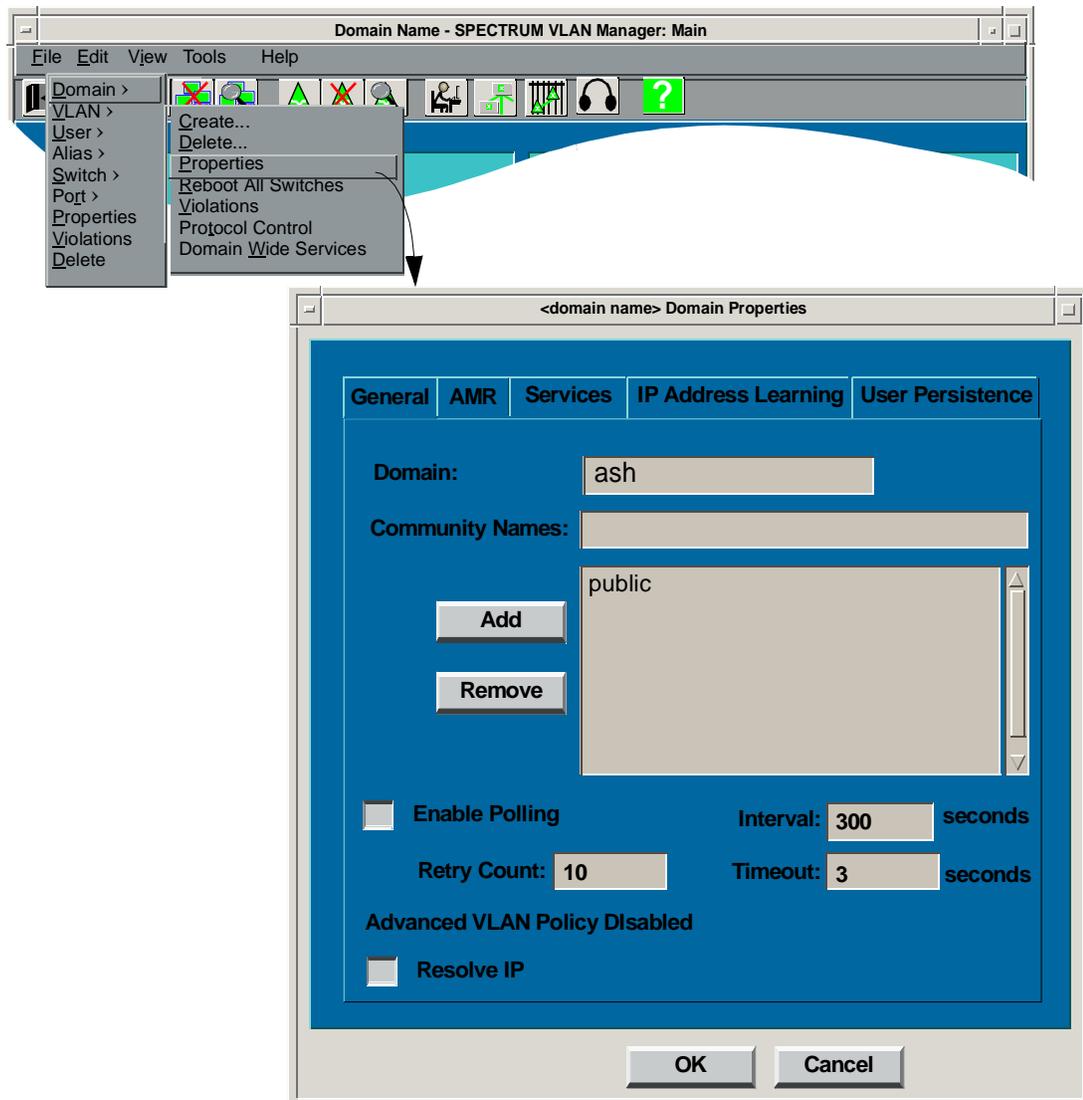
Properties lets you configure the current VLAN domain. You can configure General, AMR, Services, IP Address Learning, and User Persistence properties for the domain.

General Properties

To configure General properties for a VLAN domain:

1. Select **Properties** from the **Edit > Domain** menu to display the Properties tabbed folder.
2. Click **General** to display the domain general properties tabbed page (Figure 6-16).

Figure 6-16. General Domain Properties



3. Enter the community name(s) for a switch in the domain, and then press return or click **Add** to add the name to the community name list. Once a name is added to the community name list, it is cleared from the **Community Name** text box. Repeat this process until the community name list contains community names for all switches in the domain. "public" is the default community name. Click a community name and then click **Remove** to remove a community name.

Discovery tries each community name listed until it finds one that matches the seed switch's community name. Next, Discovery finds the seed switch's neighbors and tries to contact them using the same community names. If a switch cannot be reached using any of the community names listed, the switch will not be discovered.

4. VLAN Manager will automatically poll your network at a specified interval and add new VLAN switches and users it discovers to your topology. To use this feature, enable **Enable Polling** (button recessed), and enter the polling interval, in seconds, in the **Interval** text box. The default setting is 300 seconds.



The default polling interval is 300 seconds. Longer polling intervals may be required for large networks. If the polling interval is too small, the VLANServer will not have time to complete polling the network before the next polling cycle begins. If the polling interval is too large, important network events may not be reported in a timely manner.

5. You can change the **Retry Count** and **Timeout** values (Figure 6-16).
 - **Retry Count** - Number of times information is requested by the VLANServer before a fault is indicated and the switch icon turns Red. The default is 10 times.
 - **Timeout** - Amount of time that the VLANServer will wait between requests before it tries again (providing the Retry Count has not been exceeded). The default timeout is 3 seconds.

To change either of these values, highlight the old value and type in the new value.

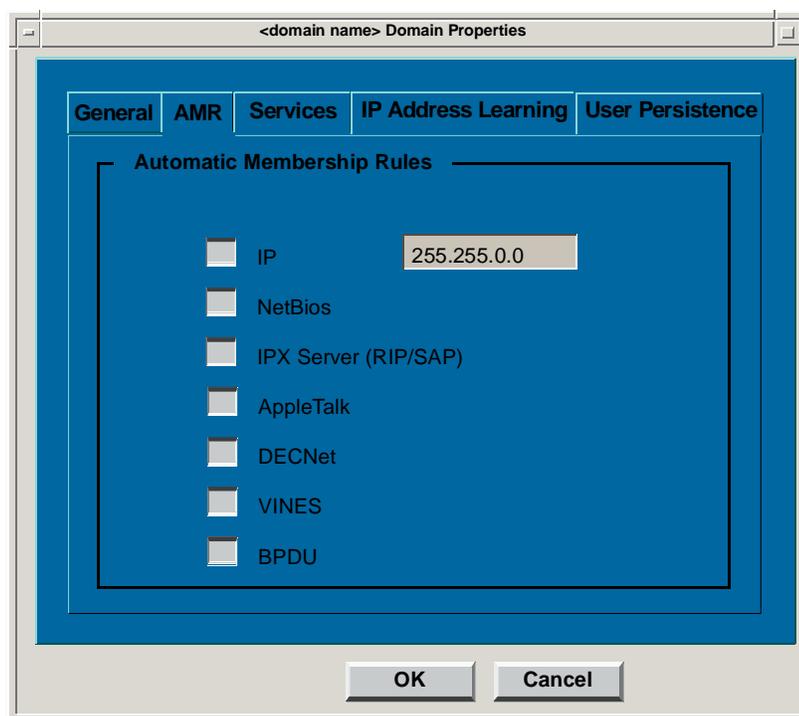
6. Use the **IP Resolve** button when you do not want VLAN Manager to perform name resolution for IP users. This expedites discovery in instances where DNS is not configured properly on an NT system.
7. Select **OK** to accept changes and close the window, or **Cancel** to close the window without making changes. To display another tabbed page, click the corresponding tab.

AMR Properties

To configure AMR properties for a VLAN domain:

1. Select **Properties** from the **Edit > Domain** menu to display the Properties tabbed folder.
2. Click **AMR** to display the domain AMR properties tabbed page (Figure 6-17). Refer to *AMR VLAN Administration*, on page 9-19, for detailed information about setting AMR properties.

Figure 6-17. Domain AMR Properties



3. Click **OK** to accept changes and close the window, or **Cancel** to close the window without making changes. To display another tabbed page, click the corresponding tab.

Services Properties

You can enable and disable configured services from this tabbed page.

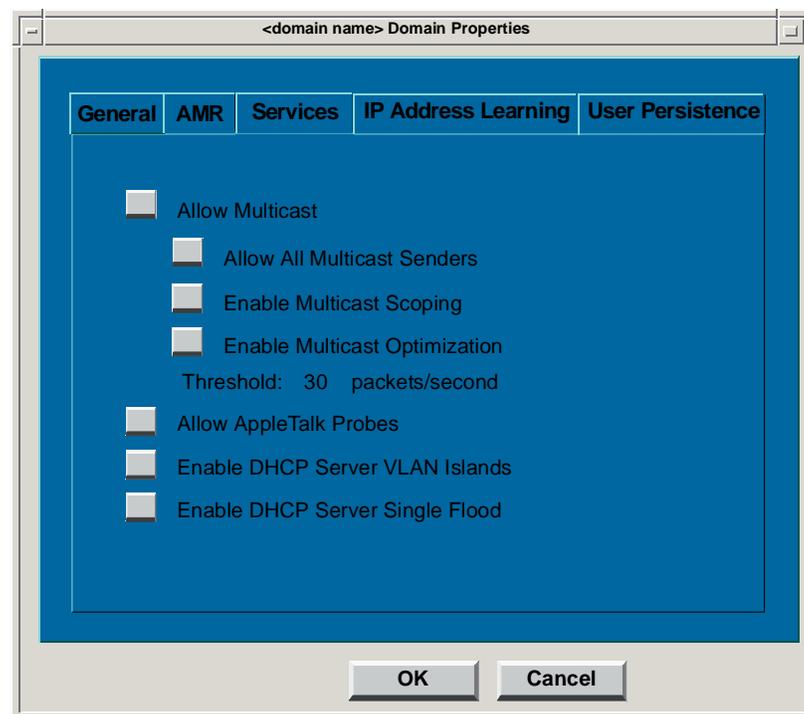
To configure Services properties for a VLAN domain:

1. Select **Properties** from the **Edit > Domain** menu to display the Properties tabbed folder.
2. Click **Services** to display the Services tabbed page (Figure 6-18) and then enable/disable the selected service(s) at the domain level.



The firmware for all switches in the domain must support these features in order for them to work optimally. If one of these services cannot be enable on a particular switch, messages are written to the VLANServer output log in the Control Panel.

Figure 6-18. Services Properties



- **Allow Multicast** - Allow (recessed button) or disallow (raised button) IP multicast call processing for this domain. IP multicast call processing enables you to set up unidirectional point-to-multipoint connections for multicast traffic within the domain. Multicasts are most often used when data from a given source must be distributed simultaneously to several destinations (e.g., sending video to

a group or disk mirroring). If this option is allowed, the Enable Multicast Scoping and Enable Multicast Optimization options become available. The multicast options may already be selected if they were enabled in the Discovery Wizard (see *Step 6 on Page 6-7*).

- **Allow All Multicast Senders** - Allow (recessed button) or disallow (raised button) all IP Multicast senders on this domain.



You can use the IPMC Sender Policy Tool to add or remove IPMC Senders individually per switch. Refer to the *SecureFast Tools Guide*.

- **Enable Multicast Scoping** - Enable (recessed button) or disable (raised button) IP Multicast Scoping. If this option is enabled, IP multicast traffic is flooded out ports with the same inherited VLAN. If it is disabled, IP multicast traffic is flooded out all ports regardless of VLAN membership.
- **Enable Multicast Optimization** - Enable (recessed button) or disable (raised button) Multicast Optimization. This option improves IP Multicast connectivity setup time by allowing you to set a Threshold value for IP Multicast packets.
 - **Threshold** - Limits the rate of connections created along the Control Channel to this value (packets per second) or less. When traffic exceeds the Threshold value, subsequent connections will be made based on VLSP. The default value is 30 packets per second, but you can change it to any integer value from 1 to 500 packets per second.
- **Allow AppleTalk Probes** - Allow (recessed button) or Disallow (raised button) AppleTalk probes to flood across the entire switch fabric even if that means crossing Open VLAN and Secure VLAN boundaries. It also allows a responding endpoint's AARP reply to the probe to be propagated back to the original probing endpoint regardless of any VLAN configurations. This feature is not enabled by default and should only be used if your SecureFast network is experiencing AppleTalk network-address collisions.
- **Enable DHCP Server VLAN Islands** - Enable (recessed button) or Disable (raised button) DHCP Server VLAN Islands. If enabled, a DHCP VLAN is created. By default the VLAN is named dhcpserver (if enabled, this name can be modified in the VLAN Islands view of the Switch Properties window. See *VLAN Islands View*, on page 7-9 for more information). You then add the DHCP servers you wish to use for servicing DHCP requests to the dhcpserver VLAN. Only DHCP Servers in the DHCP VLAN will reply to the DHCP clients' requests. This prevents unauthorized DHCP Servers from servicing DHCP requests for clients in the domain. If disabled, any DHCP Server can service DHCP requests. This functionality is disabled by default.

The DHCP Server VLAN Islands feature allows you to have several DHCP servers in your domain. You can control which DHCP server users on each switch will use by configuring each switch with the appropriate island.

- **Enable DHCP Server Single Flood** - Enable (recessed button) or Disable (raised button) DHCP Server Single Flood. The purpose of this feature is to limit the range of DHCP Server replies. If enabled, when a DHCP client sends out a request for an IP address the switch attached to the DHCP server extracts the MAC address of the client, determines the client's location, and delivers the response directly to that client. If disabled, the reply will be flooded out to all client's on the DHCP network.



VLANs that have been configured as DHCP Server VLAN Islands or AppleTalk AMR VLAN Islands should not be deleted.

3. Click **OK** to accept changes and close the window, or **Cancel** to close the window without making changes. To display another tabbed page, click the corresponding tab.

IP Address Learning Properties

If enabled, you can use this feature to enable and disable learning of subnets by the switches in a domain. Initially, since the internal subnets list is empty, all subnets will be learned. If you add a subnet to the list, only that subnet will be learned. No other subnets will be learned.

To enable or disable subnet learning for a VLAN domain:

1. Select **Properties** from the **Edit > Domain** menu to display the Properties tabbed folder.
2. Click **IP Address Learning** to display the Subnet tabbed page ([Figure 6-18](#)).

Figure 6-19. IP Address Learning Properties

**NOTE**

If a default gateway has been configured for the domain (*Configuring a Router Port*, on page 8-9), the subnet mask and any internal subnet addresses will automatically be displayed in the Subnet Mask field and the internal subnet list.

3. The current domain's natural subnet mask is displayed in the Subnet Mask field. To add a subnet to the list of internal subnets, enter a subnet IP address into the Subnet text field and then click **Add**. The subnet is added to the subnet list. Repeat this process for each subnet you want to add to the subnet list.

To remove a subnet from the subnet list, click the subnet you want to remove and then click **Remove**. The subnet is removed from the subnet list.

4. Select an Invalid IP validation mode (**No Learning**, **Discard**, **Disable**) from the Validation Mode drop-down list. Each mode performs a different level of IP address learning and call setup. Source address checking is done for the **No Learning** and **Discard** modes. No source address checking is done for the **Disable** mode. Refer to the mode descriptions provided below.

No Learning - An endpoint with an IP address which is not in the range of the subnets listed in the Internal Subnets list will have its MAC address learned but not its IP address. Call setup will take place. An entry for that endpoint will be added to the Violations table. Refer to *Violations*, on page 10-32 for information about the Violations table.

Discard - An endpoint with an IP address which is not in the range of the subnets listed in the Internal Subnets list will have its MAC address learned but not its IP address. *No* call setup will take place unless the destination has previously been resolved. An entry for that endpoint will be added to the Violations table. Refer to *Violations*, on page 10-32 for information about the Violations table.

Disable - An endpoint with an IP address which is not in the range of the subnets listed in the Internal Subnets list will have its MAC address and IP address learned. Normal call setup will take place.

5. Select **OK** to accept changes and close the window, or **Cancel** to close the window without making changes. To display another tabbed page, click the corresponding tab.

User Persistence

User Persistence enables the retention of VLAN mappings for endpoints in the event that a switch resets. When a switch resets, its user alias table is erased, and all knowledge of those users' VLAN memberships is lost. Mappings for "silent" users such as printers, and Layer 3 aliases are also lost. When the the VLANServer reestablishes contact with the switch, it may take up to two VLANServer polling intervals for the user and its previous VLAN information to be reconfigured. Users on the switch's ports will inherit the VLAN of the port to which they're connected during this time, and may be able to make the connections allowed for that VLAN, causing a potential security problem.

When you enable User Persistence, user/VLAN mappings for users (including silent users) and Layer 3 aliases are retained in the Directory (see *Using the Directory*, on page 10-14). Users and Layer 3 aliases which have been configured as persistent will be written back to the switch(es) as soon as the switch resets. This minimizes delay in call setup time, and reduces delays in making static VLAN mappings, so that no breakdown in communications or security occurs. Configuring endpoints as persistent will ensure that they always show on the switch.

The User Persistence tab in the Domain Properties view lets you select those users you wish to persist in the domain. You can also enable User Persistence on an individual user basis by enabling the **Persist User** button on the User Properties **General** Tab (see *User Properties*, on page 10-6).



Configuring a user as persistent does not prevent it from being learned on a different port. The User Restriction feature still regulates user mobility. If the user's information changes, the switch still recognizes it, and VLAN Manager is updated accordingly.

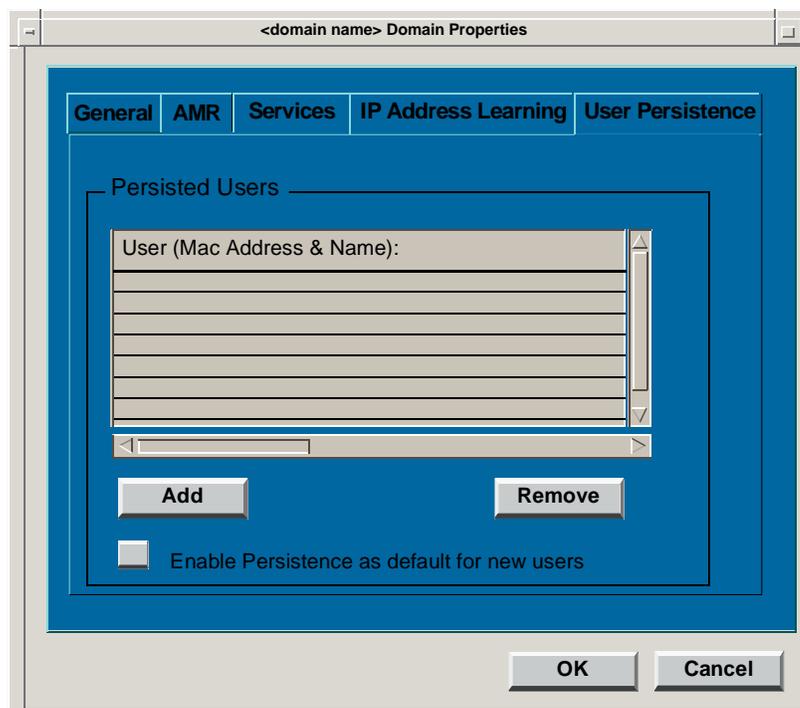
To enable User Persistence for users in a domain:

1. Select **Properties** from the **Edit > Domain** menu to display the Properties tabbed folder.
2. Click the **User Persistence** tab. If there are currently persisted users, their MAC address and User Name are displayed in the Persisted Users list.



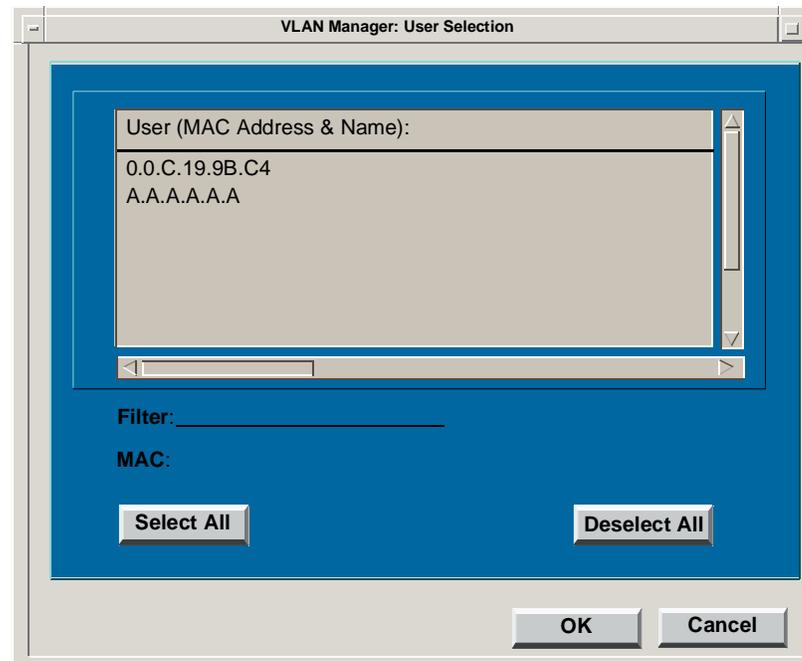
You can print the list of persisted users from the Directory view using its **Search/Filter** and **File>Save** (to file) features (see *Using the Directory*, on page 10-14).

Figure 6-20. User Persistence Tab



3. Click **Add...** to display the User Selection window. All non-persisted users in the domain are displayed in the list.

Figure 6-21. User Selection Window



4. Select the user or users you wish to be persisted, using one of the following methods:
 - a. Click on the user(s) in the list. Use the scroll bars if needed, or type part of the user's MAC address or name in the **Filter** field and press **Return** to find the user(s) you want. To select a sequence of users, click the first user and drag over the users you want to select.
 - b. Type the user's full MAC address in the **MAC** field.
 - c. Click **Select All** to select all the users in the domain.

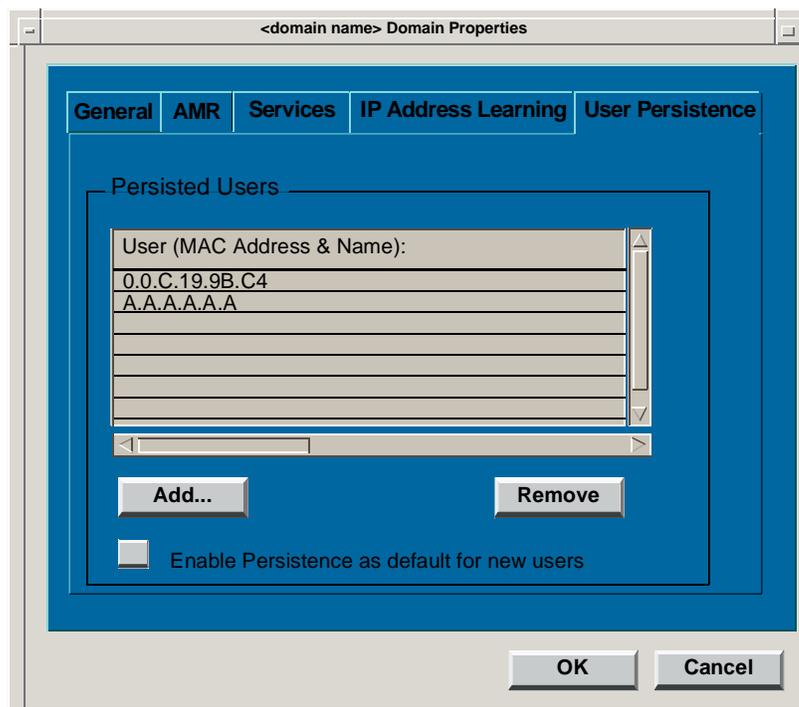
To deselect a selected user or users, click the selected user(s) in the list. To deselect a sequence of users, click the first selected user and drag over the users you want to deselect. To deselect all users, click **Deselect All**.

5. Click **OK** to return to the **User Persistence** tab.
6. If you want all users added to the domain in the future to be persisted, click (depress) the **Enable Persistence as default for new users** button. To disable this feature, click (raise) the button.

To disable User Persistence for users in a domain:

1. Select **Properties** from the **Edit > Domain** menu to display the Properties tabbed folder.
2. Click the **User Persistence** tab. The existing persisted users are displayed.

Figure 6-22. User Persistence Tab



3. Click on the user(s) in the list that you no longer wish to be persisted, using the scroll bars if needed. To select a sequence of users, click the first user and drag over the users you want to select.

To deselect a selected user or users, click the selected user(s) in the list. To deselect a sequence of users, click the first selected user and drag over the users you want to deselect.

4. Click **Remove**.
5. Click **OK**.

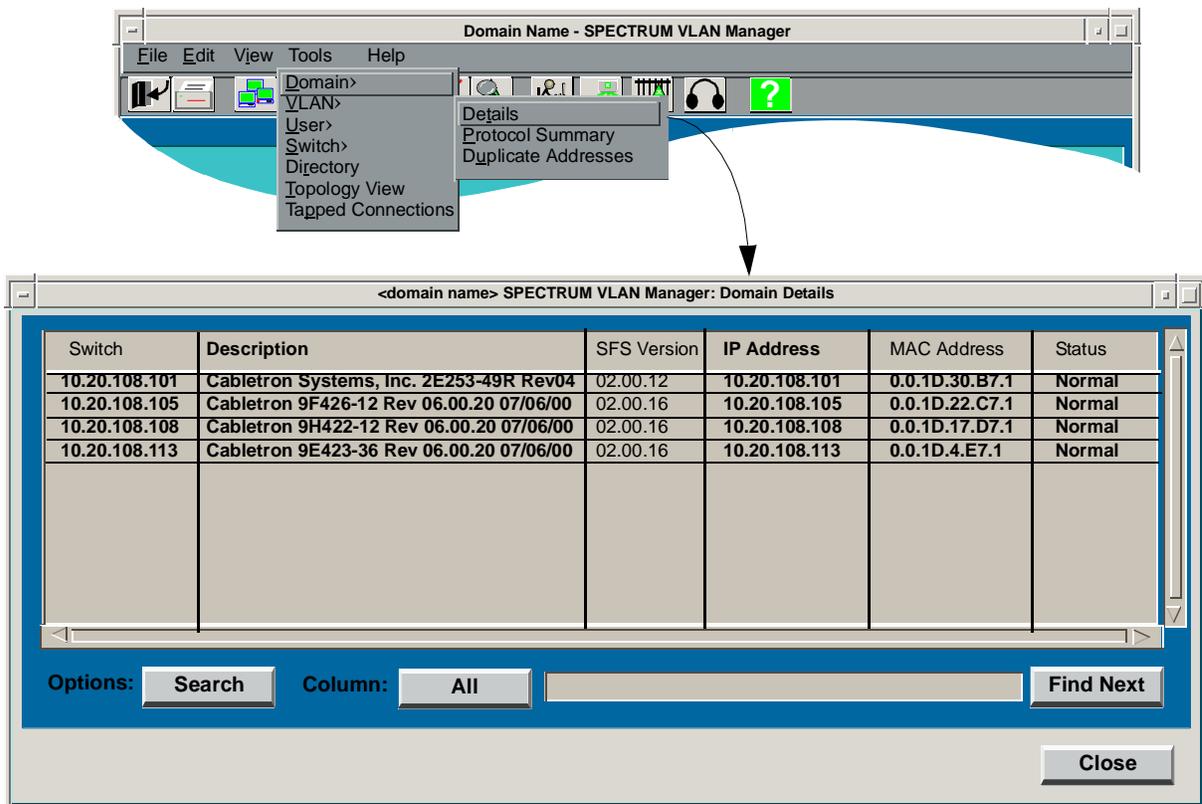
Domain Details

Details lets you display detailed information about switches contained in a selected domain. Using the pop-up menu, you can launch the Source Blocker, Flood Suppression and Violations tables, as well as the Switch Properties tabbed folder, from this window.

To display domain details:

Select **Details** from the **View > Domain** menu to display the SPECTRUM VLAN Manager's Domain Details window (Figure 6-23).

Figure 6-23. Domain Details



Domain Details Window Column Descriptions

- **Switch** - Name of the switch for which the port information is being displayed. If DNS is not being used, the switch's IP address is displayed or the name configured using Switch Properties.
- **Description** - Provides firmware/hardware information for the selected switch.

- **SFS Version** - Version of the SecureFast Services firmware component running on the switch.
- **IP Address** - Network address of the switch.
- **MAC Address** - Physical address of the switch.
- **Status** - Normal, Contact Lost, or Major.
- **Uptime** - Length of time the switch has been in operation since its last initialization. Time is shown in days, hours, minutes, and seconds. For example, 2+14:09:45 represents 2 days, 14 hours, 9 minutes, and 45 seconds.
- **Total Connections** - Number of connections for the selected switch.
- **Resolve Timeouts** - Number of times the originating switch did not receive a resolve response.
- **Local Nodes** - Number of local nodes on the selected switch.
- **Topology Change Count** - Number of interswitch link changes processed by the switch.
- **Connection Utilization** - Percent of total switch capacity for connections.
- **Node Utilization** - Percent of total possible nodes currently used.
- **Alias Utilization** - Percent of total possible aliases currently used.
- **Source Blocker Number of Entries** - Number of entries in the Source Blocker table.
- **Flood Suppression Number of Entries** - Number of entries in the Flood Suppression table.
- **Switch Violations** - Total user and port restriction violations for the selected switch.
- **Age Pass Count** - The number of aging passes that have occurred.
- **AppleTalk VLAN Island** - Displays the status of this service (enabled or disabled) as configured in the AMR Properties View of the Domain Properties window (see [AMR Properties](#) on page 6-21).
- **DHCP VLAN Island** - Displays the status of this service (enabled or disabled) as configured in the Services View of the Domain Properties window (see [Services Properties](#) on page 6-22).
- **Uplink State** - Indicates whether or not the switch is configured as an uplink switch. If it is an uplink switch, the Uplink State column indicates whether the switch is a Tier 1 or Tier 2 uplink switch. If it is not an uplink switch, the state is Disabled. See [Expanding a Domain Using Uplink Switching](#) on page 6-34 for more information on uplink switching.
- **Link State Protocol** - Indicates the status of Link State Protocol on the switch. Possible values are: Running, Halted, Pending, Faulted, Not Started, Invalid, and

Unkown. The default is Running. For switches configured as uplink switches, Not Started or Halted is displayed.

- Spanning Tree** - Indicates the status of Spanning Tree Protocol on the switch. Possible values are: Running, Halted, Pending, Faulted, Not Started, Invalid, and Unkown. The default is Running. For switches configured as uplink switches, Not Started or Halted is displayed.

Launching the Source Blocker Table

The Source Blocker table contains information about users for which non-unicast frame processing has been disabled. Non-unicast frame processing is disabled for a user when the user exceeds the maximum number of broadcasts per second threshold. Once in the table, broadcasts originating from that user are no longer processed by the switch.

To launch the Source Blocker table, click an entry in the Domain Details window and then select **Source Blocker** from the pop-up menu. The Source Blocker Configuration Tool: Main window is displayed. For detailed information about how to use this tool, refer to the *SecureFast Tools Guide*.

Launching the Flood Suppression Table

When the number of packets sent to a destination without the destination responding exceeds the threshold number, the destination is placed in the Flood Suppression table. It is removed from the Flood Suppression table as soon as a switch hears it.

To launch the Flood Suppression table, click an entry in the Domain Details window and then select **Flood Suppression** from the pop-up menu. The Flood Suppression Table is displayed. For detailed information about how to use this tool, refer to the *SecureFast Tools Guide*.

Launching the Switch Properties Tabbed Folder

You can view and edit switch attributes from the **Switch Properties** tabbed folder. Refer to *Switch Properties*, on page 7-4.

Launching the Violations Table

Switch violations occur whenever a port or user restriction violations occur. For detailed information about port and user restrictions, refer to *Restricting a Port*, on page 8-42 and *User Restrictions*, on page 10-25 respectively.

To launch the Switch Violations table, click on entry in the Domain Details window and then select **Switch Violations** from the pop-up menu. The SPECTRUM VLAN Manager: Switch Violations window is displayed. For detailed information about how to use this table, refer to *Violations*, on page 10-32.

Rebooting All Switches in a Domain

VLAN Manager lets you reboot all the switches in a domain from the user interface without having to physically push the reset button on each switch. This is particularly convenient when upgrading firmware on all the switches in a domain.



You can also reboot an individual switch in a domain. Refer to *Rebooting an Individual Switch*, on page 7-17.

Reboot All Switches lets you reset all switches in a VLAN domain, provided they have Green operational status. A switch that does not have Green operational status (e.g., the switch is pulled out of the chassis) cannot be rebooted.

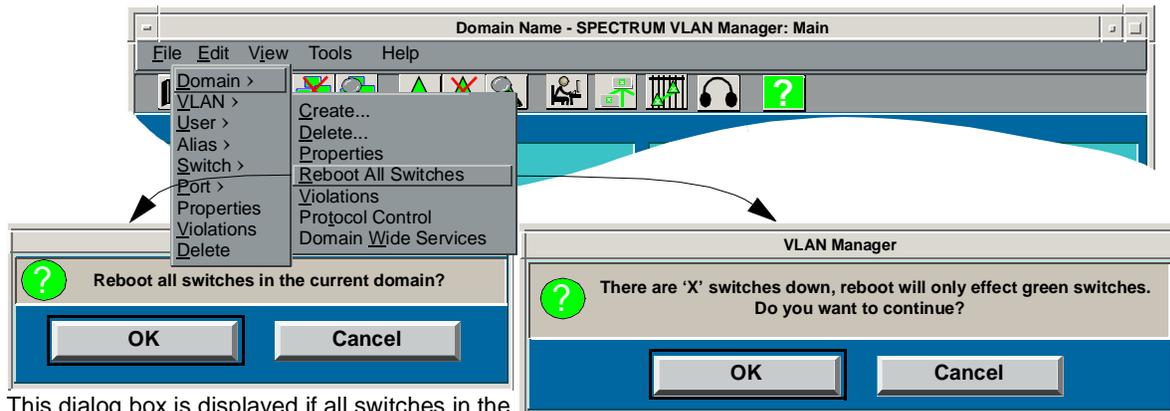
To reboot all switches in a domain:

1. Select **Reboot All Switches** from the **Edit >Domain** menu. If the Enable Dialogs (Confirmations) preference is set (refer to *Main Preferences*, on page 5-3), one of two dialog boxes is displayed, one for cases where all switches in the domain are showing Green operational status, and the other for cases where not all of the switches in the domain are showing Green operational status. Click **OK** to reboot all switches with Green operational status or **Cancel** to return to the VLAN Manager window without rebooting any switches. If the Enable Dialogs (Confirmations) preference is not set, all switches showing Green operational status are rebooted as soon as you select **Reboot All Switches**. (Figure 6-24).



1. A switch with an operational status other than Green will not be rebooted.
2. Each switch encountered with which contact was lost since the last poll will add additional time to the total reboot process.

Figure 6-24. Rebooting All Switches in a Domain



This dialog box is displayed if all switches in the domain are showing Green operational status.

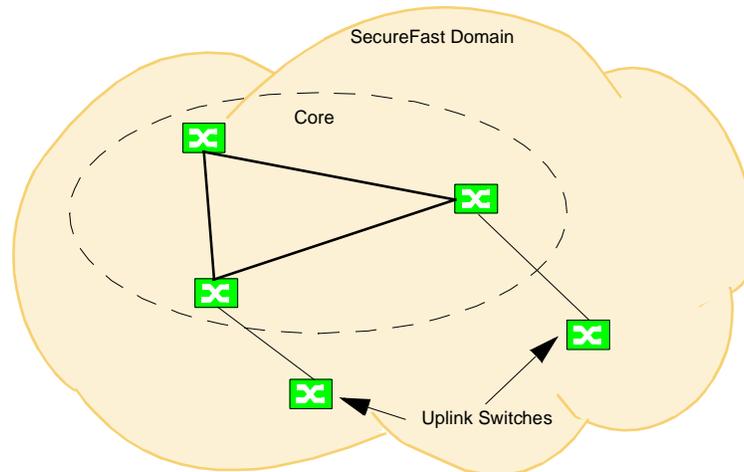
This dialog box is displayed if all switches in the domain are NOT showing Green operational status, where 'X' is the number of switches.

Expanding a Domain Using Uplink Switching



VLAN Manager enables you to configure Tier 1 uplink switches. To configure Tier 2 uplink switches, use the Uplinker tool in the `VLAN/tools/sftools` directory (Unix) or `Vlan\tools\sftools` folder (NT) in your VLAN Manager installation area. To start the tool, type `./uplinker` and follow the instructions given.

Uplink switching refers to a SecureFast network model that uses edge (uplink) switches to connect to a domain's core mesh of switches (Figure 6-25).

Figure 6-25. Uplink Switch Model

Uplink switching provides the following advantages:

- Uplink switches allow you to achieve a factor of scaling not possible with a single-area link state protocol. A single-area link state protocol permits a maximum of 128 switches in a domain. By adding uplink switches to your network, a significant increase in the number of switches and users in the SecureFast network can be achieved by implementing the uplink model. As the number of switches in a domain increases, so does the capacity to add uplink switches and the entire network scales with it.
- The diameter of the SecureFast network can be increased without affecting the link-state convergence. The uplink switches do not form peer VLSP adjacencies nor do they have to run an encapsulated spanning tree with the core switches to form the flood path. This essentially allows the network diameter of the domain to remain as it is and to be transparently extended out to the uplink switches. The link-state convergence of the domain is unaffected by the diameter extensions achieved by adding uplink switches.
- The uplink switches appear seamless and support the complete set of switch and VLAN Manager services.

Configuring Tier 1 Uplink Switching

Uplink switching is configured on a per-chassis basis. To run uplink switching on a chassis, you must set up the chassis for uplink switching and then configure it for dynamic uplink switching. You can also configure stand-alone switches as uplink switches.



Do not connect the VLANServer workstation to an uplink chassis. Contact may be lost with the VLANServer during uplink chassis initialization.

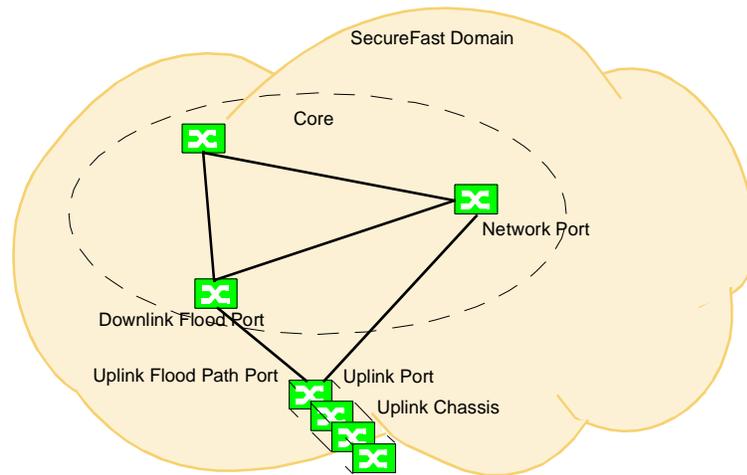
Setting Up a Chassis to Run Uplink Switching

To set up a chassis to run uplink switching:

- Make sure that the switches in the chassis are connected to each other via the chassis backplane. No chassis interswitch front panel connections are allowed.
- Make sure there is at least one front panel connection from one of the switches in the chassis to a core switch. There are two types of connections from an uplink chassis to the core switches: uplink flood and uplink.
 - The uplink flood connection is used as the uplink flood path from the uplink chassis to the core switch. Where it connects to the uplink switch port is known as the “uplink flood path” port. Where it connects to the core switch port is known as the “downlink flood” port.
 - An uplink connection to the core is used for load balancing. Where it connects to an uplink switch port is known as the “uplink” port. Where it connects to a core switch port is considered to be a network port.

If only one connection exists between the uplink chassis and the core, that connection is used as the uplink flood path. If multiple connections exist between the uplink chassis and the core, the switches in the chassis determine which connection will be used as the uplink flood path. Other connections will be designated as uplinks.

Figure 6-26. Uplink Chassis Setup



Setting Dynamic Uplink



If you add a switch to a chassis already running dynamic uplink switching, the switch is automatically configured as an uplink switch.

To configure the switches to Tier 1 uplink:

1. In the Physical pane of the VLAN Manager's Main window, select a switch in the chassis that you want to run uplink switching.
2. Select **Edit >Switch >Set/Unset Uplink** from the menu.

The VLAN Manager software finds all the switches in the chassis, determines how many switches there are in the chassis, turns off Spanning Tree and LSP (Link State Protocol) for the chassis, and notifies you that the switches will be reset.

3. Perform the following uplink operational checks to verify that the chassis is operating in uplink switching mode:
 - a. Display port properties for the uplink port. It should be shown as an Uplink Flood port. The uplink port is shown as a cloud on the uplink switch in the Main VLAN Manager window. The uplink flood port is displayed during the execution of the "uplink" program.

- b. Display port properties for the downlink port. It should be shown as a Downlink Flood port. The downlink port is shown as a cloud on the downlink switch in the Main VLAN Manager window.
- c. Select **View >Domain >Details** from the menu, and check the following columns for the applicable switches: **Uplink State** (should indicate the Tier), **Link State Protocol** (should be Not Started), and **Spanning Tree** (should also be Not Started).

If any of these checks is unsuccessful, perform the chassis setup and uplink configuration procedures again.

Unsetting Dynamic Uplink

To unset dynamic uplink on a chassis running in uplink switch mode:

1. From the Physical pane of the VLAN Manager's Main window, select a switch in the chassis that you no longer want to run in uplink switch mode.
2. Select **Edit >Switch >Set/Unset Uplink** from the menu.

The VLAN Manager software finds all the switches in the chassis, determines how many switches there are in the chassis, turns on Spanning Tree and LSP (Protocol) for the chassis, and notifies you that the switches will be reset.

Protocol Control



1. By default, all protocols and protocol frame types are enabled for a domain. To enable or disable a protocol or protocol frame type for an individual switch, refer to *Switch Protocol Control*, on page 7-19.
2. Protocol policy set at the switch level always overrides protocol policy set at the domain (fabric) level.
3. IP cannot be disabled.

The primary purpose of implementing Protocol Control is to reduce the amount of broadcast traffic on your network by limiting the types of protocols and protocol frame types that the switches being managed by a VLANServer will process. For example, if you disable all IPX frame types except IPX 802.2, you will force all users making requests

to any of the switches in your network to use the 802.2 frame type. Users making requests using the older 802.3 (RAW) frame type will not be processed.



If there are certain switches in the switch fabric that you wanted users to be able to use the 802.3 frame type, you would use the Switch Protocol Control to enable 802.3 on those switches. Switch policy overrides fabric policy so requests to those switches would be processed.

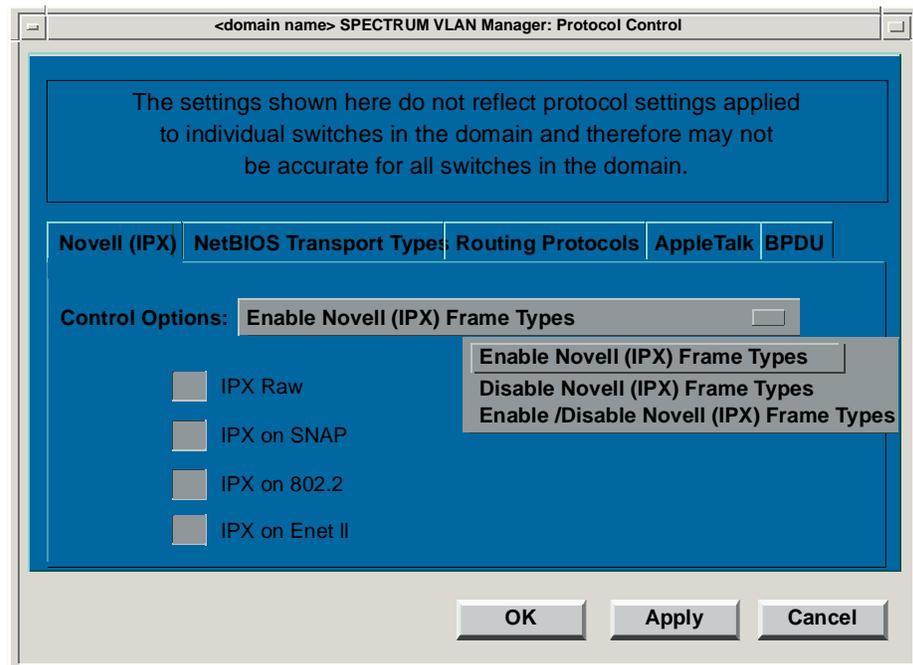
Other reasons for implementing Protocol Control on your network may include forcing users to use a certain protocol frame type or limiting the propagation of certain routing protocols through the switch fabric in your network.

You can enable or disable an entire protocol or protocol frame type.

To configure Protocol Control for a VLAN domain:

1. Select **Protocol Control** from the **Edit > Domain** menu to display the Protocol Control tabbed folder. From this page, you can enable/disable Protocol Control elements at the domain level.
 - **Protocol Control** - Enable/Disable protocols by protocol or by frame type. By default, all protocols and frame types are enabled.
 - **By Protocol** - You can enable/disable any or all of the following protocols: Novell (IPX), NetBIOS Transport Types, Routing Protocols, AppleTalk, and BPDU
 - **IPX Frame Types** - Raw, SNAP, 802.2, Enet II
 - **NetBIOS Frame Types** - IP - NetBIOS, IPX-NetBIOS, and NetBEUI on 802.2
 - **Routing Frame Types** - OSPF Broadcast, OSPF Multicast, Interior Gateway Protocol, RIP/RIP II, RTMP (AppleTalk)
 - **AppleTalk Frame Types** - DDP on SNAP and AARP on SNAP
 - **BDPU Frame Type** - Spanning Tree

Figure 6-27. Protocol Control



2. Click a protocol tab to display the control options for that protocol.
3. Select a control option from the **Control Options** drop down list.
4. If you selected **Enable/Disable <protocol> Frame Types** from the control options drop down list, enable/disable frame types by clicking the button that corresponds to the frame type you want to enable (recessed) or disable (raised).
5. Select **Apply** to accept configuration changes and leave the Properties window open, **OK** to accept changes and close the window, or **Cancel** to close the window without making changes. To display another tabbed page, click the corresponding tab.

Domain Wide Services

The Domain Wide Services window lets you manage (enable/disable) services on each switch in a domain. This window displays the manageable services available for the domain, displays all of the switches on the domain, shows the status of each service on each switch, and lets you enable/disable each service. In addition, this window gives you the opportunity to configure a domain wide default setting (enabled/disabled) for each service.

The services available for management in the Domain Wide Services window are:

- Flood Suppression
- Source Blocker
- DHCP Client Tagging
- Multicast
- Redundant Access
- User Mobility
- Call Tap
- AppleTalk Service
- Novell Service
- NetBIOS over IPX Service
- NetBIOS over IP Service
- NetBEUI Service



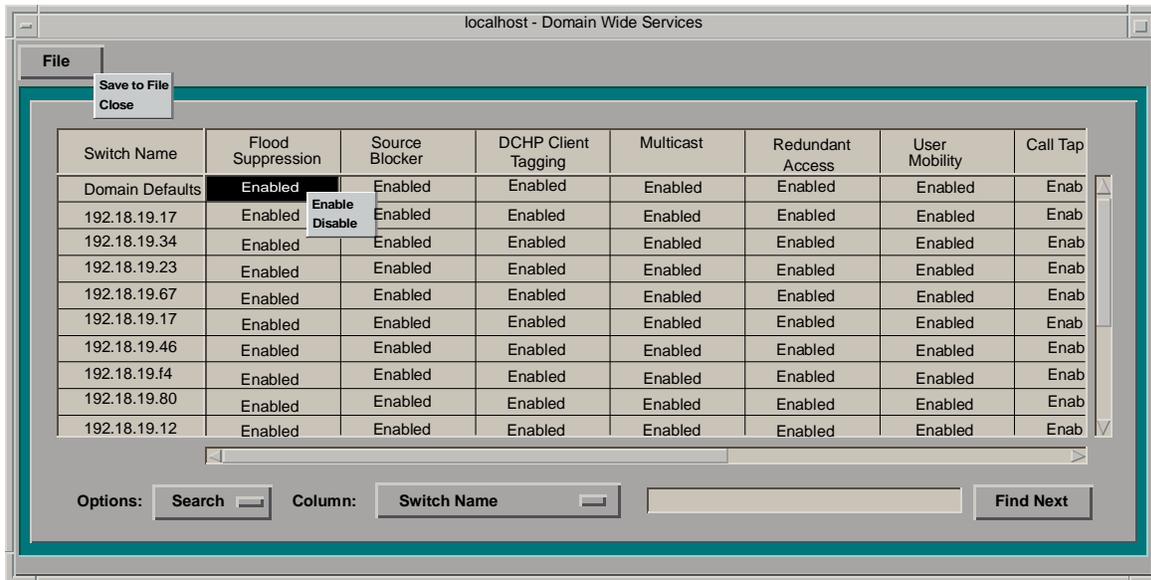
Initial discoveries will read the settings for the individual switch and set the services for that switch accordingly. Whenever a domain discovery is executed, the Domain Wide Services will all be reset to the Domain Defaults setting for each service on each switch.

You can save a view of your settings before executing a discovery by selecting **File**—> **Save to File**.

To manage services on each switch:

1. Select **Domain Wide Services** from the **Edit >Domain** menu. The Domain Wide Services window (Figure 6-28) is displayed.

Figure 6-28. Domain Wide Services



2. Under the **Switch Name** column, locate the IP address of the switch you want to configure. Click in the field to the right of the selected switch under the service you want to configure.
3. Click the right mouse button to display the pop-up menu. Select **Enable** or **Disable**.

To configure a default setting:



If you change the value for Domain Defaults, a message box will ask you to choose to Enable (or Disable) the Domain Default, if you want to change settings for all switches in the domain, or not change them.

If you choose to change the settings, the value of that service is changed as you have specified for all switches in the domain. This is helpful if you want to disable the service in the entire domain.

If you choose not to change the settings, only the value for the Domain Default will change. This is helpful if you want to change the value which newly discovered switches will use, but you want existing switches in the domain to continue to use whatever they have been configured as individually.

After making these decisions, click **OK** to apply the change, or **Cancel** to back out.

1. In the **Domain Defaults** row, in the column of the service you wish to configure, select **Enable** or **Disable** from the pop-up menu.
2. A message window will appear confirming that you want to change the domain wide settings for the selected service.
3. Click **OK** to set changes, or **Cancel** to exit the window without accepting the changes.

Any switch that joins the domain will acquire the Domain Defaults settings.

To save a view of your current Domain Wide Services settings:

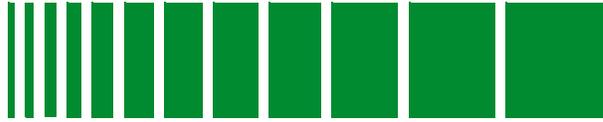
1. Select **File >Save to File**.
2. In the Save Domain Wide Services window, enter the directory in which you would like to save the view of your settings and click **OK**.

Using Search/Filter

Use the **Options** button to do a search or filter. You can search or filter by any table column. You can also **Filter** by **None**, which returns the table to the non-filtered state.

To use the search/filter:

1. Select **Search** or **Filter** from the **Options** list and the selection criteria from the **Column** list.
2. Click anywhere in the text box to the right of the **Column** selections, and then enter the text to be matched.
 - **Search** finds and highlights the first instance of a switch that matches the search criteria as it is entered. Click **Find Next** to find the subsequent instances of switches that match the same criteria.
 - **Filter** selectively eliminates entries from the **Switches** list that do not match the criteria entered. Switches that match the filter criteria are displayed.



Managing Switches

This chapter provides step-by-step instructions for performing switch administration tasks, using SPECTRUM VLAN Manager's graphical user interface. It also contains reference information and helpful tips to help you perform these tasks.

Overview

Switch management tasks are initiated from the **E**dit and **E**dit >**S**witch menus, the **V**iew >**S**witch menu, the Toolbar, or the Switch pop-up menus. You create and delete switches, force a switch to perform a poll, and force a switch to synchronize with the VLAN Manager from the **E**dit and **E**dit >**S**witch menus. You view switch details, expand and collapse the switch view, and manage switch attributes from the **V**iew >**S**witch menu.



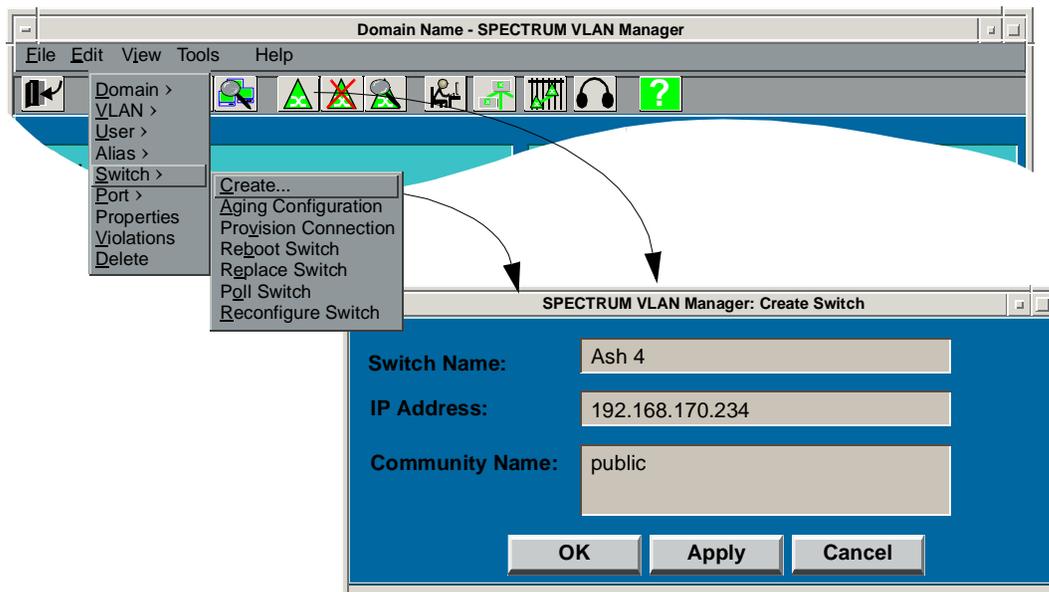
You can use the Switch pop-up menu to perform many switch management tasks. To display the pop-up menu, click on a switch and then click and hold the right mouse button. Drag the cursor to the task you want to perform, and then release the button.

Adding a Switch

To add a switch to a domain (Figure 7-1):

1. Select **C**reate from the **E**dit > **S**witch menu or click on the  from the Toolbar to display the SPECTRUM VLAN Manager's Create Switch dialog box.

Figure 7-1. Adding a Switch to a Domain



2. Enter a unique name or the name of the switch which has been registered with the name service for the new switch in the **Switch Name** text box.
3. Enter the IP address of the new switch in the **IP Address** text box.
4. Enter the community name for the new switch in the **Community Name** list box, if it is not already listed.
5. Press **OK** to create a new switch and close the window, **Apply** to create a new switch and leave the window open, or **Cancel** to dismiss the VLAN Manager - New Switch dialog box without adding a switch.

Deleting a Switch

To delete a switch (Figure 7-2):

1. Select the switch you want to delete.



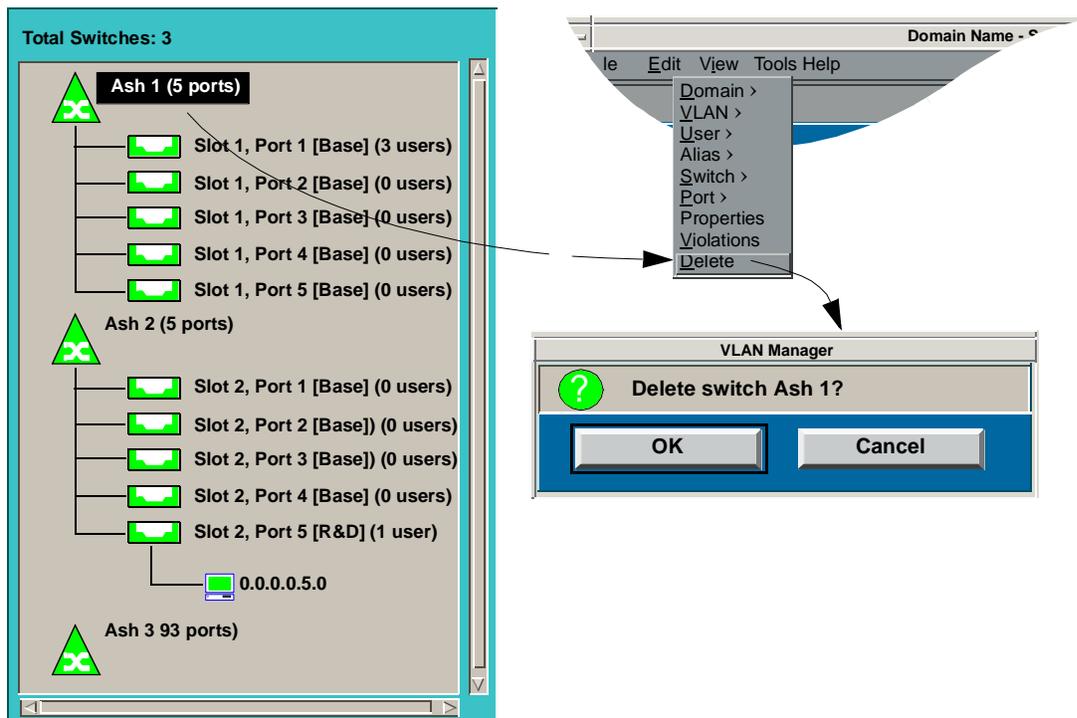
Do not delete a switch unless the switch has been physically removed from the network. If a switch is deleted without being physically removed from the network, changes to your network may not be reflected accurately by the VLAN Manager.



If you are deleting a switch on which persistent user(s) have been configured, you will see a message informing you of this, letting you know that deleting the switch disables persistence for those users, and giving you the option of backing out.

2. Select **Delete** from the **Edit** menu, select  from the Toolbar, or use the switch pop-up menus.
3. Confirm that you want to delete the selected switch by pressing the **OK** button in the VLAN Manager confirmation box.
4. Click the **Cancel** button to return to the VLAN Manager window without making any changes.

Figure 7-2. Deleting a Switch



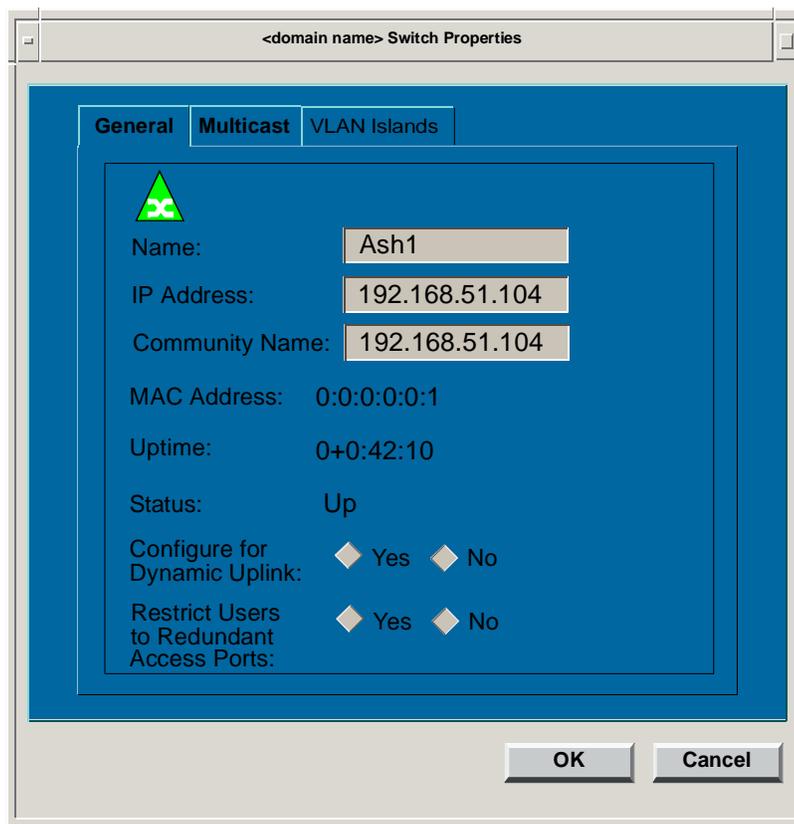
Switch Properties

To view and/or edit switch properties, select a switch, use the right mouse button to bring up the switch pop-up menu, and then select **Properties** or choose **Properties** from the **Edit** menu. The Switch Properties tabbed folder is displayed. This folder contains the following tabs: **General**, **Multicast**, and **VLAN Islands**.

General Switch Properties

The General View of the Switch Properties Window provides general information about the selected switch (Figure 7-3). The **Name**, **IP Address**, and **Community Name** fields are editable. This information is also available from Switch Details.

Figure 7-3. Switch Properties



- **Name** - Name of the switch for which the port information is being displayed. If DNS is not being used, either the switch's IP address or the name you have assigned to the switch is displayed. This field can be edited.
- **IP Address** - Network address of the switch. This field can be edited.
- **MAC Address** - Physical address of the switch.
- **Community Name** - Community name assigned to this switch.
- **Uptime** - Length of time the switch has been in operation since its last initialization. Time is shown in days, hours, minutes, and seconds. For example, 2+14:09:45 represents 2 days, 14 hours, 9 minutes, and 45 seconds.
- **Status** - Normal or Contact Lost.

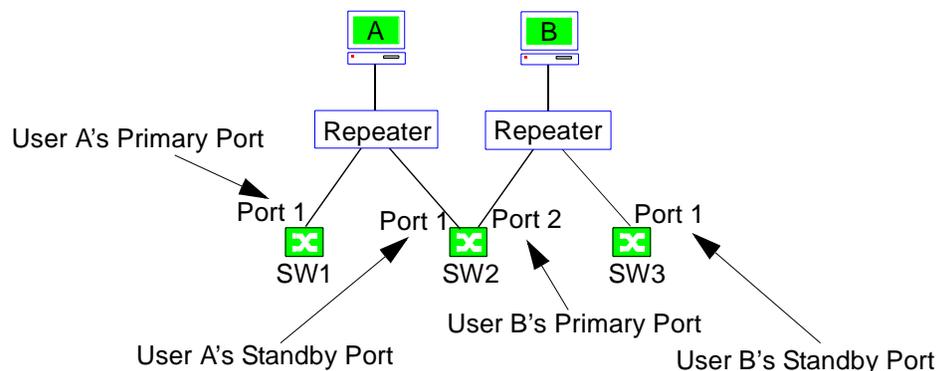
- Configure for Dynamic Uplink** - Enable or disable uplink switching. Refer to *Expanding a Domain Using Uplink Switching*, on page 6-34.
 - Yes** - Enables uplink switching.
 - No** - Disables uplink switching.
 - Neither** - Feature not supported by firmware.
- Restrict Users to Redundant Access Ports** - Used to restrict redundant access users to redundant access ports on a per-switch basis. The users restricted by using this feature cannot be moved to ports other than those to which they are restricted. In addition, the aliases of users restricted by using this feature cannot be used by another device.
 - Yes** - Restricts redundant access users (MAC and aliases) to a redundant access port(s).
 - No** - Do not restrict redundant access users to a redundant access port(s).
 - Neither** - Feature not supported by firmware.



If you use Redundant Access User Restrictions, do not restrict users or ports for redundant users using the user or port restrictions available from user or port properties. Doing so may cause unpredictable results.

If you use this feature, enable *all* switches with redundant access ports configured (Primary and Standby).

Figure 7-4. Redundant Access User Restrictions Example



For example, in the configuration shown in [Figure 7-4](#), you must enable Redundant Access User Restrictions on SW1, SW2, and SW3. If one of the switches, say SW3, is not enabled, unpredictable connection results may occur to User B when User B's 'standby' port is controlling connections to User B.

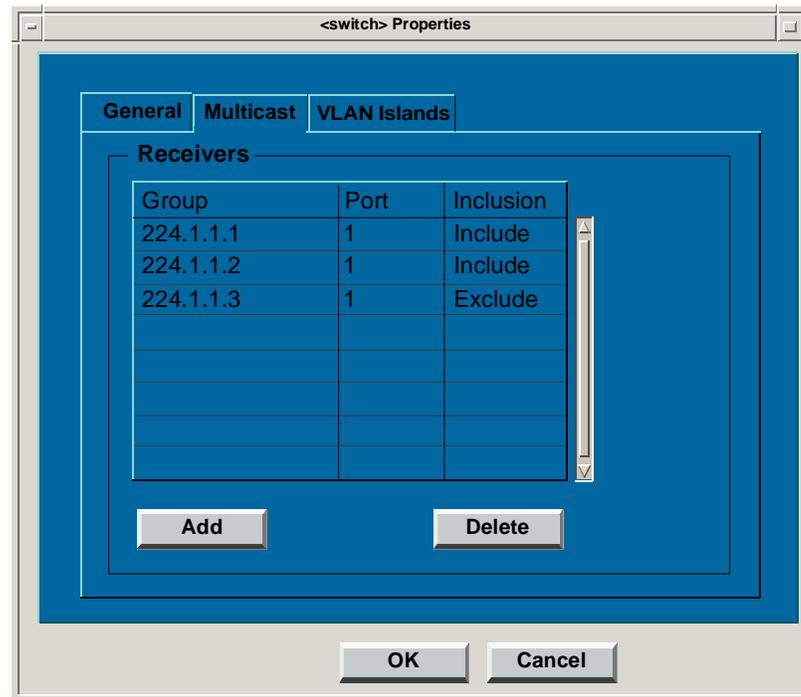
To further clarify this concept, consider the following:

Initially, User A is seen on its 'primary' port (SW1, Port1). All connections to and from User A are established through the 'primary' port. The redundant access ports on SW1 and SW2 are enabled, so User A is restricted to the ports on those switches to which it is connected (SW1, Port 1 and SW2, Port1). In addition, no other device can use any of User A's aliases. If User A's 'primary' port goes out of service, establishing connections to User A will be taken over by the 'standby' port (SW2, Port 1) without incident since User A is restricted to SW2, Port1.

Initially, User B is seen on its 'primary' port (SW2, Port 2). All connections to and from User B are established through its 'primary' port. The ports on SW2 are enabled, the port on SW3 is not, so User B is restricted to the ports on SW2 to which it is connected (Port 2). If User B's 'primary' port goes out of service, establishing connections to User B will be taken over by its 'standby' port. In this case, connections to and from User B may be unpredictable since User B is not restricted to SW3, Port1 and any of its aliases could be assigned to another device resulting in a conflict between two or more users contending for the same alias.

Multicast View

The Multicast View of the Switch Properties Window provides receiver information about IP Multicast groups associated with the selected switch ([Figure 7-5](#)). You can also add or delete receivers using this window.

Figure 7-5. Switch Properties (Multicast)

- **Group** - IP Multicast group name.
- **Port** - Access port number.
- **Inclusion** - Include or Exclude.
 - **Include** - Allow IP Multicasts
 - **Exclude** - Do Not allow IP Multicasts
- **Add/Delete** - Since Multicast is port-based, **Add** and **Delete** let you include or exclude certain or all IP Multicast groups on certain or all ports of a switch.

Delete a Receiver

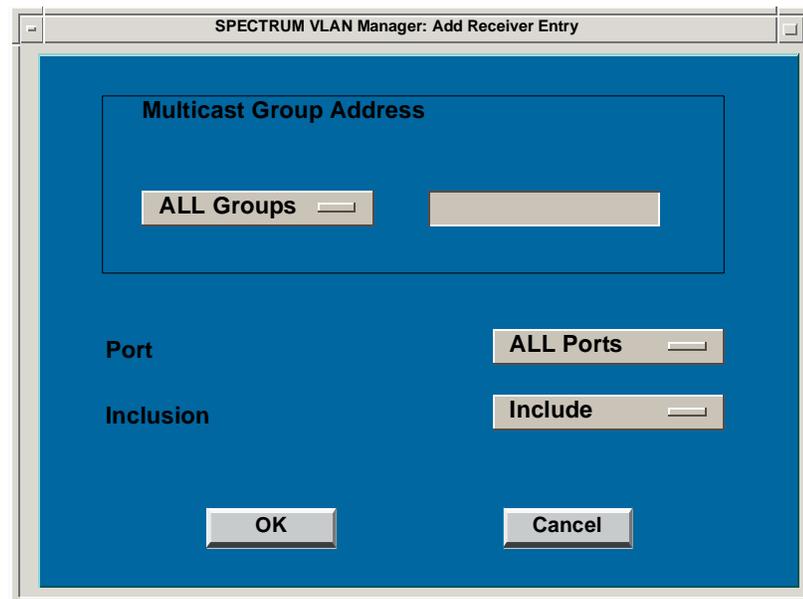
To delete a receiver:

1. Select the receiver you want to delete and then click **Delete**.

Add a Receiver

To add a receiver:

1. Click **Add** from the **Switch Properties** —> **Multicast** window. The Add Receiver Entry window is displayed (Figure 7-6).

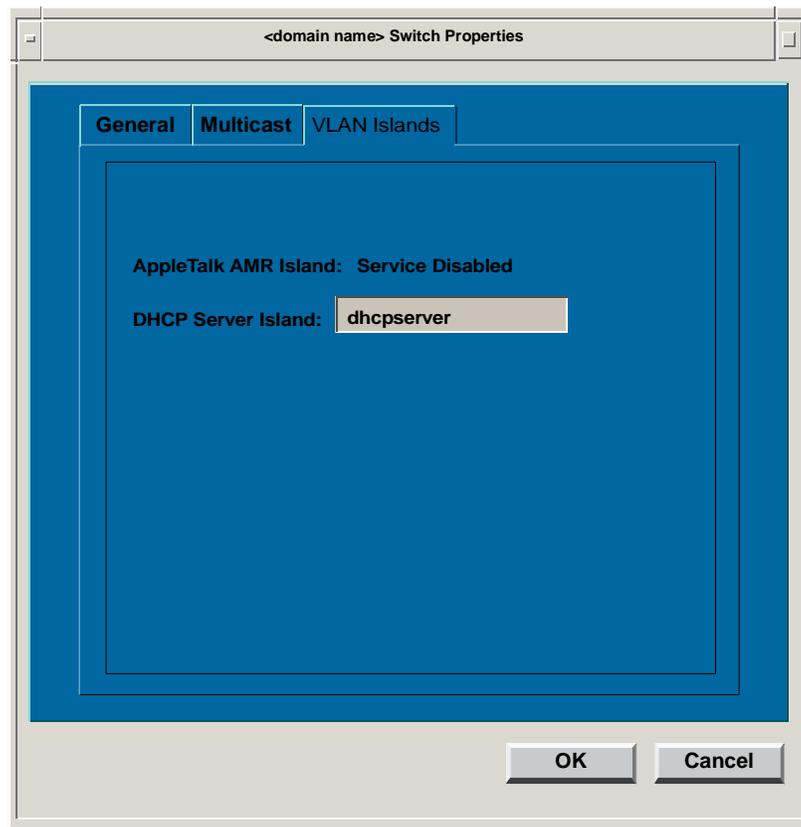
Figure 7-6. Add Receiver

2. Select the Multicast group address to which you want to add a receiver. You may select the “default”, **All Groups**, or select **Custom** or **IGMP Groups** from the drop-down list. If you select **Custom**, enter the IP Multicast address of the group.
3. Select the port you want to add as a receiver to the group you selected in the previous step. You may select the “default”, **All Ports**, or select a port from the drop-down list.
4. Select a policy: **Include** or **Exclude**. If you select **Include**, IP Multicasts will be allowed from the Multicast Group Address to the Port you selected. If you select **Exclude**, IP Multicasts will not be allowed from the Multicast Group Address to the Port you selected.
5. Click **OK** to accept changes and close the window or click **Cancel** to dismiss the window without making changes.

VLAN Islands View

The VLAN Islands View of the Switch Properties Window displays the VLANs being used for AppleTalk AMR Islands and DHCP Server Islands (Figure 7-7) of the selected switch. In addition, this view allows you to change the name of the Appletalk AMR VLAN or DHCP Server VLAN.

Figure 7-7. Switch Properties (VLAN Islands)



- **AppleTalk AMR Islands** - Displays the status of this service (enabled or disabled) as configured in the AMR tab of the Domain Properties Window (see *AMR Properties*, on page 6-21, for more information). If the field states “Service Disabled”, the service is not enabled. If enabled, the name of the AppleTalk AMR VLAN will appear in an editable field. The default name for the AppleTalk AMR VLAN is `appletalk`. To change the name of the VLAN, simply click in the field and enter the new name. The VLAN will be created when an AppleTalk packet is processed on the switch.



Default AppleTalk AMR VLANs will appear in the AMR VLANs folder. Customized AppleTalk AMR VLANs, which are specified via the VLAN Islands tab of Switch Properties will appear in the VLANs folder.

- **DHCP Server Islands** - Displays the status of this service (enabled or disabled) as configured in the Services tab of the Domain Properties Window (see *Services*

Properties, on page 6-22, for more information). If the field states “Service Disabled”, the service is not enabled. If enabled, the name of the DHCP Server VLAN will appear in an editable field. The default name for the DHCP Server VLAN is dhcpserver. To change the name of the VLAN, simply click in the field and enter the new name. The VLAN will be created on the switch and the VLANServer will create the model so you can add the DHCP server to the VLAN.

These values can be seen for all switches in the domain in Domain Details (See *Domain Details* on Page 6-30.).



VLANs which have been configured as DHCP Server VLAN Islands or AppleTalk AMR VLAN Islands should not be deleted.



If AppleTalk AMR or DHCP Server Island features are enabled but the firmware doesn't support the Island feature, the fields in the VLAN Islands tab will not be editable but they will indicate the VLANs being used by default (ie. appletalk, dhcpserver).

Displaying Switch Details

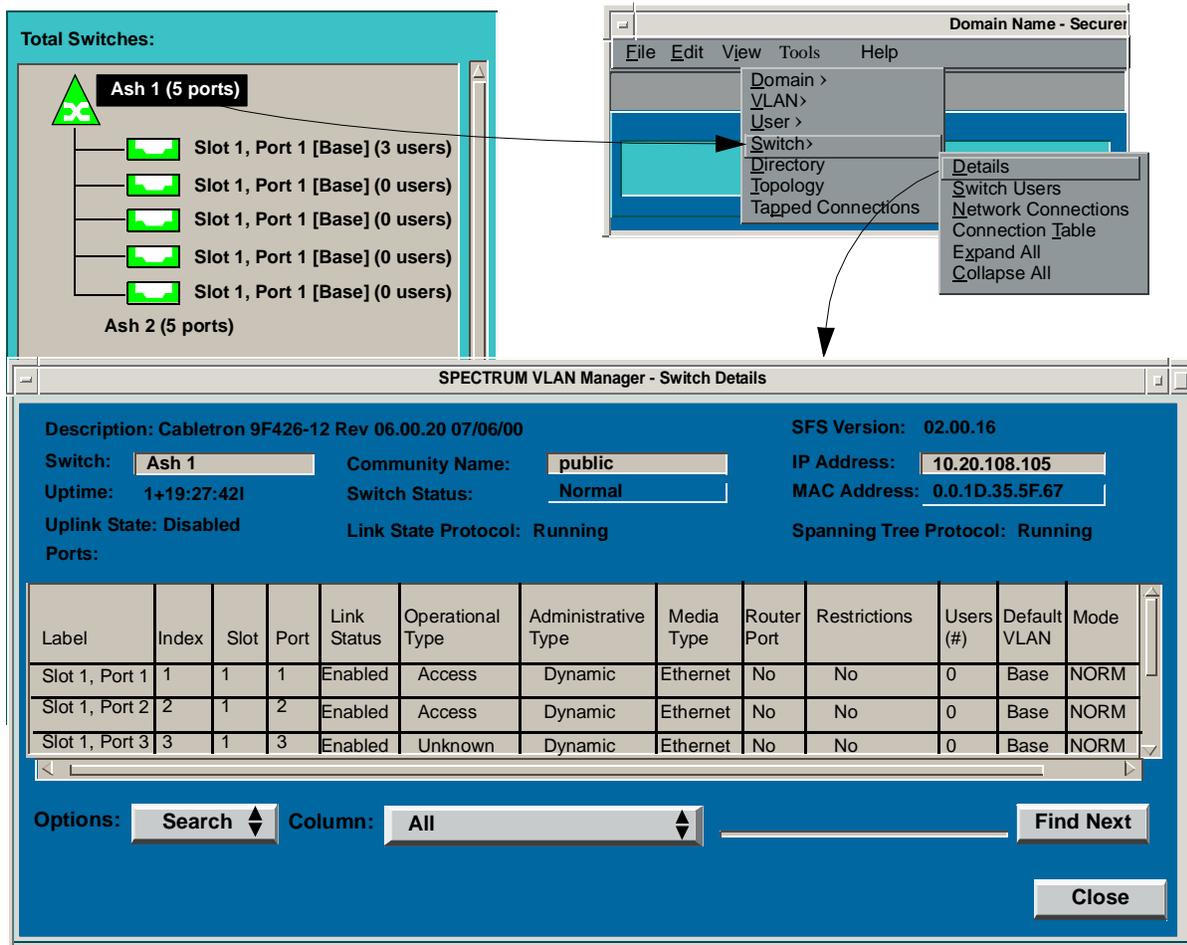
The Switch Details window provides information about each port of the selected switch. In addition, the Switch Details window gives you the opportunity to edit certain fields. The Search/Filter feature accessible from this window lets you find a particular port quickly without having to scroll through the entire list.

To display switch details (Figure 7-8):

1. Select a switch from the switch pane.
2. Select **Details** from the **View >Switch** menu, click  from the Toolbar or use the Switch pop-up. The SPECTRUM VLAN Manager - Switch Details window is displayed.

The Switch Details window contains general information fields and **Ports** fields. General information fields provide information describing the characteristics of the selected switch. **Ports** fields provide specific information about each port on the selected switch.

Figure 7-8. Displaying Switch Details



General Information Fields

- **Description** - Provides firmware/hardware version information for the selected switch.
- **SFS Version** - Version of the SecureFast Services firmware component running on the switch.
- **Switch** - Name of the switch for which port information is being displayed. If DNS is not being used, the switch's IP address is displayed, or the name you have assigned.
- **Community Name** - Community name being used to communicate with the switch.
- **IP Address** - Network address of the switch.

- **Uptime** - Length of time the switch has been in operation since its last initialization. Time is shown in days, hours, minutes, and seconds. For example, 2+14:09:45 represents 2 days, 14 hours, 9 minutes, and 45 seconds.
- **Switch Status** - Normal, Contact Lost, Major, or Supressed.
- **MAC Address** - Physical address of the switch.
- **Uplink State** - Indicates whether or not the switch is configured as an uplink switch. If it is an uplink switch, the Uplink State column indicates whether the switch is a Tier 1 or Tier 2 uplink switch. If it is not an uplink switch, the state is Disabled. See [Expanding a Domain Using Uplink Switching](#) on [page 6-34](#) for more information on uplink switching.
- **Link State Protocol** - Indicates the status of Link State Protocol on the switch. Possible values are: Running, Halted, Pending, Faulted, Not Started, Invalid, and Unkown. The default is Running. For switches configured as uplink switches, Not Started or Halted is displayed.
- **Spanning Tree** - Indicates the status of Spanning Tree Protocol on the switch. Possible values are: Running, Halted, Pending, Faulted, Not Started, Invalid, and Unkown. The default is Running. For switches configured as uplink switches, Not Started or Halted is displayed.

Ports Fields

The Ports List displays information about all ports on the switch. Each entry in the Ports List provides information associated with a specific port. A scroll bar to the right of the table lets you to scroll through the table.

- **Label** - Name assigned to a port. Default labels are **Slot x, Port x** for physical ports, **Port Index x** for logical ports, and **INB** for INB ports. You can change these names to something more meaningful to you by using the [Editing a Port Label](#) feature.
- **Index** - The number assigned to a logical port.
- **Slot** - The physical slot a board is plugged in to. This only applies to chassis ports. The slot number will be omitted for logical ports.
- **Port** - The physical port number.
- **Link Status** - **Enabled** > Link detected or **Disabled**> Link not detected.
- **Operational Type** - Type of port this port is acting as: Access, Access Only, Downlink Flood, Flood, Going Access, Hybrid, Network, Network Only, Other, Redundant Access Primary, Standby, Standby Access Redundant Unknown (the Administrative Type is set to "Redundant" but the Link Status is down), Standby FCL Conflict, Standby Looped Port, Standby RA Nonprimary, Unknown, Uplink, or Uplink Flood.
- **Administrative Type** - Function you have designated this port to provide.

- Dynamic (Default) (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)). If set to Dynamic, the port will automatically be designated as either an access port or a network port. Refer to [Physical Window Pane, on page 3-21](#) for explanations of access and network ports.
 - Interdomain (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)). Use this type only if the port connects to a different domain.
 - Network (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)).
 - Uplink (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)).
 - Downlink (see [Expanding a Domain Using Uplink Switching, on page 6-34](#)).
 - Redundant (see [Configuring Dynamic Redundant Access Ports, on page 8-28](#)).
 - Uplink Flood (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)).
 - Flood (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)).
 - Standby (see [Configuring Dynamic Redundant Access Ports, on page 8-28](#)).
 - Endstation (user). Use this type for endpoints connected to the port, or use Dynamic to have the switch use the appropriate type automatically.
- **Media Type** - Valid entries are: **Ethernet, FDDI, ATM, Token Ring, WAN, INB, Host Control, Host Data, ATM SVC, ATM PVC, Unknown, ATMF LEC, ATMF PVC, ATMF SVC**.
 - **Router Port** - Router connected to the port: **Yes** or **No**.
 - **Restrictions** - **Yes** or **No**.
 - **Yes** - Port is restricted to one or more specified MAC addresses.
 - **No** (default) - Port is not restricted to one or more specified MAC addresses.
 - **Users (#)** - Number of users learned on the port.
 - **Default VLAN** - Default VLAN for the port.
 - **Mode** - Mode assigned to a port: NORMAL or LOCKED.
 - LOCKED - All users attached to a locked port will only be members of the port's default VLAN.
 - NORMAL - All inherited users will be members of the port's default VLAN. All statically assigned users will be members of the VLAN(s) to which they have been assigned.
 - **Self ARP Packet Learning** - For access ports, indicates whether or not Self ARP Packet Learning is **Enabled** or **Disabled** on the port. If the cell in the table is empty, the port is not an access port, and this attribute does not apply. For more information on Self ARP Packet Learning, see [Page 8-5](#) of the [Port Properties](#) section of Chapter 8.
3. Click **OK** to accept changes and close the window, **Apply** to accept changes and leave the window open, or **Cancel** to dismiss the Switch Details dialog box without making changes.

Using Search/Filter

Use the **Options** button to find a particular port. You can search or filter by any table column. You can also **Filter** by **None**, which returns the table to the non-filtered state.

To use the search/filter:

1. Select **Search** or **Filter** from the **Options** list and the selection criteria from the **Column** list.
2. Click anywhere in the text box to the right of the **Column** selections, and then enter the text to be matched.
 - **Search** finds and highlights the first instance of a port that matches the search criteria as it is entered. Click **Find Next** to find the subsequent instances of ports that match the same criteria.
 - **Filter** selectively eliminates entries from the **Ports** list that do not match the criteria entered. Ports that match the filter criteria are displayed.

Downloading Firmware to a Switch

You can download and upgrade SecureFast VLAN firmware to your SecureFast switches using this menu option. Select **TFTP Download** from the **Tools** menu. Refer to the *SPECTRUM VLAN Manager Installation Guide* for detailed information about this procedure.

Forcing a Switch to be Polled Immediately

A switch poll normally occurs at the interval set in the domain discover or domain configure window. Polling looks for physical changes to your switch, for example, learning a new endstation on a switch port or noticing that a user has moved. **Poll Switch**, which is available from the **Edit >Switch** menu, lets you force the VLANServer to poll a switch immediately. You use this feature if you make physical changes to your network and don't want to wait until the next scheduled poll to see the results.

When you click **Poll Switch**, the selected switch's delta (change) tables are read by the VLANServer to determine what physical changes have occurred since the last poll. The normal poll interval is *not* reset after a forced poll. If the poll interval for a switch is set for five minutes and you force a poll after two of the five minutes have elapsed, the next poll will occur in three minutes, *not* five minutes.

If successful, the VLAN Manager will display the "Poll Switch Successful" message.

Forcing a Switch to Reconfigure Immediately

Reconfigure Switch, which is available from the **Edit >Switch** menu, lets you enforce the VLANServer's database on a switch. Clicking **Reconfigure Switch** causes the VLAN Manager to look at data in the selected switch. If the data differs from its corresponding data in the VLANServer database, the switch's data is updated to match the data in the VLANServer's database. For example, if a switch has User A as a member of VLAN 'Red' and the VLANServer has User A as a member of VLAN 'Blue', then the Reconfigure command will force the switch to update its data so that User A is a member of VLAN 'Blue'. If successful, the VLAN Manager will display the "Reconfigure Switch Successful" message.

Rebooting an Individual Switch

VLAN Manager lets you reboot a switch from the user interface without having to physically push the reset button on the switch. This is particularly convenient when upgrading firmware on a switch.



Rebooting a switch will cause the switch to interrupt processing packets and should be done with care.



You can also reboot all switches in a domain. Refer to *Domain Details*, on page 6-30.

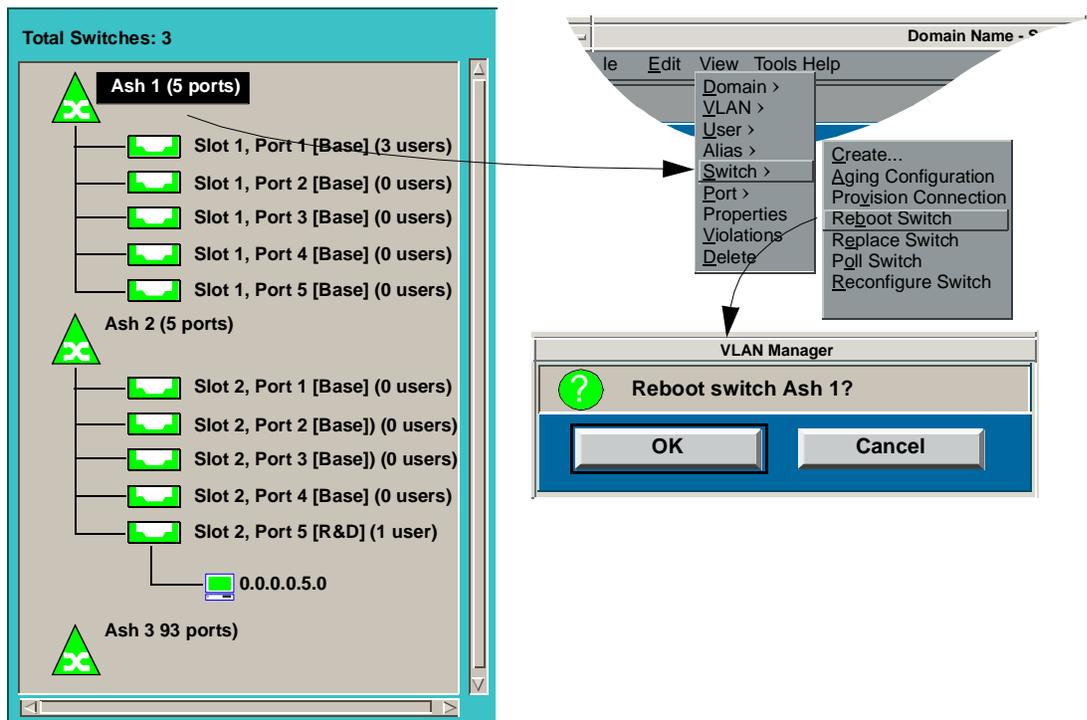
To reboot an individual switch:

1. Select the switch you want to reboot from the VLAN manager Main view. The selected switch must have Green operational status.
2. Select **Reboot Switch** from the **Edit >Switch** menu (Figure 7-9). If the Enable Dialogs (Confirmations) preference is set (refer to *Main Preferences*, on page 5-3), a dialog box is displayed, asking for confirmation to reboot the selected switch. Click **OK** to reboot the switch or **Cancel** to return to the VLAN Manager window without making any changes. If successful, the “Switch reboot request successful - reboot will occur momentarily” message is displayed.



To verify the switch has been rebooted, check the switch Uptime in the Domain Details view or Switch Details view. A message also gets written to the Control Panel. It gives the date and time of the switch reset.

Figure 7-9. Rebooting an Individual Switch



Replacing a Switch

When you physically replace a switch in a domain, address information about the original switch is not cleared from the alias tables of the other switches in the domain. Even if you configure the new switch with the IP address of the switch that was replaced, the alias tables of the other switches in the domain will still contain the MAC address of the switch that was replaced, not the MAC address of the new switch.

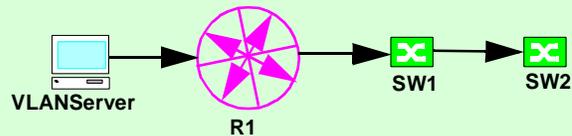


With one exception, switch module replacement must match the failed module exactly. The exception is the 9E423-24. You can replace a 9E423-24 with another 9E423-24 or a 9E423-36.

Replace Switch, which is available from the **Edit >Switch** menu, clears the address information of the switch that was replaced from the alias tables of all switches in a domain. The new switch's address information is written into the alias tables of the other switches in the domain as they learn about the new switch.



In addition to using Replace Switch, you have to manually clear the ARP cache on the VLANServer workstation and routers in the switch's path. For instance, if your domain looked like the one shown below, and you replaced SW2, you would use Replace Switch on SW2 to clear the alias table for SW1 and manually clear the ARP cache for R1 and the VLAN Server workstation.



If you replace a switch with a switch of a different type (other than the exception described above), perform the following steps:

1. Remove the old switch.
2. Delete the switch.
3. Install the new switch.
4. Create the switch.
5. Manually configure customized settings such as locked ports, network ports, and default VLANs.

Switch Protocol Control

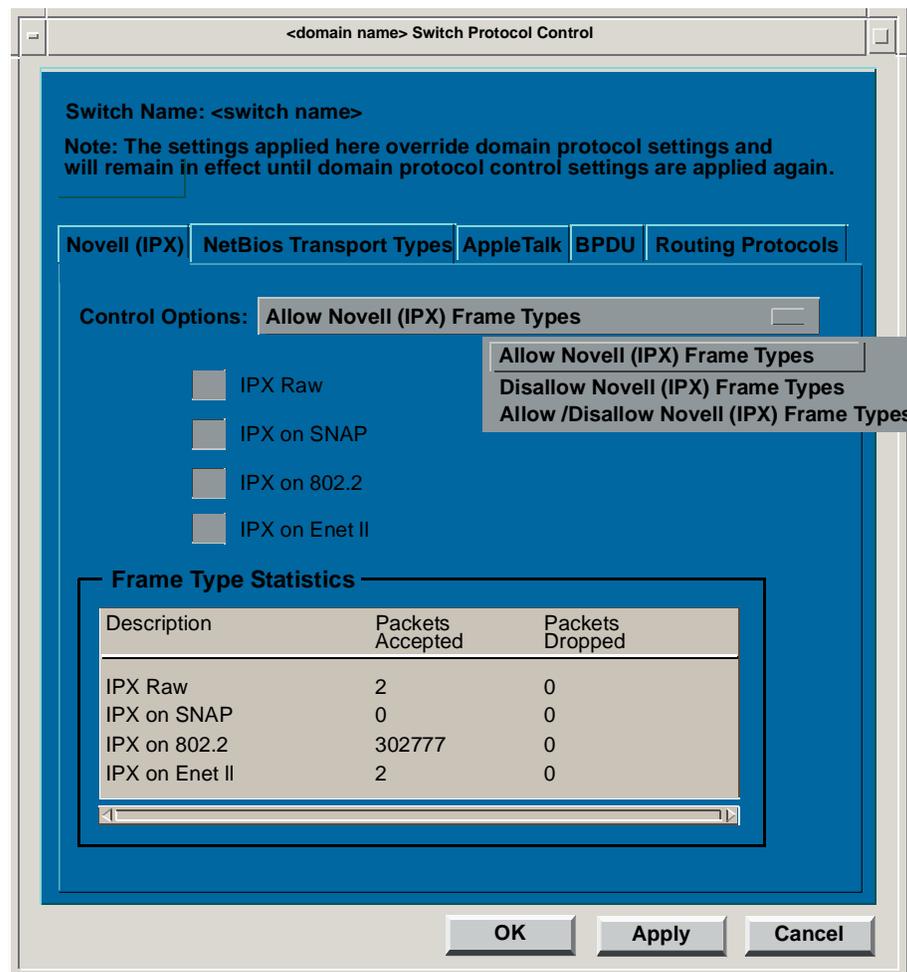


1. By default, all protocols and protocol frame types are enabled for a switch. IP cannot be disabled.
2. Protocol policy set at the switch level always overrides protocol policy set at the domain level unless Domain Protocol Controls are applied afterwards.

To set switch protocol policy:

1. Select a switch from the VLAN Manager's Main window.
2. Select **Switch Protocol Control** from the **Tools** menu to display the Switch Fabric Policy Configuration window (Figure 7-10). From this window, you can enable or disable any of the protocols and protocol frame types for the selected switch. Frame type statistics are shown for each frame type.

Figure 7-10. Setting Switch Policy



3. Click the tab that corresponds to the protocol you want to configure (e.g., Novell (IPX), NetBIOS, AppleTalk, IP, BPDU, Routing).
4. Select a control option from the **Control Options** drop down list.

5. If you selected **Allow/Disallow <protocol> Frame Types** from the control options drop down list, allow/disallow frame types by clicking the button that corresponds to the frame type you want to enable (recessed) or disable (raised).
6. Select **Apply** to accept configuration changes and leave the Properties window open, **OK** to accept changes and close the window, or **Cancel** to close the window without making changes. To display another tabbed page, click the corresponding tab.

Managing Ports

This chapter provides step-by-step instructions for performing port administration tasks using SPECTRUM VLAN Manager's graphical user interface. It also contains reference information and helpful tips to help you perform these tasks.

Overview

Port information displayed in VLAN Manager windows is divided into two categories: Physical and Logical.

- **Physical** - The slot in a chassis into which a board is plugged and the physical port on the front panel of a board.
- **Logical** - A Port Index (i.e., a virtual port assignment).

The Switch Details window provides a correlation between the two types of ports.



If you use a MIB management tool other than the VLAN Manager application, you will only see logical port designations.

You manage a port using the **Edit >Port** menu selections, the switch port pop-up menu, Port Properties, and the **Tools >Port Redirect** menu selection.

- You can use the **Edit >Port** menu selections to unlock a port, set or unset a port to be a router port, and set and unset a port to be a redundant port.
- You can use the switch port pop-up menu to lock and unlock a port, set or unset a port to be a router port, set and unset a port to be a redundant port, and view or set port properties.

- You can use Port Properties to edit General, VLAN, Multicast, and Restrictions properties.
- You can use the **Tools >Port Redirect** menu selection to remap a port's data stream to another port.

Port Menus

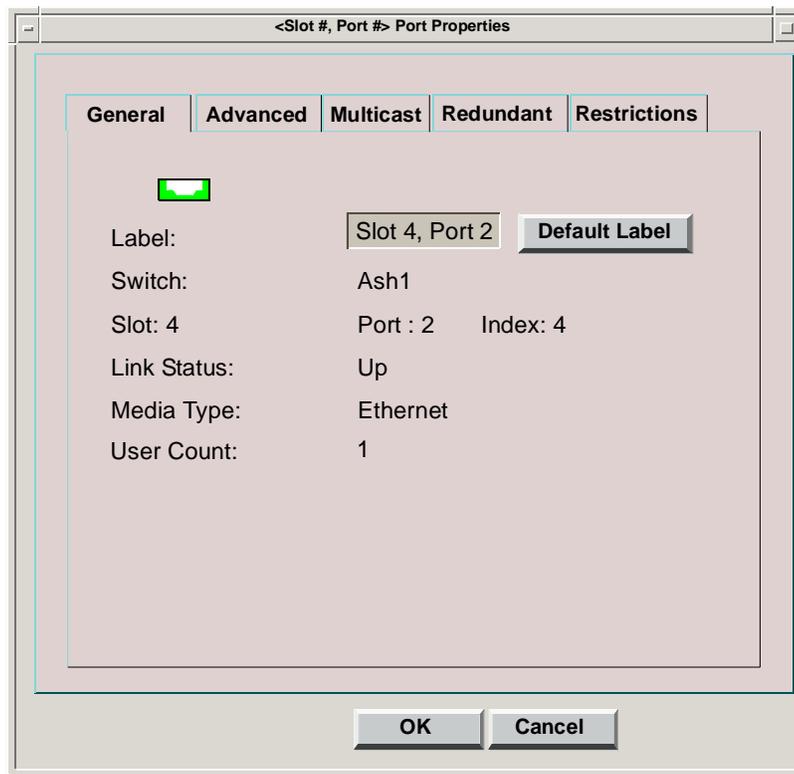
The Port menu selections are **Router Wizard**, **Toggle Lock/Unlock**, **Set/Unset Router Port**, and **Set/Unset Redundant Port**.

- **Router Wizard** - Lets you configure a router port.
- **Toggle Lock/Unlock** - Lets you lock or unlock a port. If the port to which an endpoint is connected is LOCKED, that endpoint will assume membership in the Default VLAN for that port, regardless of any previous membership.
- **Set/Unset Router Port** - Lets you set and unset a port to be a router port. Once the port is toggled, layer 3 learning/discovery is disabled beyond the router's MAC address.
- **Set/Unset Redundant Port** - Lets you configure endpoints within a VLAN domain to be connected to more than one switch access port.

Port Properties

To view and/or edit port properties, select a switch port, use the right mouse button to bring up the port pop-up menu, and then select **Properties** or choose **Properties** from the **Edit** menu. The Properties window appears, with the **General** tab open.

Figure 8-1. Port Properties - General Tab

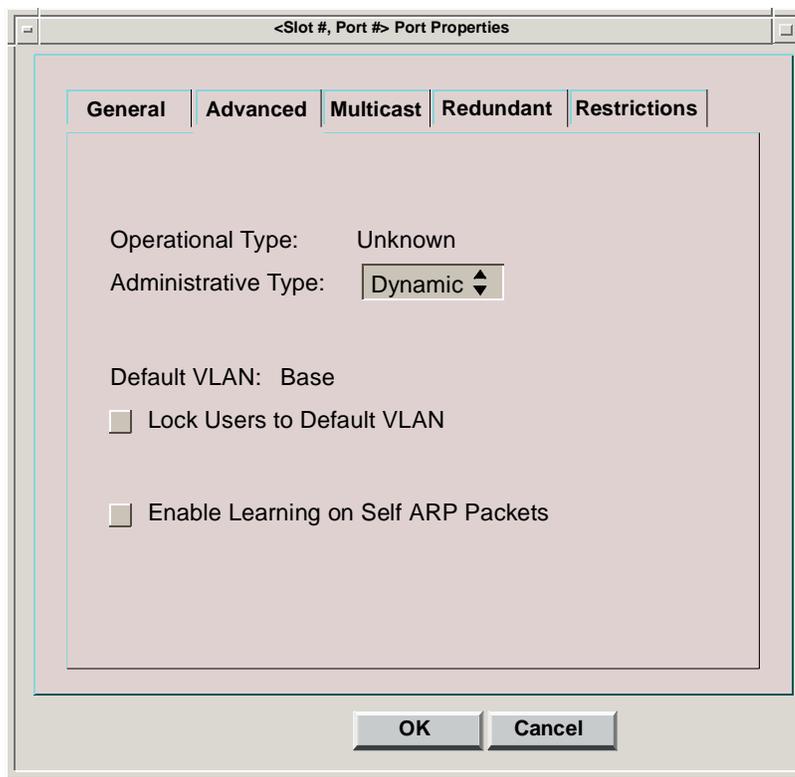


The Port Properties window consists of the **General**, **Advanced**, **Multicast**, **Restrictions**, and, if the port is configured as a redundant access port, **Redundant** tabs. If a tab does not apply to the selected port, that tab is not displayed.

- **General** Tab - Provides the following information about the selected switch port:
 - **Label** - Name assigned to a port. Default labels are Slot x, Port x for physical ports and Port Index x for logical ports. You can change these names to something more meaningful to you by entering the name you want into the **Label** text field. To change to the default name, click **Default Label**.
 - **Switch** - Name of the switch.

- **Slot** - Numerical identifier of the slot where the switch is installed in the chassis. Logical ports display 0.
- **Port** - Physical port number. This only applies to physical ports. The port number will always be 0 for logical ports.
- **Index** - Logical number assigned to a port.
- **Link Status** - Up or Down.
- **Media Type** - Ethernet, FDDI, ATM, Token Ring, WAN, INB, ATM SVC, ATM PVC, Unknown, ATMF LEC, ATMF PVC, or ATMF SVC.
- **User Count** - Number of endstations attached to this port.
- **Advanced Tab** - Provides the following information about the selected switch port. Some of the information is editable.

Figure 8-2. Port Properties - Advanced Tab



- **Operational Type** - Type of port this port is acting as: Access, Access Only, Downlink Flood, Flood, Going Access, Hybrid, Network, Network Only, Other, Redundant Access Primary, Standby, Standby Access Redundant Unknown (the Administrative Type is set to "Redundant" but the Link Status is down), Standby FCL Conflict, Standby Looped Port, Standby RA Nonprimary, Unknown, Uplink, or Uplink Flood.
- **Administrative Type** - Function you have designated this port to provide.
 - Dynamic (Default) (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)). If set to Dynamic, the port will automatically be designated as either an access port or a network port. Refer to [Physical Window Pane, on page 3-21](#) for explanations of access and network ports.
 - Interdomain (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)). Use this type only if the port connects to a different domain.
 - Network (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)).
 - Uplink (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)).
 - Downlink (see [Expanding a Domain Using Uplink Switching, on page 6-34](#)).
 - Redundant (see [Configuring Dynamic Redundant Access Ports, on page 8-28](#)).
 - Uplink Flood (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)).
 - Flood (see [Configuring Tier 1 Uplink Switching, on page 6-35](#)).
 - Standby (see [Configuring Dynamic Redundant Access Ports, on page 8-28](#)).
 - Endstation (user). Use this type for endpoints connected to the port, or use Dynamic to have the switch use the appropriate type automatically.
- **Default VLAN** (Access Ports only - unavailable for other port types) - VLAN to which endstations on this port will be assigned unless otherwise specified. For detailed information about AMR VLAN properties, refer to [AMR VLAN Administration, on page 9-19](#).
- **Lock Users to Default VLAN** (Access Ports only - unavailable for other port types) - Enables you to lock all users on the selected port to the port's default VLAN.
 - Locked** ()- All users attached to a locked port will only be members of the port's default VLAN. A lock icon is displayed to the right of a locked port.
 - Unlocked** ()- All inherited users will be members of the port's default VLAN. All statically assigned users will be members of the VLAN(s) to which they have been assigned.
- **Enable Learning on Self ARP Packets** - Allows you to enable and disable Self ARP Packet Learning on an Access Port. This field will be unavailable if the selected port is not an Access Port, or if the firmware of the switch where the Access Port is located does not support Self ARP Packet Learning.

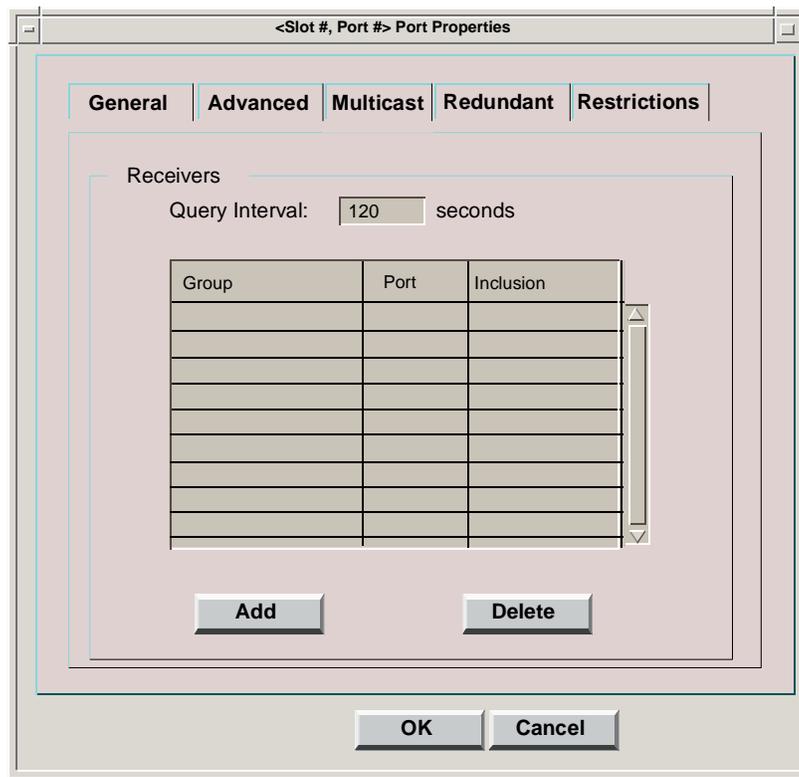
A Self ARP is an IP ARP packet where the source and IP addresses are the same, used to inform other devices of an IP/MAC which the source intends to use. Self ARP Packet Learning is commonly used in redundant server configurations, where the devices have different MAC addresses but a common IP address.

When the primary server fails and the secondary server takes over, the secondary sends out a Self ARP as notification that the common IP address is now bound to the secondary's MAC address.

If Self ARP Packet Learning is Enabled (button depressed), the port will learn the Layer 3 address from the self-originating ARP packet. If it is Disabled (button not depressed), the port will not learn the Layer 3 address from the self-originating ARP packet. The default is Disabled.

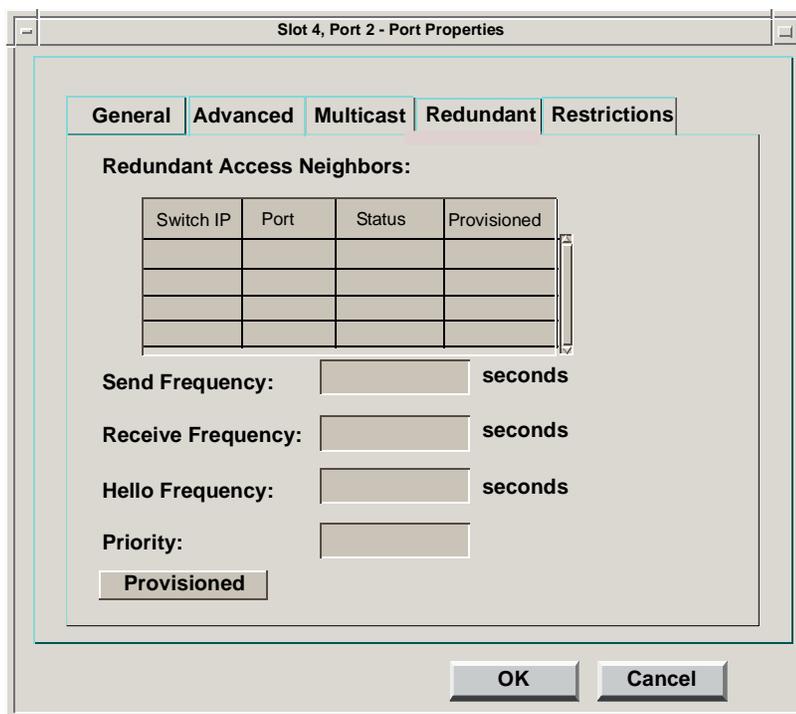
- **Multicast Tab** - Displays the IP multicast query interval setting and enables you to change it. For more information about IP Multicast properties, refer to [Editing Multicast Properties](#), on page 12-3.

Figure 8-3. Port Properties - Multicast Tab



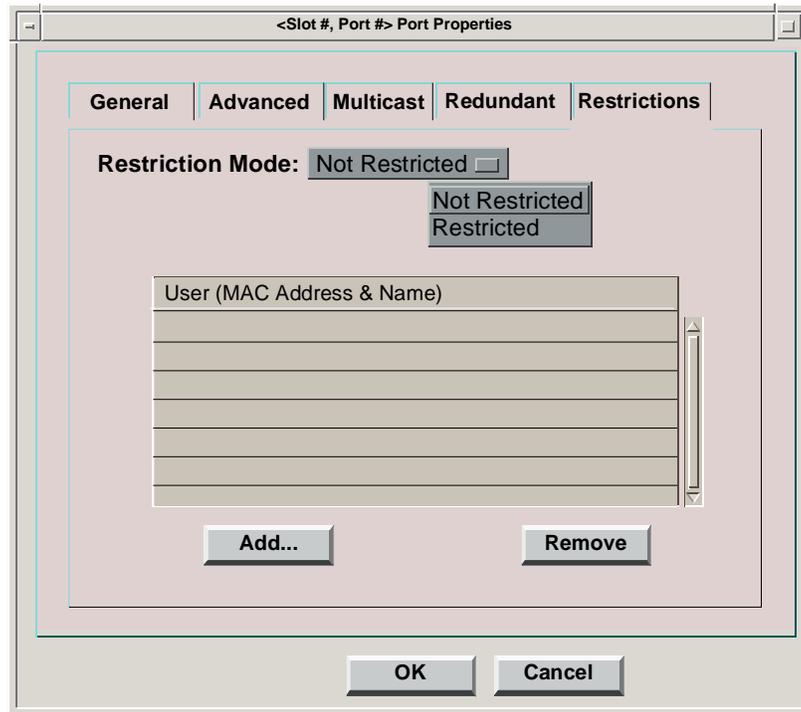
Redundant Tab - This tab appears only if the selected port is configured as a redundant access port. It provides a table of all the selected port's redundant access neighbors, including each neighbor port's **Switch IP** address, its **Port** number, its **Status** (Primary or Secondary), and whether or not it is **Provisioned**. The **Frequency** and **Priority** fields also apply to the selected port. You can also provision redundant access ports from this tab. For more information, see [Configuring Dynamic Redundant Access Ports, on page 8-28](#).

Figure 8-4. Port Properties - Redundant Tab



- **Restrictions** Tab - Indicates whether or not a port is restricted, and if it is, the MAC address(es) to which it is restricted. The User table is editable. If restricting a port is not supported by switch firmware, “Not Supported” is displayed. For more information see *Restricting a Port*, on page 8-42.

Figure 8-5. Port Properties - Restrictions Tab



Editing a Port Label

To edit a port label:

1. Select the port you want to re-label.
2. Select **Properties** from the **Edit** menu or from the Port pop-up menu. The **General** Port Properties tabbed page is displayed.
3. Enter the new port label into the **Label** text field (maximum length = 32).

4. Click **OK** to change the port name and close the Port Properties tabbed folder or **Cancel** to dismiss the Port Properties tabbed folder without making any changes to the port's label.



A port label is used throughout the VLAN Manager application. If the default port labels are used (Slot x, Port x), they will be used in every window where port information is shown. If you re-label a port, that label will be used in every window where port information for that port is shown.

Configuring a Router Port

Configuring a port as a router port facilitates communication with a router by providing switches in a domain with data needed to process connection requests destined for subnets that are internal or external to the SecureFast domain. The way in which connection requests are processed depends on the information you provide in the Router Wizard. The steps used by a switch to process connection requests is described in [Flow of Events](#).

Flow of Events

- Use the Router Wizard to define subnets/routes of the domain.
- VLANServer writes the internal, external, and default gateway data into all of the switches in the domain.
- As endstations transmit packets on the network, ARP broadcasts are intercepted and destination IP addresses are attempted to be resolved in the switch's local directory.
- If resolved, the MAC address found is used to send a unicast ARP request to the endpoint.
- If the specific entry is not resolved and since there are entries in the switch's Subnet Resolve Table, the IP address in the ARP request is ANDed with the defined subnet mask and the result is looked up in the subnet resolve table of the Ingress switch.
- If the match is to an internal entry, a remote resolve is sent to the other switches in the domain since they service the subnet.
- If the specific IP address is resolved, the endpoint's MAC is used in a unicast ARP request to the destination.
- If the specific IP address is not resolved, the ARP request is flooded.
- If the match is to an external entry, the router MAC address associated with that entry is used in the unicast ARP request.
- If no internal or external match is made, the MAC address of the default gateway is used in the unicast ARP request.

Using the Router Wizard

The Router Wizard is used to configure a port to be a router port. You can configure one router per port or multiple routers per port.

To launch the Router Wizard:

1. In the VLAN Manager Main window, select the port.
2. Use the right mouse button to bring up the port pop-up menu, or go to the **Edit >Port** menu.
3. For a port that has not yet been configured as a router port, select **Set/Unset Router Port**. For a port already set to be a router port, select **Router Wizard**. In either case, the Router Wizard Summary window ([Figure 8-6](#)) opens.

Figure 8-6. Router Wizard Summary

Router Wizard Summary

Port Information
 Switch IP: 192.168.180.107
 Port: 1
 Layer Three Learning: **Enabled** Disabled
 Multicast Proxy Address: 5.4.3.2

Domain Information
 Domain: 51
 Subnet Mask: 255.255.255.0
 Default Gateway: 0.0.C.18.C8.6E

Protocol Information
 Enable OSPF Multicast
 Enable VRRP Multicast

Internal Subnets
 To change the internal subnet list, modify a Router List entry

MAC Address	Router IP Addresses	Default Gateway (Yes/No)	External Subnets	Router Restricted (Yes/No)
0.0.C.2.73.E9	192.168.180.101	No	192.168.170.0	No
0.0.C.5.78.A3	192.168.181.101	No	192.168.170.0	No
0.0.C.7.94.E2	192.168.182.101	No	192.168.170.0	No

Buttons on the right: OK, Apply, Add, Delete, Modify, Exit

The Router Wizard's Summary window provides you with a snapshot of all routers currently configured for the selected port. You can configure Multiple routers on a port. Port settings are shown in the Port Information box located in the upper left of the window. Domain settings are shown in the Domain Information box located in the center of the window. Internal Subnets are displayed in the Internal Subnets list, located in the right side of the window. Router settings are shown in the Router List.

In the Protocol Information box, you can enable or disable the multicast groups for the OSPF and/or VRRP protocols (see *Enabling OSPF Multicast*, on page 8-45 and *Enabling VRRP Multicast*, on page 8-47).

Buttons located on the right side of the Router Wizard Summary window provide you with the following router configuration options:

- Click **Exit** to dismiss the Summary window without applying any changes.
- To add a router to this port, click **Add**. Step 1 of the Router Wizard or the MAC Selection window is displayed.
- To delete router configurations from this port, select the MAC address of the router from the Router List, and then click **Delete**. The selected router, and its corresponding subnets, are removed from the Router List, the switch, and the VLANServer database.
- To modify the settings for a router in the Router List, select the MAC address of the router for which you want to modify the settings, and then click **Modify**. Step 1 of the Router Wizard is displayed.

- To apply all changes made during this Router Wizard session and leave the Summary window open, click **Apply**.
- To apply all changes made during this Router Wizard session and close the Summary window, click **OK**.



1. Configuring a port set to be a router port using the Router Wizard is not required, however, if configured correctly, doing so will help optimize network performance.
2. If you use the Router Wizard to configure the router to be used as the Default Gateway for a domain, you must also configure all non-Default Gateway routers in the domain as well.

Step 1

1. If not supplied (or incorrect), enter the MAC address of the router connected to the port you are configuring (Figure 8-7). Use the “.” character as an address delimiter, not the “:” character.



1. If this router’s MAC address has not been discovered (e.g., the router has not been physically connected to the network yet), or if multiple MAC addresses have been learned on the port, you will have to manually enter the router’s MAC address or use the MAC Selection View.
2. If this MAC address already exists on another port in the domain (or any domain being managed by the VLANServer), the router configuration will fail. The following error message will be displayed: Router Configuration failed for MAC address x.x.x.x.x.x. Error is: User already exists on another port.

Figure 8-7. Router Configuration - MAC Address



2. Click **Cancel** to exit the Router Wizard and return to the Summary or **Next** to proceed to the next step.



The Router Wizard cannot be launched if the Discovery Wizard is running. In addition, two or more instances of the Router Wizard cannot be running at the same time.

Step 2

Figure 8-8. Router Configuration - Router IP/Subnet Mask

A screenshot of a Windows-style dialog box titled "<switch><slot><port>- Router Wizard: Step 2". The dialog has a blue border and a grey background. On the left is a vertical panel with a wizard character illustration. The main area contains the text "What is the primary IP Address and subnet mask for this router?". Below this are two input fields: "Router IP:" with the value "192.168.180.1" and "Subnet Mask:" with the value "255.255.255.0". A note below the fields reads: "*By changing the subnet mask you are changing the mask for the whole SecureFast domain." At the bottom are four buttons: "Cancel", "< Back", "Next >", and "Finish".

1. If not supplied or incorrect, enter the 32-bit, IP address of the primary router interface connected to the port you are configuring (Figure 8-8).



The primary IP address of the router connected to the selected port is automatically entered into the Router IP field if the alias has been learned by the switch (i.e., RIP, OSPF, or IGRP is running on the router). If none of those protocols are running, you will have to enter the primary IP address of the router into the Router IP field. Check the configuration of the router to determine the primary IP address.

2. Enter the 32-bit subnet mask address (e.g., 255.255.255.0). This address is ANDed to the Primary IP address to define the network portion of that address.



The subnet mask must be the same for all routers in a domain.

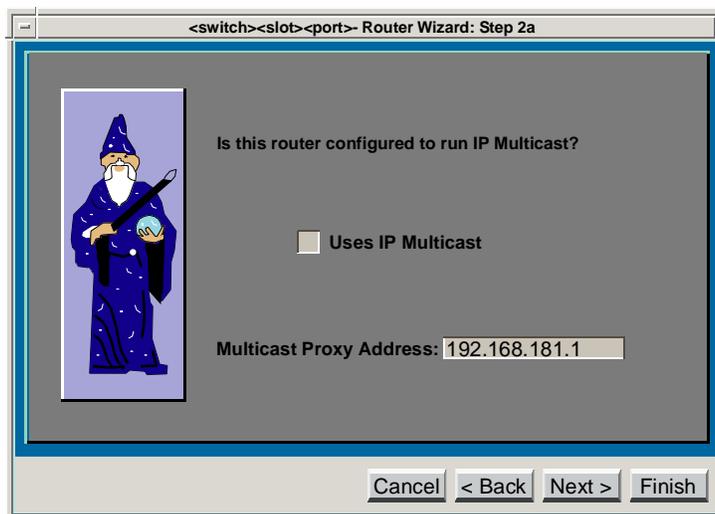
3. Click **Cancel** to exit the Router Wizard and return to the Summary. Click **Back** to return to the previous step, or **Next** to proceed to the next step.

Step 2a



Step 2a will not be displayed if IP Multicast has not been enabled from **Edit >Domain >Properties**.

Figure 8-9. Router Configuration - IP Multicast



1. Choose whether or not you want this router and all routers on this port to run IP Multicast (Figure 8-9).

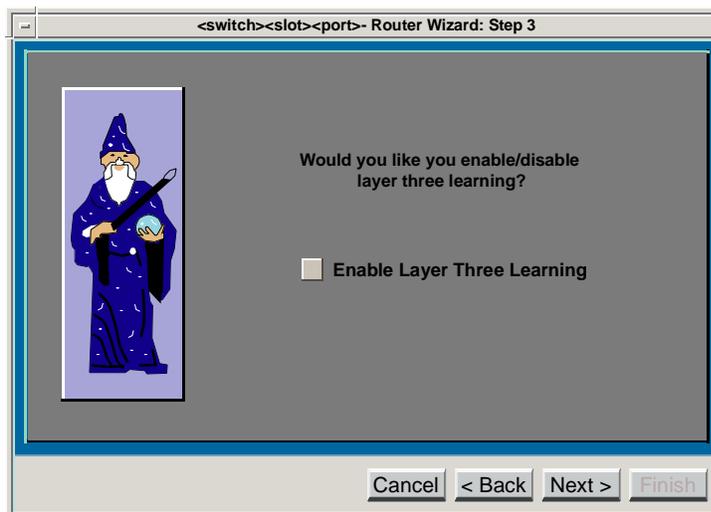
- Uses **IP Multicast** (recessed)- If you set a switch port to support IP Multicast, the switch will forward IP Multicast packets out the router port. You must complete the Multicast Proxy Address text field.
- **Multicast Proxy Address** - This address can be any address between 1.1.1.1 and 254.254.254.254 that is not in use by another device. It is used as the IGMP query address. The switch to which a multicast router is attached serves as a proxy device on behalf of all SecureFast switches and multicast groups in the domain. IGMP (Internet Group management Protocol) membership queries generated by a multicast router are intercepted and processed at the ingress switch port. This switch responds to the queries by transmitting IGMP membership reports for all multicast groups within the SecureFast domain.
- Uses **IP Multicast** (raised) - If you set a switch port not to support IP Multicast, the switch will not forward IP Multicast packets out the router port.

Refer to [Chapter 12, Managing IP Multicast Groups](#) for information about IP Multicast groups.

2. Click **Cancel** to exit the Router Wizard and return to the Summary. Click **Back** to return to the previous step, or **Next** to proceed to the next step.

Step 3

Figure 8-10. Router Configuration - Layer Three Learning



1. Choose whether or not you want to allow layer three learning for this router MAC ([Figure 8-10](#)).

- **Enable** (recessed) - IP addresses for all endpoints on the port will be learned.
 - **Disable** (raised) - No IP addresses for endpoints on the port will be learned.
2. Click **Cancel** to exit the Router Wizard and return to the Summary. Click **Back** to return to the previous step, or **Next** to proceed to the next step.

Step 4

Figure 8-11. Router Configuration - Default Gateway



If switches are added to a domain after the domain's Default Gateway has been configured or if the switches are unreachable at the time the Default Gateway was configured, Default Gateway information will not be written to those switches. If those switches are subsequently configured as the Default Gateway for the domain, there will be no warning indicating that you are configuring two Default Gateways for the domain and network operations will be unpredictable.



1. Choose whether or not you want this router to be the Default Gateway for the current domain (Figure 8-11).



1. Connection requests to subnets not listed in a switch's Subnet Resolve Table are sent to the Default Gateway.
2. There can only be one router MAC specified as the Default Gateway per domain.

- **Default Gateway** (recessed) - If you set this router's MAC address to be the Default Gateway for a domain, connection requests to the subnets shown as internal subnets in the switch's Subnet Resolve Table for that MAC address are processed by the switches in the domain.
 - **Non-Default Gateway** (raised) - If you set this router's MAC address *not* to be the Default Gateway for a domain, connection requests to subnets shown as external subnets in the Subnet Resolve List for this MAC address are sent to this router because it is responsible for servicing those subnets.
2. Click **Cancel** to exit the Router Wizard and return to the Summary. Click **Back** to return to the previous step, or **Next** to proceed to the next step.

Step 5

Figure 8-12. Router Configuration - Restrict Router to Port



1. Choose whether or not you want this router to be restricted to this port (Figure 8-12). The default is not restricted.

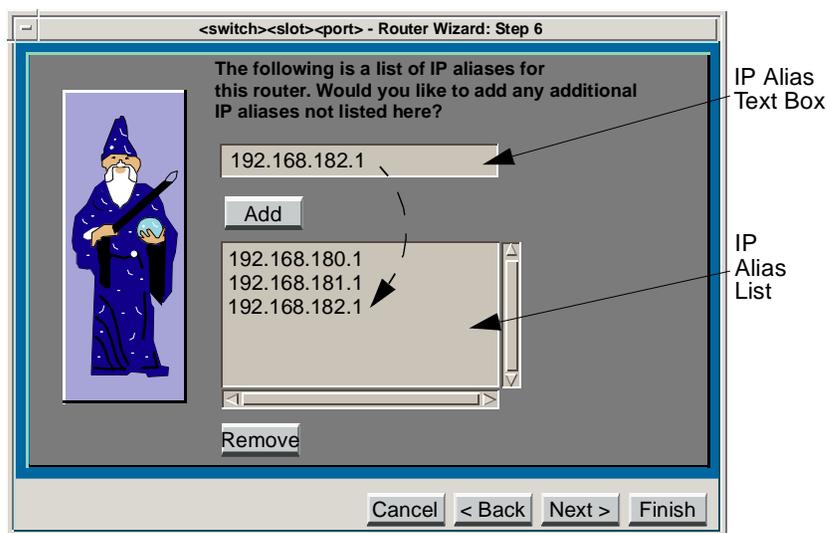


If you restrict a router to a port, all addresses associated with that router also become restricted to the port.

2. Click **Cancel** to exit the Router Wizard and return to the Summary. Click **Back** to return to the previous step, or **Next** to proceed to the next step.

Step 6

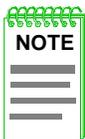
Figure 8-13. Router Configuration - IP Aliases



Addresses are AND'ed with the domain's subnet mask and displayed as internal subnets in the switch's Subnet Resolve List and are used to create IP aliases for the router MAC address.

This window lets you add or remove IP aliases to the IP Alias List (Figure 8-13).

- To add an IP alias to the list, enter an IP alias into the IP Alias Text Box and then click **Add**. The IP alias is added to the list.
- To remove an alias from the list, select the IP alias you want to remove and then click **Remove**. The entry is removed from the list.

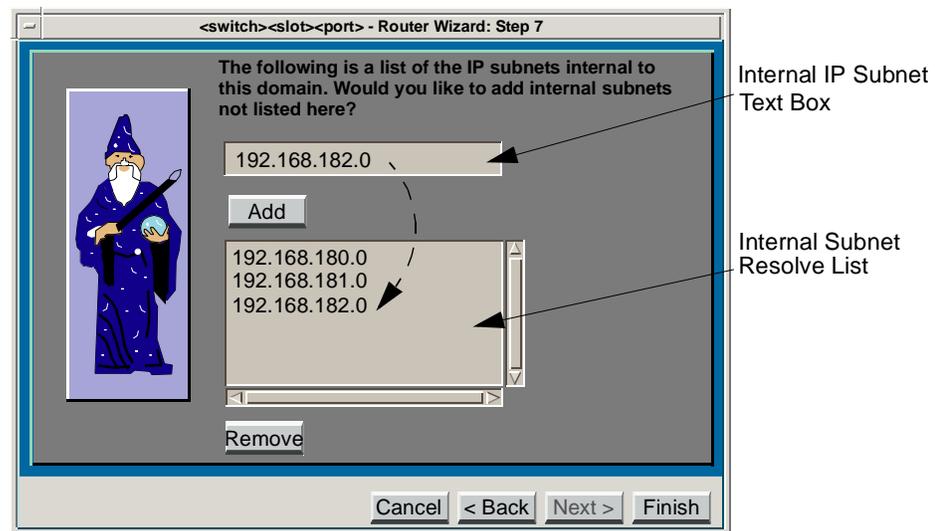


IP aliases shown in this list are the aliases for the router MAC being configured. Each alias represents a subnet that will be serviced by the switches in the domain.

1. Enter all IP aliases for the router connected to this switch port. Check the configuration of the router to determine its aliases.
2. Click **Cancel** to exit the Router Wizard and return to the Summary. Click **Back** to return to the previous step, **Next** to proceed to the next step.

Step 7

Figure 8-14. Router Configuration - Internal Addresses



This window allows you to add or remove IP subnets to the internal Ip subnets list.



Subnet addresses added to the IP Address Learning Properties tabbed page (*IP Address Learning Properties*, on page 6-24) are automatically entered into the Internal Subnet Resolve List and the Internal Subnets list in the Router Wizard Summary Window.

1. Add or remove internal IP subnets to the list as required.
 - a. To add an internal IP subnet to the list, enter an IP subnet into the Internal Subnet IP Address Text Box and then click **Add**. The internal IP subnet is added to the Internal Subnet Resolve List and the Internal Subnet list in the Router Wizard Summary Window.
 - b. To remove an internal subnet from the list, select the IP address of the subnet you want to remove and then click **Remove**. The entry is removed from the Internal

Subnet Resolve List and the Internal Subnets Window in the Router Wizard Summary Window.

2. Click **Cancel** to exit the Router Wizard and return to the Summary. Click **Back** to return to the previous step, or **Finish** to display the Summary window.



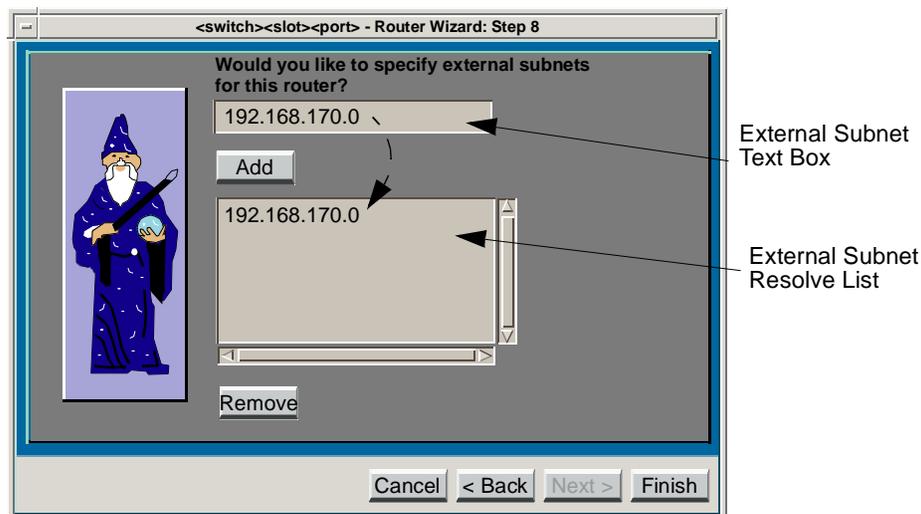
Step 8 of the Router Wizard has a direct correlation with the selection you made in Step 4 (Default Gateway). Step 8 will only appear if you opted for this router to *not* be configured as the Default gateway for the domain.

Step 8

Router Not Configured as the Default Gateway

If you chose this router *not* to be the Default Gateway for the domain, [Figure 8-15](#) is displayed. Connections to destination addresses in a subnet specified in this list are resolved to the MAC address of this router.

Figure 8-15. Router Configuration - Non-Default Gateway External Subnets



1. Add or remove external IP subnets to the list as required.
 - a. To add an external subnet to the list, enter an IP subnet into the External IP Subnet Text Box and then click **Add**. The subnet is added to the External Subnet Resolve List.
 - b. To remove a subnet from the list, select the IP subnet you want to remove and then click **Remove**. The entry is removed from the External Subnet Resolve List.

2. Click **Cancel** to exit the Router Wizard and return to the Summary. Click **Back** to return to the previous step, or **Finish** to display the Summary window.

Router Port Configuration Examples

This section provides four examples that show how router ports can be configured on SecureFast networks. The sample network shown in [Figure 8-16](#) is used for all examples.

The router connected to SW2, Port1, Router A, has been configured as the Default Gateway for the domain. Router A's IP aliases have been entered into the IP Alias List. These aliases are automatically entered into SW2, Router A's Internal Subnet Resolve List and are used to create IP aliases for the router MAC. The subnets in Router A's Internal Subnet Resolve List are propagated to the Subnet Resolve Tables of all the switches in the domain.

A router connected to SW3, Port1, Router B, has been configured *not* to be a Default Gateway for the domain. Router B's IP aliases have been entered into the IP Alias List. Router B's subnet, 170, has been entered into SW3, Router B's External IP Subnet List. This subnet is propagated to the Subnet Resolve Tables of all the switches in the domain.

Another router connected to SW3, Port1, Router C, has been configured *not* to be a Default Gateway for the domain. Router C's IP aliases have been entered into the IP Alias List. Router C's subnet, 160, has been entered into SW3, Router C's External IP Subnet List. This subnet is propagated to the Subnet Resolve Tables of all the switches in the domain.

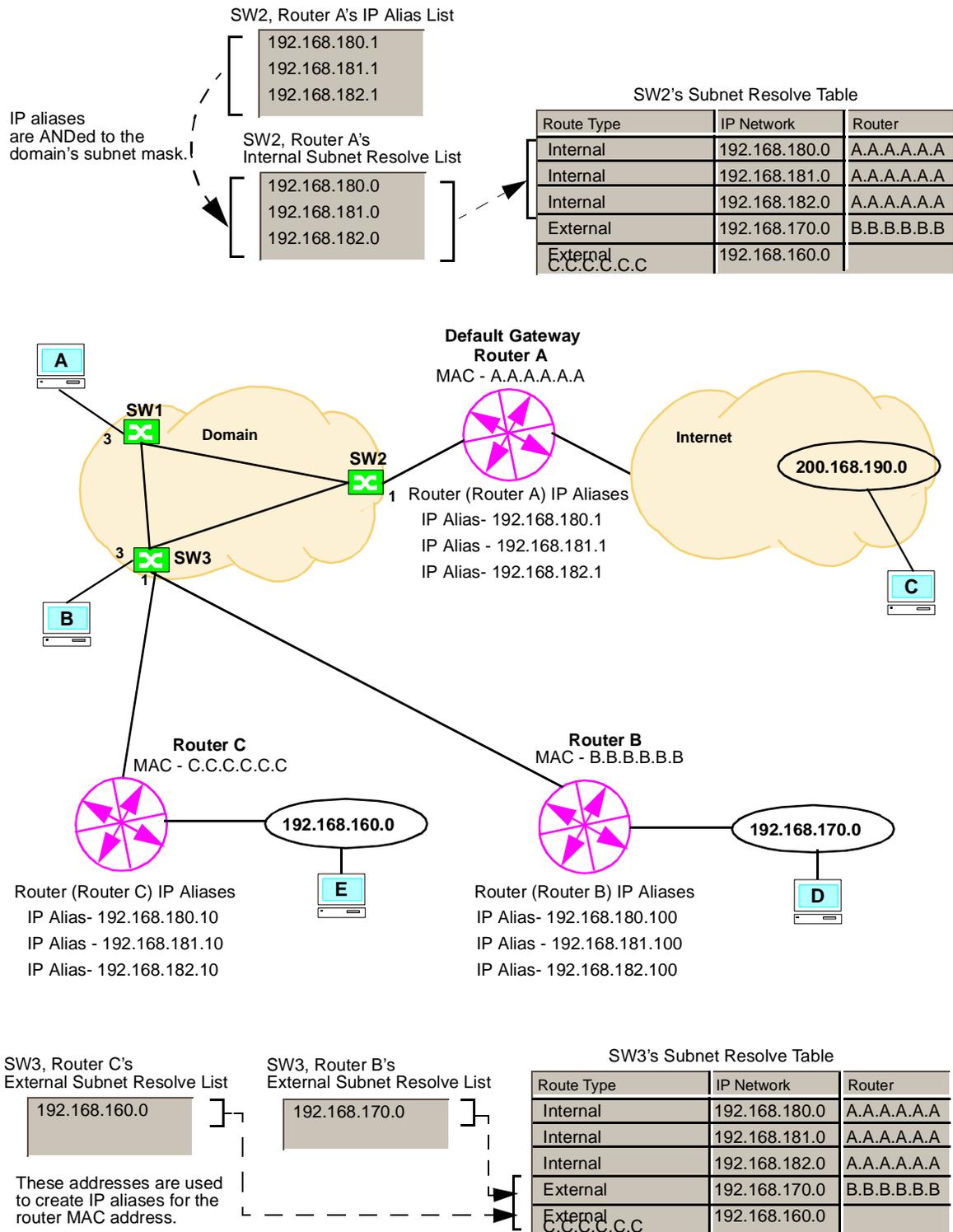
Configuration information is shared between all switches in the domain. As a result, the Subnet Resolve Tables for all switches in the sample network will contain the same information consisting of all internal and external subnets to be serviced by all switches and routers in the domain.

Proxy ARP is *enabled* on all routers and each router is aware of the subnets that the other routers are configured to service. The subnet mask for all subnets is 255.255.255.0.

Example 1

Endpoint A wants to talk to endpoint B. Endpoint A ARPs for endpoint B. SW1 intercepts the broadcast frame (ARP). SW1 consults its local directory for the MAC address corresponding to IP in the ARP request. A match may or may not be found. If a match is found then SW1 sends a unicast ARP request to endpoint B and a connection is established. If no match is found then the Subnet Resolve Table is consulted. Endpoint B's IP address when ANDed with the subnet mask will match an internal IP network entry. Having discovered that endpoint B's address is an internal address, the switch will generate a remote resolve request, asking all other switches for endpoint B's MAC address. If no response is heard the frame will be flooded. If endpoint B's MAC address is resolved then SW1 sends a unicast ARP request to endpoint B. The response establishes a connection from endpoint A to endpoint B.

Figure 8-16. Sample Router Port Configuration Network



Example 2

Endpoint A wants to talk to endpoint D. Endpoint A ARPs for endpoint D. SW1 intercepts the broadcast frame (ARP). SW1 consults its local directory for the MAC address corresponding to IP in the ARP request. A match will not be found. The Subnet Resolve Table is consulted. Endpoint D's IP address when ANDed with the subnet mask matches an entry that is external. Having found an external match SW1 generates a unicast ARP request to router B's MAC address which was found to correspond to the external address matched. Router B will have to be running Proxy ARP and will send an ARP response back to endpoint A establishing a connection between endpoint A and router B.

Example 3

Endpoint A wants to talk to endpoint C. Endpoint A ARPs for endpoint C. SW1 intercepts the broadcast frame (ARP). SW1 consults its local directory for the MAC address corresponding to the IP in the ARP request. A match will not be found. The Subnet Resolve Table is consulted. Endpoint C's IP address when ANDed with the subnet mask is not matched with either an internal or external address. Since Router A is defined as the default gateway, a unicast ARP request is sent to Router A's MAC. Proxy ARP must be running on router A. Router A sends an ARP response back to endpoint A. A connection is established between endpoint A and the router.

Example 4

Endpoint A wants to talk to endpoint E. Endpoint A ARPs for endpoint E. SW1 intercepts the broadcast frame (ARP). SW1 consults its local directory for the MAC address corresponding to IP in the ARP request. A match will not be found. The Subnet Resolve Table is consulted. Endpoint E's IP address when ANDed with the subnet mask matches an entry that is external. Having found an external match SW1 generates a unicast ARP request to Router C's MAC address which was found to correspond to the external address matched. Router C will have to be running Proxy ARP and will send an ARP response back to endpoint A establishing a connection between endpoint A and router C.

Locking/Unlocking a Port

VLAN Manager lets you lock or unlock a port. If the port to which an endpoint is connected is locked, that endpoint will assume membership in the Default VLAN for that port, regardless of any previous static membership.

To lock or unlock a port, select the port you want to change, and then choose **Toggle Lock/Unlock** from the Port menu or use the pop-up menu. The  icon is displayed next to locked ports.

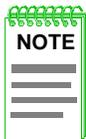


This operation is also available from the Switch Port pop-up menu and from the VLAN tab of Port Properties.

Setting/Unsetting a Router Port

To use Set/Unset Router Port:

1. Click on the access port you want to toggle.
2. Select **Set/Unset Router Port** from the **Edit >Port** menu. If the port is currently unset, the port will be set, the access port icon is replaced by a router port icon , and the router wizard summary is displayed (Figure 8-7). If the port is currently set, it will be unset and all subnet information will be removed from the subnet resolve tables for the routers on that port.



Two Router Wizard cannot be running at the same time so if the Router Wizard is already running when you set a port to be a router port, the port icon will change to the router icon (indicating that Layer 3 learning has been disabled) but the Router Wizard will not be launched.



This operation is also available from the Switch Port pop-up menu.

3. Fill in the appropriate fields in the router wizard. Refer to *Configuring a Router Port*, on page 8-9.

Redundant Access

Redundant Access (RA) lets you configure endpoints within a VLAN domain to be connected to more than one switch access port ([Figure 8-17](#)). This feature is particularly useful in situations where loss of connections due to port failure cannot be tolerated (e.g., connections to a file server). In addition, redundant switches can be in separate chassis, eliminating single points of failure in your network.



Dynamic Redundant access ports are configured automatically for the SVC model using HSIMs.

Redundant ports are classified as either 'Primary' or 'Standby'. The 'Primary' port provides network connectivity. The 'Standby' port is waiting to provide network connectivity.

Two icons identify redundant access ports: the 'Primary' port icon  and the 'Standby' port icon .

If the redundant access port is also a router port, the icons are  for the 'Standby' router port and  for the 'Primary' router port.

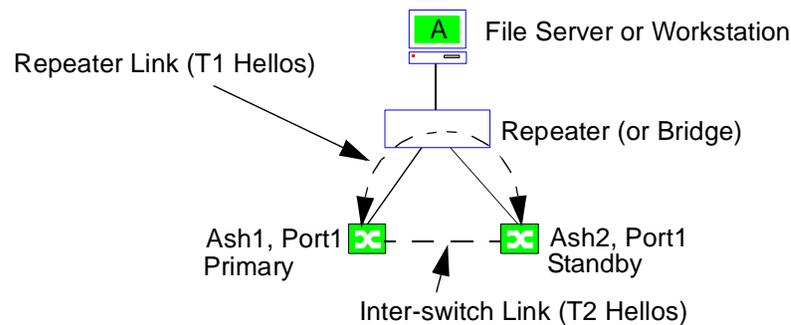
You can configure Redundant Access ports in two ways, Dynamic Redundant Access and Provisioned Redundant Access. In most situations, Dynamic Redundant Access is preferred; however, in special situations, Provisioned Redundant Access is required. For instance, if the device you want to provide redundant network connectivity for is configured with two network interface cards sharing the same MAC address.

Dynamic and Provisioned Redundant Access function the same way except for the manner in which redundant neighbors are identified. Refer to [Dynamic Redundant Access Functional Overview](#) and [Provisioned Redundant Access Functional Overview](#) for more information.

Dynamic Redundant Access Functional Overview

A sample network configuration that would use Dynamic Redundant Access Ports is shown in [Figure 8-17](#).

Figure 8-17. Dynamic Redundant Access Ports



In this configuration, Endpoint A has two points of access into the network, Ash1, Port1 and Ash2, Port1. When you configure these ports to be redundant, they start sending switch Hellos through the repeater in order to locate other redundant access ports. These Hellos are called T1 Hellos. In our example, Ash1, Port1 and Ash2, Port1 hear each other's T1 Hellos. At that point, one of the switches is elected to be the primary point of access for all endpoints behind the repeater. This election is based on port priority (which is user configurable from the Redundant Port Properties tab) or switch MAC address. The port with the highest priority is elected to be the primary point of access. If both ports have the same priority, the switch with the highest MAC address is elected.



If no T1 Hellos are heard from a neighbor switch, a switch will elect itself as 'primary'. The port will function normally, it just has no backup in case of a failure. If switch Hellos from a neighboring switch are heard at a later time, the switches will negotiate to elect a 'primary' port based on normal election criteria (port priority or switch MAC address).

In our configuration, Ash1, Port1 is the primary port and Ash2, Port1 the standby port. Once the election of the primary port has taken place, the switches start sending out another type of switch Hellos. These Hellos, called T2 or 'Heartbeat Hellos', are used by the standby switch to monitor the primary port's status. In our example, if Ash2, Port1 does not hear T2 Hellos from Ash1, Port1 in a specified number of seconds, Ash2, Port1 will determine if Ash1, Port1 is really gone. It does this by listening for T1 Hellos from Ash1, Port1. If it hears T1 Hellos, Ash2, Port1 stays as 'standby'; however, if it does not hear T1 Hellos, it transitions to 'primary'. The time it takes to transition (the failover rate) is user configurable from the Redundant Port Properties tab.



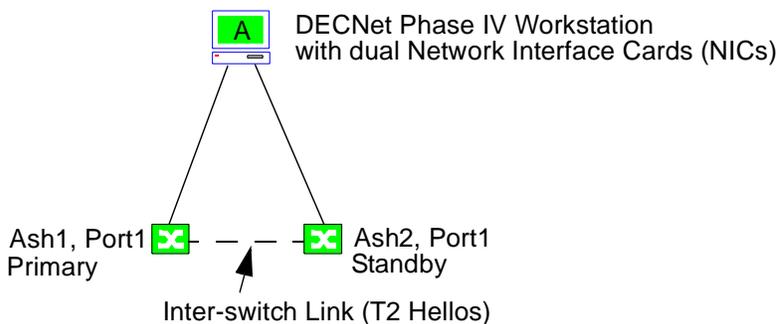
1. A 'standby' switch port can also change to 'primary' if either the 'standby' port's priority increases to above the 'primary' port's priority or the 'primary' port's priority is decreased below the 'standby' port's priority.
2. Any time a new redundant access port is detected, an election takes place. This means that the current 'primary' port may not stay 'primary' depending on the new port's priority.
3. Resetting the 'primary' switch will cause the 'standby' to transition to 'primary' until the original 'primary' switch becomes operation and is re-elected as 'primary'.

Provisioned Redundant Access Functional Overview

Provisioned Redundant Access is only meant to be used in situations where a device has multiple network interfaces, all sharing the same MAC address (e.g., a DECNet Phase IV workstation with dual NICs sharing the same MAC address). It is not meant to be used as a replacement for Dynamic Redundant Access.

A sample network configuration that would require Provisioned Redundant Access to be used is shown in [Figure 8-18](#).

Figure 8-18. Provisioned Redundant Access Ports



In this configuration, Endpoint A has two points of access into the network, Ash1, Port1 and Ash2, Port1. Unlike the Dynamic Redundant Access Port configuration shown in the previous section, there is no repeater link over which T1 Hellos can be exchanged. Because T1 Hellos cannot be exchanged, redundant port neighbor information will not be learned dynamically and must therefore be configured manually. Once neighbor information is configured (provisioned), Provisioned Redundant Access Ports will function like Dynamic Redundant Access Ports.

The need for Provisioned Redundant Access ports can be best understood by comparing the configurations shown in this section and the [Dynamic Redundant Access Functional Overview](#) section. Basically, you use Provisioned Redundant Access Ports when there is

no other way for redundant access port switches to dynamically discover each, as is the case in the configuration described in this section. You must manually configure redundant access port neighbor information.

You might ask why use redundant access at all in this situation. Why not just cable each of the workstation's interfaces to a different switch port and let the workstation decide which interface to use. The problem with this approach is that since both of the workstation's interfaces share the same MAC address, that same MAC address will be seen on two different ports on the network (i.e., it will be seen as user mobility).

By provisioning redundant access ports, only one of the ports designated as redundant will be electrically active at any given time, so the user mobility condition will not exist. The workstation's MAC address will only be seen on the active port, the 'primary'. The workstation will use whatever interface is connected to the 'primary' redundant access port. If the 'primary' port fails, the 'standby' port will transition to 'primary' and the workstation will transition to the interface connected to the new 'primary' port.

Configuring Dynamic Redundant Access Ports



If you set a network port that represents a link between two switches to be redundant, connection between the switches will be lost, because one of the ports will become a standby port and switch "Hellos" will be ignored.

To configure Dynamic Redundant Access, perform the following:

1. Run Domain Discovery.
2. Select **Set/Unset Redundant Port**.
3. Make physical connections.

Run Domain Discovery

Once the VLANServer and VLAN Manager have been started, run Domain Discovery. Select **Discovery** from the **File >Domain** menu. All user ports without physical connections to them are shown as access ports in the 'initial' state  (blue).

Select Set/Unset Redundant Access Ports

The **Set/Unset Redundant Port** menu selection lets you set or unset the ports supporting an endpoint.

Setting Dynamic Redundant Access Ports

To assign Dynamic Redundant Access ports to a particular endpoint:

1. Select a switch access port you want to designate as a redundant port.



This can also be done via Administrative Type on the Port Properties General tabbed page.

2. Select **Set/Unset Redundant Port** from the **Edit >Port** menu. The selected port's icon will change from  to  indicating that the port is in the 'initial' state (Figure 8-19).

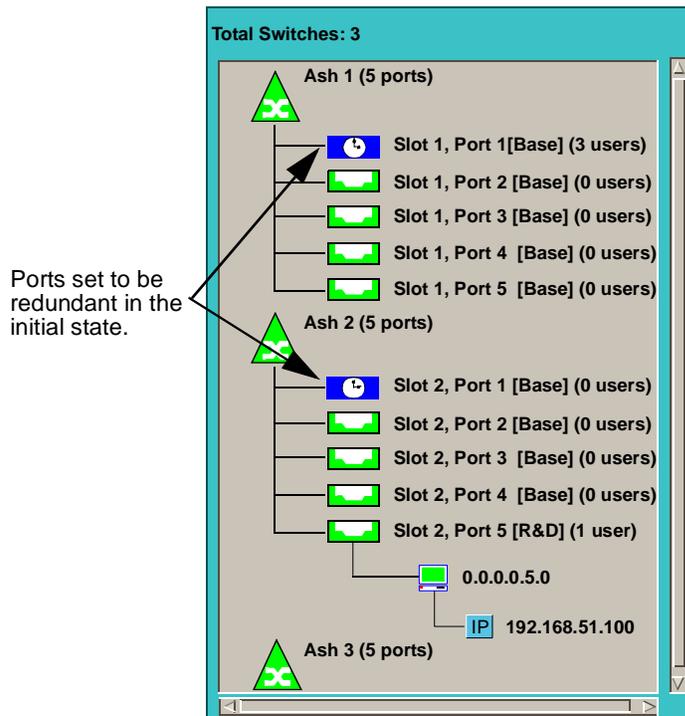
When a physical connection is made to the port, the icon color will change from BLUE (Initial) to GREEN (Up). If the port is assigned to be the 'Primary' port, the port icon will change from  to . If the port is assigned to be a 'Standby' port, the icon shape will change from  to .



All ports configured as Dynamic Redundant Access ports for a user must be assigned the same Default VLAN. If all ports are not assigned the same Default VLAN, the user's VLAN membership may be wrong if one port goes down and another takes over.

3. Repeat Steps 1 and 2 for each switch access port you want designated as Dynamic Redundant Access ports.

Figure 8-19. Set Dynamic Redundant Access Ports



4. Repeat this process for each endpoint requiring dynamic redundant access capability.

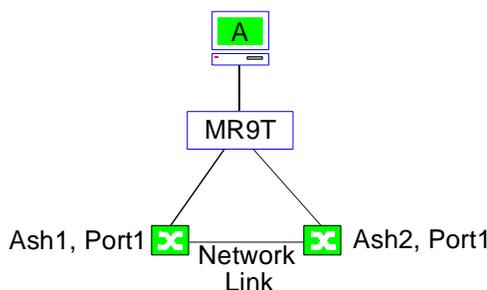
Make Physical Connections

Physically connect an endpoint requiring dynamic redundant access to a repeating device (e.g., Cabletron’s MR9T repeater, legacy bridge, or a file server with redundant ports) and then make the connections from the repeating device to the switch ports that will support that endpoint. Repeat this process for each endpoint requiring redundant access ports.



If a link to a Dynamic Redundant Access port is removed, the port associated with that link will return to the ‘initial’ BLUE standby state . This indicates the link has been lost.

Figure 8-20. Making Physical Connections



**Never set a network port to be redundant.
Contact with the switch will be lost.**

In the example above (Figure 8-20), endpoint A is connected to an MR9T and connections are made from the MR9T repeater to switch Ash 1, Port1 and switch Ash2, Port1. Since redundant access port functionality has been invoked (refer to *Select Set/Unset Redundant Access Ports*, on page 8-28), once the connections are made, one port will be designated as the 'active' port  for endpoint A, and the other will be designated as the 'standby' port  port for endpoint A.



Redundant Access port states may not change until two poll cycles have been completed. For example, if the poll interval is set to 300 (default), redundant port states will not change for up to 600 seconds.

Unconfiguring Dynamic Redundant Access Ports

To unset Dynamic Redundant Access port functionality for a particular endpoint:

1. Select one of the ports designated to support a particular endpoint.
2. Select **Set/Unset Redundant Port** from the **Edit >Port** menu.



This can also be done by selecting **Dynamic** as the Administrative Type on the Port Properties General tabbed page.

3. Disconnect the physical connection from the port. The port icon for that port will change from a redundant access port icon,  or , to , a normal port icon.

Configuring Provisioned Redundant Access Ports



Do not use Provisioned Redundant Access in a configuration where Dynamic Redundant Access can or should be used. Dynamic Redundant Access is more tolerant of misconfigurations, network problems/failures, etc.

Configuring Provisioned Redundant Access Ports

To configure Provisioned Redundant Access, perform the following:

1. Run Domain Discovery.
2. Select **Set/Unset Redundant Port**.
3. Provision redundant access port neighbor information.
4. Make physical connections.

Run Domain Discovery

Once the VLANServer and VLAN Manager have been started, run Domain Discovery. Select **Discovery** from the **File >Domain** menu. All user ports without physical connections to them are shown as access ports in the 'initial' state  (blue).

Select Set/Unset Provisioned Redundant Access Ports

The **Set/Unset Redundant Port** menu selection lets you set or unset the ports supporting an endpoint.

Setting Redundant Access Ports

To assign redundant access ports to a particular endpoint:

1. Select a switch access port you want to designate as a redundant port.



This can also be done via Administrative Type on the Port Properties General tabbed page.

2. Select **Set/Unset Redundant Port** from the **Edit >Port** menu. The selected port's icon will change from  to  indicating that the port is in the 'initial' state (Figure 8-19).

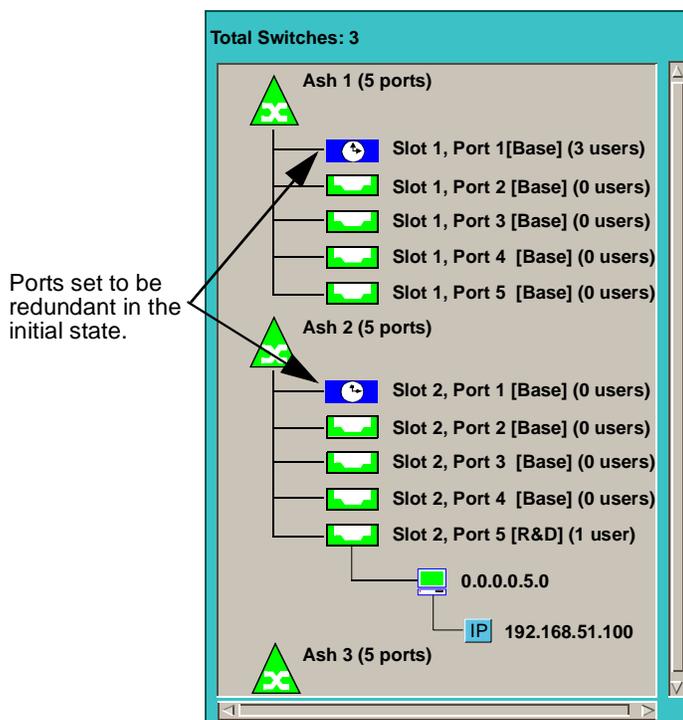
When a physical connection is made to the port, the icon color will change from BLUE (Initial) to GREEN (Up). If the port is assigned to be the 'Primary' port, the port icon will change from  to . If the port is assigned to be a 'Standby' port, the icon shape will change from  to .



All ports configured as redundant access ports for a user must be assigned the same Default VLAN. If all ports are not assigned the same Default VLAN, the user's VLAN membership may be wrong if one port goes down and another takes over.

- Repeat Steps 1 and 2 for each switch access port you want designated as redundant.

Figure 8-21. Set Provisioned Redundant Access Ports



Provision Redundant Access Port Neighbor Information

1. Select **Properties** from the **Edit** menu or use the port pop-up menu to display the Port Properties tabbed folder.
2. Click **Redundant** to display the Redundant Port Properties tabbed page (Figure 8-22).

Figure 8-22. Redundant Port Properties

Slot 4, Port 2 - Port Properties

General Advanced Multicast **Redundant** Restrictions

Redundant Access Neighbors:

Switch IP	Port	Status	Provisioned

Send Frequency: seconds

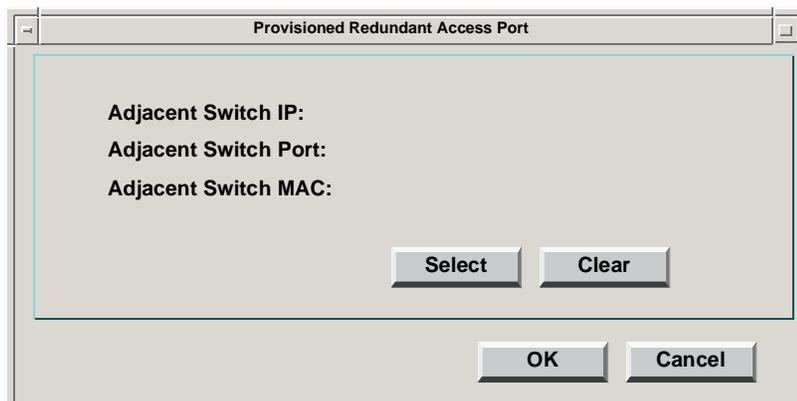
Receive Frequency: seconds

Hello Frequency: seconds

Priority:

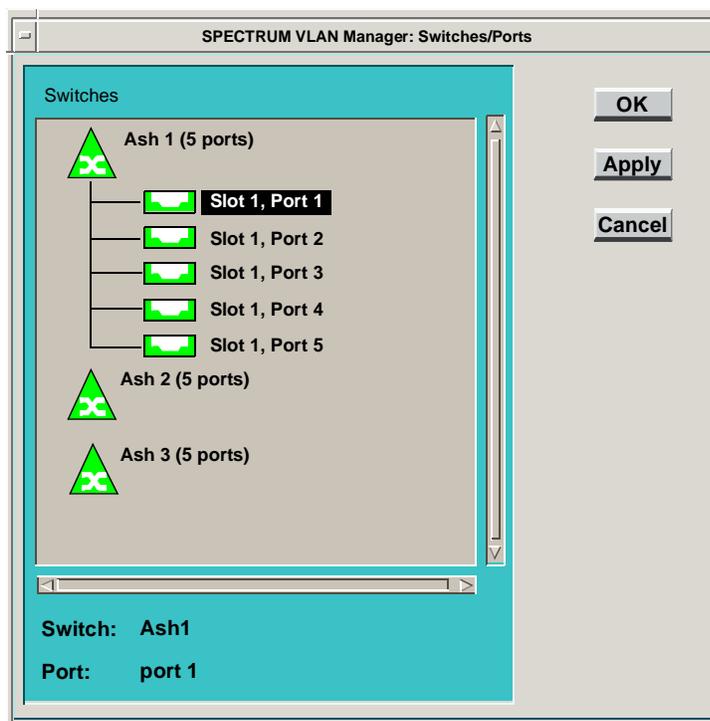
This window provides a table of all the selected port's redundant access neighbors, including each neighbor port's **Switch IP** address, its **Port** number, its **Status** (Primary or Secondary), and whether or not its redundant access is **Provisioned**. The **Frequency** and **Priority** fields also apply to the selected port.

3. Click **Provisioned** to bring up the Provisioned Redundant Access Port window.

Figure 8-23. Provisioned Redundant Access Port

If the selected port is not provisioned, the **Adjacent Switch IP**, **Adjacent Switch Port**, and **Adjacent Switch MAC** fields are listed as Not Selected.

4. Click **Select** to display the Redundant Access Port Neighbor window ([Figure 8-24](#)).

Figure 8-24. Redundant Access Port Neighbor

- Choose the switch and port that you want to designate as this redundant access port's neighbor. Click **OK** to select the port and dismiss the Switches/Ports window, **Apply** to select the port and leave the window open, or **Cancel** to return to dismiss the window without making a selection. Repeat this procedure for all redundant access ports you want to provision.

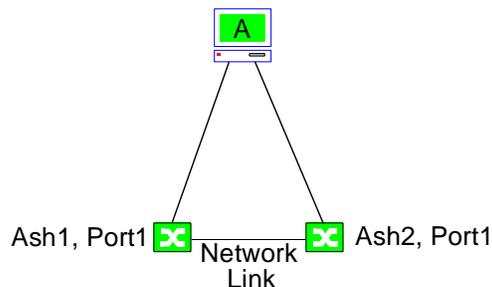
Make Physical Connections

Physically connect each of the endpoint's network interfaces to the switch ports that will support that endpoint. Repeat this process for each endpoint requiring redundant access ports.



If a link to a redundant port is removed, the port associated with that link will return to the 'initial' BLUE standby state . This indicates the link has been lost.

Figure 8-25. Making Physical Connections



**Never set a network port to be redundant.
Contact with the switch will be lost.**

In the example above (Figure 8-20), endpoint A is connected to switch Ash 1, Port1 and switch Ash2, Port1. Since redundant access port functionality has been invoked one port will be designated as the 'active' port  for endpoint A, and the other will be designated as the 'standby'  port for endpoint A.



Redundant port states may not change until two poll cycles have been completed. For example, if the poll interval is set to 300 (default), redundant port states will not change for up to 600 seconds.

Unconfiguring Provisioned Redundant Access Ports

To unset Provisioned Redundant Access port functionality for a particular endpoint:

1. Select one of the ports designated to support a particular endpoint.
2. Select **Set/Unset Redundant Port** from the **Edit >Port** menu.



This can also be done by selecting **Dynamic** as the Administrative Type on the Port Properties General tabbed page.

3. Select **Properties** from the **Edit** menu or use the port pop-up menu to display the Port Properties tabbed folder.
4. Click **Redundant** to display the domain Redundant Properties tabbed page (Figure 8-22), then click **Provisioned**.
5. Click **Clear**, then click **OK**.
6. Disconnect the physical connection from the port. The port icon for that port will change from a redundant icon,  or , to , a normal port icon.

Setting Redundant Port Properties

Redundant port properties lets you:

- Set the period of time it takes to transition (failover) from the 'Primary' port to a 'Standby' port if the primary port fails by changing the Send, Receive, and Hello Frequency parameters. In most cases, it is not necessary to change these parameters. If you do change them, make sure they are consistent between switches using the guidelines provided. For instance, if Switch 1's Send Frequency is set to 5 seconds, and Switch 2's Receive Frequency is set to 2 seconds, Switch 2 will keep aging out Switch 1 as its redundant access neighbor because it expects to receive T2 Hellos at least every 2 seconds from Switch 1 but Switch 1 is only sending T2 Hellos out one every 5 seconds.
- Choose the 'Primary' port.
- Provision redundant access port neighbor information.

The following section describes how to configure frequency and priority properties. For information about how to configure Provisioned Redundant Access ports, refer to *Configuring Provisioned Redundant Access Ports*, on page 8-32.

Configure Redundant Access Port Frequency and Priority Properties

To configure redundant access port frequency and priority properties for a VLAN domain:

1. Select **Properties** from the **Edit** menu or use the port pop-up menu to display the Port Properties tabbed folder.
2. Click **Redundant** to display the Redundant Port Properties tabbed page (Figure 8-26).

Figure 8-26. Redundant Port Properties

Slot 4, Port 2 - Port Properties

General Advanced Multicast **Redundant** Restrictions

Redundant Access Neighbors:

Switch IP	Port	Status	Provisioned

Send Frequency: seconds

Receive Frequency: seconds

Hello Frequency: seconds

Priority:

This window provides a table of all the selected port's redundant access neighbors, including each neighbor port's **Switch IP** address, its **Port** number, its **Status** (Primary or Secondary), and whether or not its redundant access is **Provisioned**. The **Frequency** and **Priority** fields also apply to the selected port.



The **Send Frequency**, **Receive Frequency**, and **Hello Frequency** attributes are dependent on each other. To ensure optimal redundant port failover performance, always set the **Receive Frequency** to four times the **Send Frequency** and the **Hello Frequency** to two times the **Send Frequency**.

- **Send Frequency** - The number of seconds a switch port will wait between switch Hellos. Valid times are 1 through 300 seconds. The default is 1 second.
- **Receive Frequency** - The number of seconds a switch port being initialized will wait for switch Hellos from another switch before electing itself as 'primary'. Valid times are 1 through 1200 seconds. The default is 4 seconds.
- **Hello Frequency** - The number of seconds a switch port will wait for Hello messages from another switch before transitioning (failover) to 'primary'. Valid times are 1 through 1200 seconds. The default is 2 seconds.



The faster the failover time, the larger the Hello message overhead. A larger overhead requires a switch to use more of its processing power to ensure redundant connectivity instead of user connectivity.

Also, Hello messages use the same network segments as user traffic. This creates contention for network bandwidth. The default period provides a fast failover time. To cut down Hello message overhead in situations where failover time is not an issue, increase the failover time.

- **Priority** - The switch with the highest priority will be elected the 'primary' port. If the priority for multiple switch ports is equal, the switch with the highest MAC address will be elected 'primary'. Valid numbers are 0 through 64. The default is 32.
3. Set Redundant properties.
 - Enter the desired value into the **Send Frequency** text field, and then enter four times that amount into the **Receive Frequency** text field and two times the **Send Frequency** into the **Hello Frequency** text field.
 - Enter the desired value into the **Priority** text field.

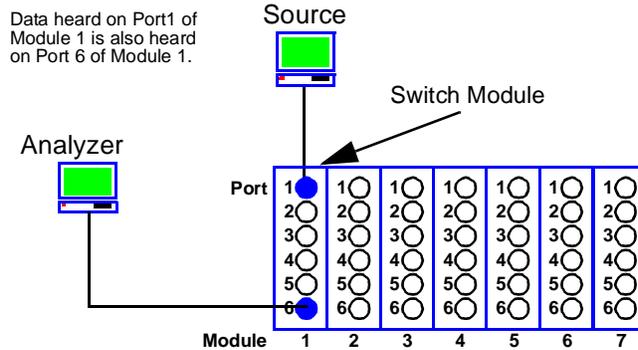
Redirecting a Port

The Port Redirect feature lets you redirect data from one or more ports directly to another port, essentially mirroring the traffic at the "redirect" port. This feature is useful in that it lets you use an external analyzer on the "redirect" port to analyze data without disturbing normal switching operations at the original source ports.

Data can be redirected to ports on the same module. Data can be redirected to ports on different modules if the firmware in those modules supports Distributed Chassis Management. Check the Firmware Release Notes for your particular modules to find out if Distributed Chassis Management is supported.

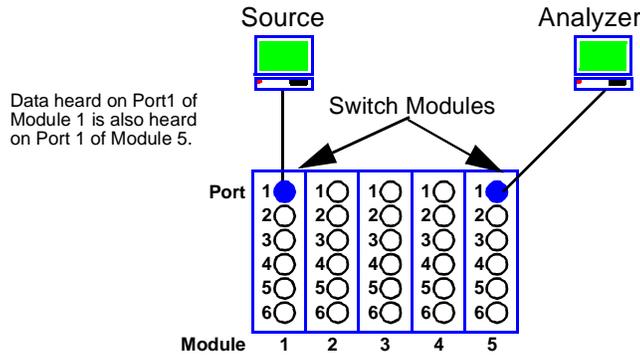
For instance, on modules that do not support Distributed Chassis Management, data can only be redirected to ports on the same module ([Figure 8-27](#)).

Figure 8-27. Redirecting Data Between Ports on the Same Module



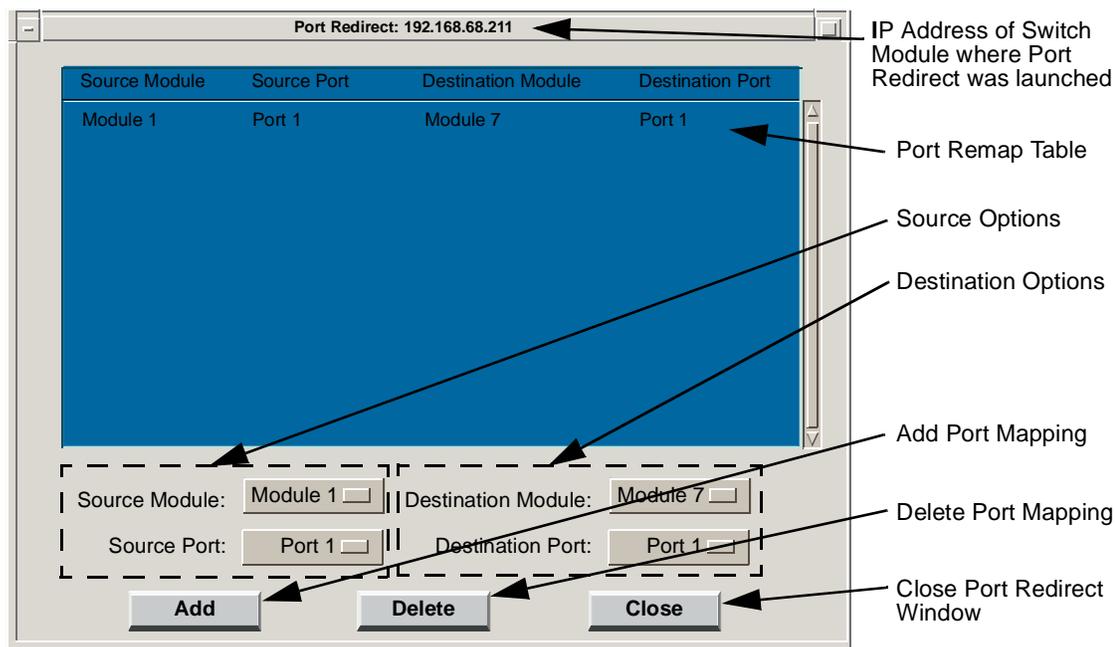
On the other hand, some modules do support Distributed Chassis Management so data can be redirected to ports on the same module or to ports on other modules of the same type in the same chassis (Figure 8-28).

Figure 8-28. Redirecting Data Between Ports on Different Modules



The Port Redirect window (Figure 8-29) displays the port remap table. You can add new entries to and delete existing entries from the table. When you set a source port to redirect to a destination port, the destination port will send out all data received or transmitted on the source port.

Figure 8-29. Port Redirect Window



Note that the Port Redirect window for a SS9000 series switch module has two additional buttons near the top of the window, Table Start/Stop and Table Enable/Disable. You can start or stop interface remapping and enable or disable the interface remapping function at the device using these buttons.

Launching Port Redirecting from the VLAN Manager

To redirect a port, select a switch from the VLAN Manager’s Main window and then click **Port Redirect** from the **Tools** menu. The Port Redirect window is displayed, with the current port mappings listed in the Port Remap Table. You can add or delete port mappings to this table, using the **Add** and **Delete** buttons located at the bottom of the window.

Adding a Port Mapping

To add an entry to the Port Remap Table:

1. Click **Source Module** and then select the desired source module. If Distributed Chassis Management is not supported, this field will be grayed out or contain a single entry.

2. Click **Destination Module** and then select the desired destination module. If Distributed Chassis Management is not supported, this field will be grayed out or contain a single entry.
3. Click **Source Port** and then select the desired source port.
4. Click **Destination Port** and then select the desired destination port.
5. Click **Add** to add the redirect pair you have just selected to the interface remap table. Port data will immediately begin to be redirected to the destination port.

Deleting a Port Mapping

To delete an entry from the interface remap table:

1. Click anywhere on the entry in the Port Remap Table that you want to delete.
2. Click **Delete** to delete that entry from the table. Port data will immediately cease to be redirected to the destination port.

Restricting a Port

VLAN Manager lets you restrict a port using Port Restrictions or a user using User Restrictions. This section explains how you can use Port Restrictions to restrict a port to a certain MAC addresses. This is very useful in situations where the security of a port is required. By restricting a port to certain MAC addresses, connection requests from users (MAC addresses) other than those to which the port has been restricted will not be processed. Mobility of the users to which a port is restricted is allowed unless a user itself is restricted (refer to *User Restrictions*, on page 10-25).

User Restrictions, on page 10-25 explains how you can use User Restrictions to restrict users to any number of specified ports (Restricted Mobility) or restrict any or all of a user's aliases to the port to which the user is connected (Restricted Alias).

[Table 8-1](#) provides a short description of each type of restriction and illustrates how each type of restriction affects a user's alias(es) and a user's mobility.

Table 8-1. Types of Restrictions

Type of Restriction	Description	User Alias(es)	User Mobility
Port Restriction	Restricts a port to certain MAC addresses.	User aliases are not considered	User mobility is allowed. Only the users on a port's Port Restriction list can move to the port; however, a user on the list can move to any non-restricted port or to any other port which is restricted to that user's MAC address.
User Restriction (Restricted Mobility)	Restricts a user (MAC address) to certain ports.	All user aliases associated with the user are locked to the user's MAC address. No other MAC address can use any of the user's aliases.	Some user mobility is allowed. User can move to any port to which it is restricted.
User Restriction (Restricted Alias)	Restricts a user alias to the user.	Any selected user alias associated with the user can be locked to the user's MAC address. No other MAC address can use any of the user's locked aliases.	No user mobility is allowed. User's MAC address is restricted to the port to which the user is connected.

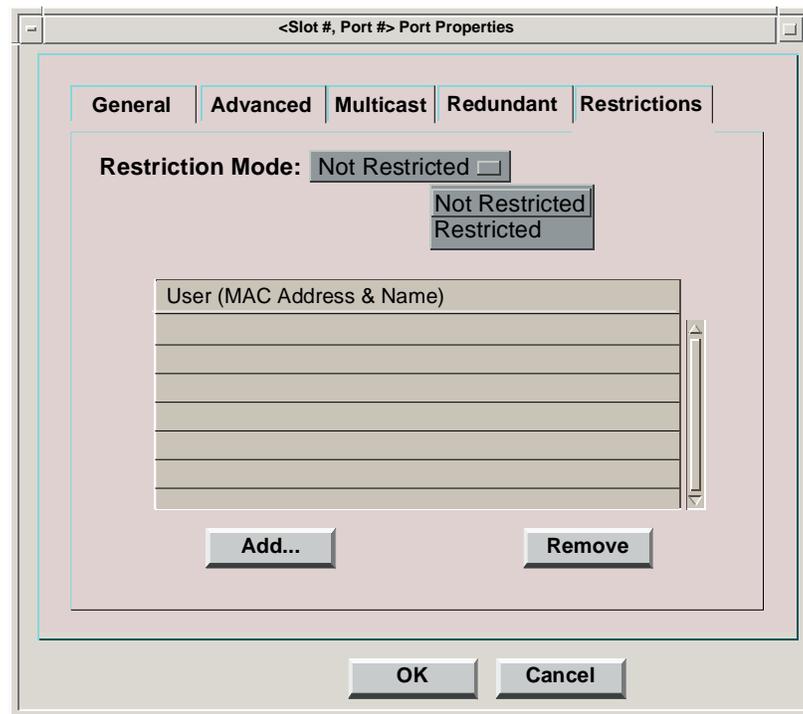


If you use Redundant Access, do not restrict users or ports for redundant users using the user or port restrictions available from user or port properties. Doing so may cause unpredictable results.

Using Port Restrictions to Restrict a Port

To restrict a port to certain MAC addresses:

1. Select a port from the VLAN Manager Main window.
2. Select **Properties** from the **Edit** menu or use the port pop-up menu to display the Port Properties tabbed folder and then click the **Restrictions** tab to display the restrictions tabbed page (Figure 8-30). This page lets you set/unset port restrictions and lets you view, add, and remove user MAC addresses/Names currently restricted to the port.

Figure 8-30. Restricting a Port

3. Choose **Restriction Mode**. If you choose **Not Restricted**, any MAC address that is not restricted to another port can use the port. If you choose **Restricted**, only those MAC addresses listed in the MAC Address list can use the port.

If you selected **Restricted**, continue with Step 4; if you selected **Not Restricted**, continue with Step 5.

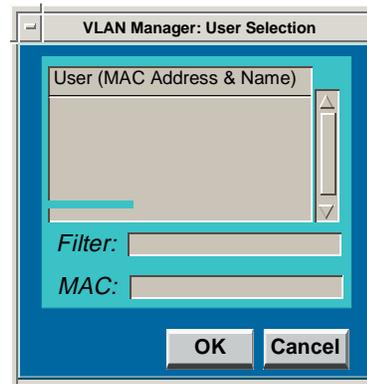
4. Click **Add** to display the VLAN Manager: User Selection dialog box (Figure 8-31). The MAC addresses/Names of all users in the current domain are shown in the user list. Select the user(s) you want to add and then click **OK** to add the MAC addresses/Names to the MAC Addresses list or **Cancel** to return to the Restrictions tabbed page without making changes to the list.



You can use the filter feature to find a user(s) quickly. As you type characters in the Filter text box, only those users that match your criteria are displayed.

OR

You can enter the MAC address of the user directly into the MAC field.

Figure 8-31. Port Restrictions - Add MAC Addresses

5. Click **OK** to accept the changes and close the window, or **Cancel** to close the window without making any changes.



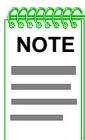
To identify, view, and remedy port violations, refer to *Violations*, on page 10-32.

Enabling OSPF Multicast

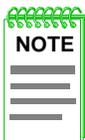
The OSPF (Open Shortest Path First) protocol provides best route determination for routers. Because routers running this protocol use a well-known multicast address to communicate with other routers, the following conditions must exist if a router connected to a SecureFast port is running OSPF:

- IP Multicast must be enabled
- multicast groups must be created on the switches
- the port must be configured to receive the multicast group's packets

The Router Wizard's **Enable OSPF Multicast** option creates both of these conditions, eliminating the need to configure them manually. Enabling OSPF Multicast on a router port enables IP Multicast for the domain, if it is not already enabled, and adds the 224.0.0.5 and 224.0.0.6 Multicast Groups (router ports which are utilizing OSPF) to the port.



OSPF is available in SecureFast firmware version 2.0.13 and later.



The **Enable OSPF Multicast** feature in the Router Wizard is not to be confused with Domain and Switch Protocol Control for OSPF Broadcast. See *Protocol Control*, on page 6-38 and *Switch Protocol Control*, on page 7-19 for information on Protocol Control.

To enable OSPF multicast:

1. In the VLAN Manager Main window, select the port to which the router is connected.
2. Use the right mouse button to bring up the port pop-up menu, or go to the **Edit >Port** menu.
3. For a port that has not yet been configured as a router port, select **Set/Unset Router Port**. For a port already set to be a router port, select **Router Wizard**. The Router Wizard Summary window (Figure 8-6) will open.
4. If the port is not a router port, set it as a router port (see *Configuring a Router Port*, on page 8-9).
5. In the Protocol Information box of the the Router Wizard Summary window, select **Enable OSPF Multicast**, then click **OK**.
6. To ensure that the OSPF Multicast Groups were added to the Router Port, select **Properties** from the port pop-up menu. In the **Multicast** tab, check to see that the 224.0.0.5 and 224.0.0.6 Multicast Groups are listed in the **Group** field for the selected port.

To disable OSPF multicast:

1. In the VLAN Manager Main window, select the port to which the router is connected.
2. Use the right mouse button to bring up the port pop-up menu, or go to the **Edit >Port** menu.
3. Select **Router Wizard**. The Router Wizard Summary window (Figure 8-6) will open.
4. In the Protocol Information box, deselect **Enable OSPF Multicast**, then click **OK**.
5. To ensure that the OSPF Multicast Groups were removed from the Router Port, select **Properties** from the port pop-up menu. In the **Multicast** tab, check to see that the 224.0.0.5 and 224.0.0.6 Multicast Groups are no longer listed in the **Group** field for the selected port.

Enabling VRRP Multicast

VRRP (Virtual Router Redundancy Protocol) provides a way to have one or more backup routers when using a statically configured default router on a LAN. Without VRRP, if the router specified for forwarding packets from a group of hosts on a LAN fails, there is no way to provide for a backup router. With VRRP, a virtual IP multicast address can be specified (224.0.0.18) as a default. This multicast address is shared among the routers, with one designated as the master router and the others as backups. If the master fails, the multicast address is mapped to a backup router's IP address and this backup becomes the master router.

Because routers using this protocol use a well-known multicast address to communicate with other routers, the following conditions must exist if a router connected to a SecureFast port is running VRRP:

- IP Multicast must be enabled
- multicast groups must be created on the switches
- the port must be configured to receive the multicast group's packets

The Router Wizard's **Enable VRRP Multicast** option creates both of these conditions, eliminating the need to configure them manually. Enabling VRRP on a router port enables IP Multicast for the domain, if it is not already enabled, and adds the 224.0.0.18 Multicast Group (router ports which are utilizing VRRP) to the port.



VRRP is available in SecureFast firmware version 2.0.12 and later.

To enable VRRP multicast:

1. In the VLAN Manager Main window, select the port to which the router is connected.
2. Use the right mouse button to bring up the port pop-up menu, or go to the **Edit >Port** menu.
3. For a port that has not yet been configured as a router port, select **Set/Unset Router Port**. For a port already set to be a router port, select **Router Wizard**. The Router Wizard Summary window (Figure 8-6) opens.
4. If the port is not a router port, set it as a router port (see *Configuring a Router Port*, on page 8-9).
5. In the Protocol Information box of the Router Summary Window, select **Enable VRRP Multicast**, then click **OK**.
6. To ensure that the VRRP Multicast Group was added to the Router Port, select **Properties** from the port pop-up menu. In the **Multicast** tab, check to see that the 224.0.0.18 Multicast Group is listed in the **Group** field for the selected port.

To disable VRRP multicast:

1. In the VLAN Manager Main window, select the port to which the router is connected.
2. Use the right mouse button to bring up the port pop-up menu, or go to the **Edit >Port** menu.
3. Select **Router Wizard**. The Router Wizard Summary window ([Figure 8-6](#)) opens.
4. In the Protocol Information box, deselect **Enable VRRP Multicast**, then click **OK**.
5. To ensure that the VRRP Multicast Group was removed from the Router Port, select **Properties** from the port pop-up menu. In the **Multicast** tab, check to see that the 224.0.0.18 Multicast Group is listed in the **Group** field for the selected port.

Managing SecureFast VLANs

This chapter provides step-by-step instructions for performing SecureFast VLAN, and AMR VLAN administration tasks using SPECTRUM VLAN Manager's graphical user interface. It also contains reference information and helpful tips to help you perform these tasks.

Overview

SPECTRUM VLAN Manager lets you group users regardless of their physical locations. Users can be grouped based on certain predefined criteria, such as protocol or address range, or based on administrative requirements such as function performed or security access level required. You group users by creating VLANs and then assigning membership to users in those VLANs, based upon the criteria you have established. Refer to [Assigning Membership in VLANs, on page 9-13](#), for information about how to assign user membership in a VLAN. Automatic membership is possible using AMR (Automatic Membership registration).

In addition to creating VLANs, VLAN Manager lets you perform many other VLAN management tasks, including deleting VLANs, displaying VLAN details, assigning default VLANs, and applying basic policy to VLANs.

Basic VLAN policy lets you set a VLAN's status and policy. Additional VLAN policy settings are available by using the Advanced VLAN Policy application. Refer to [Chapter 15, Advanced VLAN Policy](#) for information about this application.



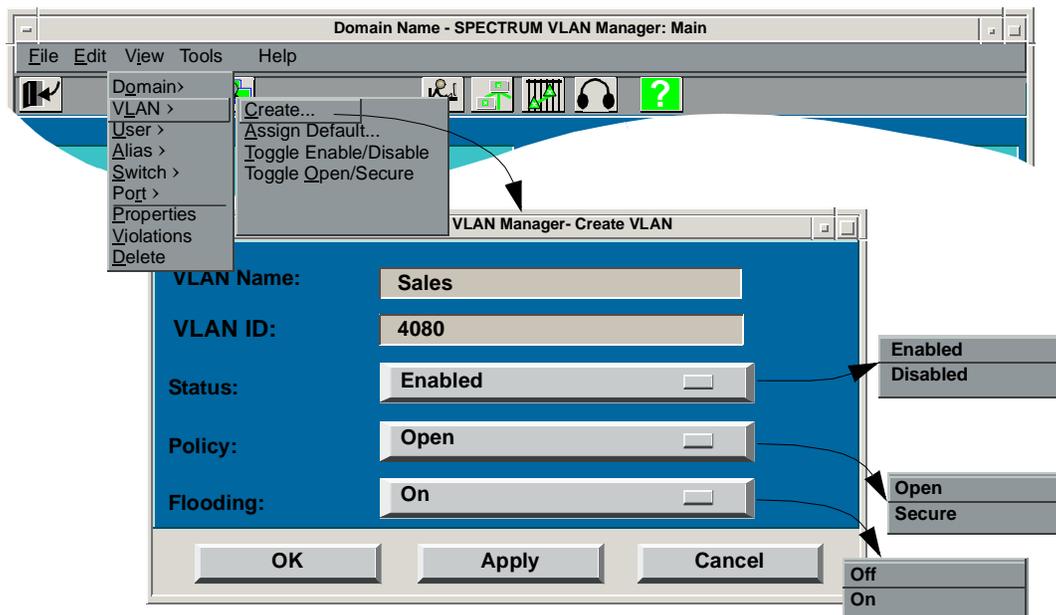
You can use the VLANs pop-up menu to perform many VLAN management tasks. To display the pop-up menu, click on a VLAN or user and then click and hold the right mouse button. Drag the cursor to the task you want to perform, and then release the button.

Creating VLANs

To create VLANs (Figure 9-1):

1. Select **Create** from the **Edit > VLAN** menu or click  on the Toolbar to display the Create VLAN dialog box.

Figure 9-1. Creating VLANs



2. Click anywhere in the **VLAN Name** text box, and then enter a unique name for the new VLAN. VLAN names can be up to 16 characters in length. Spaces are not allowed in the name.

To create a Wild Card VLAN: In certain troubleshooting situations, you may wish to create a “wild card VLAN” which can be applied (dragged) to a port in order to temporarily make the port a member of all VLANs, so that all broadcasts may be analyzed on one port. To create a wild card VLAN, enter “wildcard_vlan” (without the quotes) as the **VLAN Name**. When you type the last letter of this name, the remaining fields on the window will be set. The Wild Card VLAN is always enabled and open, and flooding is always ON. These defaults cannot be changed. Therefore, after entering the name, skip to [Step 7](#). If you are not creating a Wild Card VLAN, go on to [Step 3](#).

3. Choose a VLAN ID. A VLAN ID is unique number assigned to a VLAN. Refer to *VLAN Properties*, on page 9-6 for more information about the VLAN ID attribute.
4. Choose **Enabled** or **Disabled** from the “**Status**” selections.

- **Enabled** - The VLAN can be used according to the policy (Open or Secure) attached to it.



You can use Advanced VLAN Policy to fine tune connection and flooding policy for VLANs that already exist in the domain. Refer to [Chapter 15, Advanced VLAN Policy](#).

5. Choose **Open** or **Secure** from the “**Policy**” selections.

- **Open** - If the source switch can resolve the destination MAC address for an endpoint on another VLAN, the connection will be established.
- **Secure** - Members of one VLAN are restricted from communicating with members of another VLAN. Inter-VLAN communication operating in Secure mode requires a router that has been configured to be a member of both VLANs. If the VLAN membership of either or both of the source and destination endpoints is configured for Secure policy, the switch will not allow the connection between those endpoints.



There is a period of time (one poll cycle), after a switch resets, when users assigned static membership in a secure VLAN come up as members of the VLAN before they are mapped to their static secure VLAN. During this period of time, it is possible for the users in the secure VLAN to connect to users in the default port VLAN.

To ensure that users in a secure VLAN remain secure, assign inherited membership in the VLAN. Drag the VLAN to the port(s) to which the users in the VLAN are connected. The default VLAN for the port(s) is a secure VLAN and the members of the VLAN are always secure, even if the switch resets or assign the port VLAN to be secure, flooding off and disabled.

6. Choose **On** or **Off** from the “**Flooding**” selections.



If Flooding is turned **Off**, broadcast frames will not be flooded. This may result in a network failure to establish connections to endpoints that are plugged into the switching infrastructure.

Flooding should only be turned **Off** under special circumstances (e.g., when a highly secure environment is required).

- **On** - Broadcast packets are flooded to ports of the same VLAN or ports which have a member of the same VLAN on them.
- **Off** - Broadcast packets are not flooded to ports of the same VLAN.

7. Select the **OK** button to create a new VLAN and close the window, **Apply** to create a new VLAN and leave the window open, or **Cancel** to dismiss the Create VLAN dialog box without adding a new VLAN.

Deleting VLANs

Delete lets you delete entire VLANs. Deleted VLANs are removed from the VLANServer database. This section describes how to delete entire VLANs.

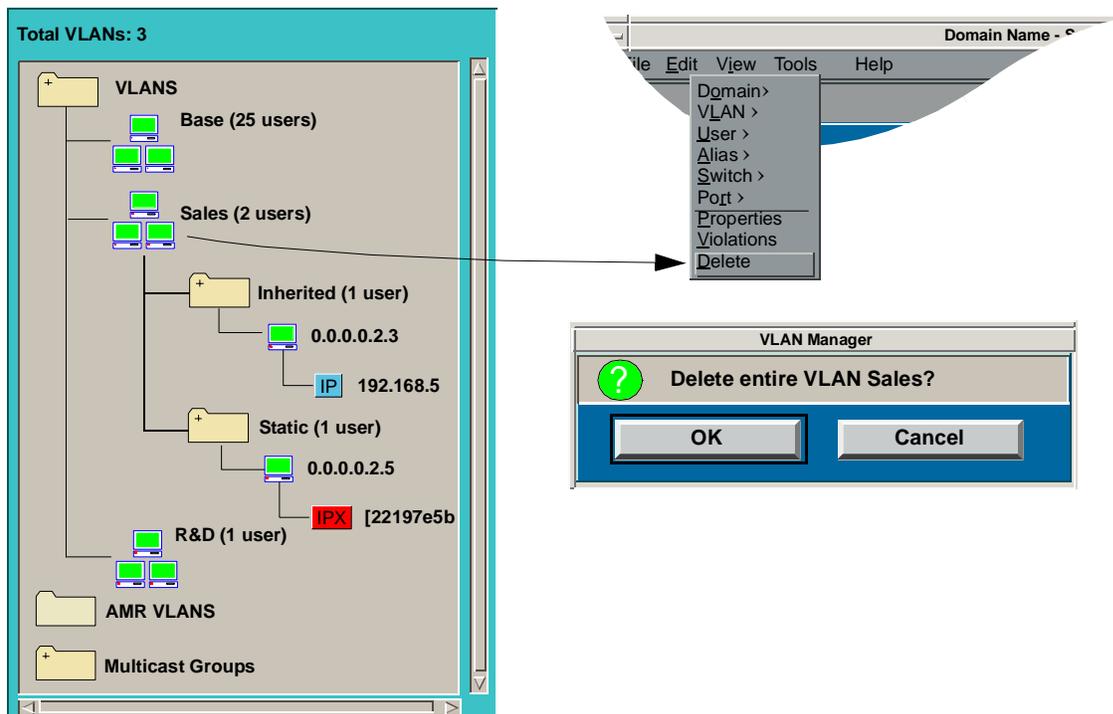
To delete an entire VLAN (Figure 9-2):

1. Click on the name of the VLAN you want to delete.
2. Select **Delete** from the **Edit** menu, or select  (Delete VLAN) from the Toolbar. Confirm that you want to delete the selected VLAN by pressing the **OK** button in the VLAN Manager confirmation box. Press the **Cancel** button to return to the VLAN Manager window without making any changes.



You can use the pop-up menu to perform this operation by clicking on a VLAN icon, holding down the right-hand mouse button to display the pop-up menu, dragging the cursor down to Delete VLAN, and then releasing the button.

Figure 9-2. Deleting Entire VLANs



Removing a User from a VLAN

To remove a user from VLAN:

1. Click on the user you want to remove from a VLAN.
2. Click **Remove from VLAN** from the **Edit >User** menu.



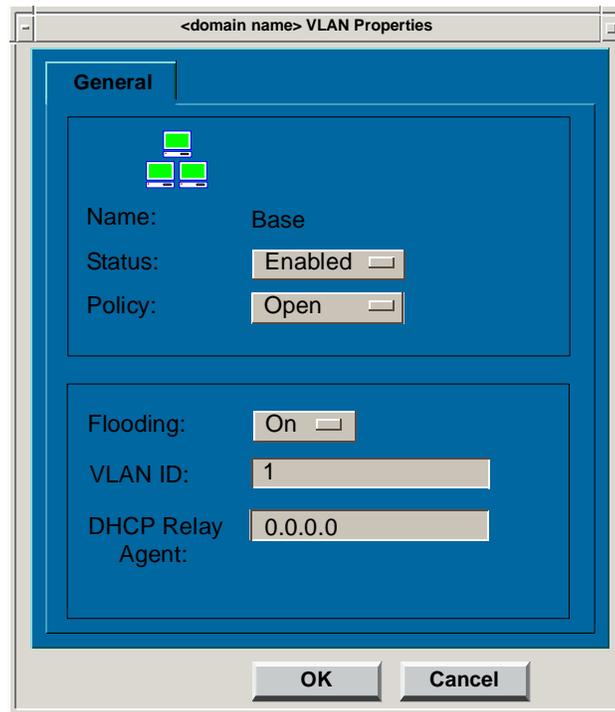
You can also initiate this operation from the VLAN User pop-up menu. Multiple users can be removed using the **Remove Users** button located in the VLAN Details window.

3. Click **Cancel** to close the window without removing the users, or click **OK** to remove users.

VLAN Properties

Lets you configure the properties of the selected VLAN ([Figure 9-3](#)).

Figure 9-3. VLAN Properties



- **Name** - Name assigned to the selected VLAN.
- **Status - Enabled or Disabled.**
 - **Enabled** - The VLAN can be used according to the policy (Open or Secure) attached to it.
 - **Disabled** - The VLAN cannot be used. Calls will not be processed and the icon representing the VLAN will be the color 'Blue'.



You can use Advanced VLAN Policy to fine tune connection and flooding policy for VLANs that already exist in the domain. Refer to [Chapter 15, Advanced VLAN Policy](#).

- **Policy - Open or Secure.**

- **Open** - If the source switch can resolve the destination MAC address for an endpoint on another VLAN, the connection will be established.
- **Secure** - Members of one VLAN are restricted from communicating with members of another VLAN. Inter-VLAN communication operating in SECURE mode requires a router that has been configured to be a member of both VLANs. If the VLAN membership of either or both of the source and destination endpoints is configured for SECURE policy, the switch firmware will not allow the connection between those endpoints.

- **Flooding - On or Off.**



If Flooding is turned **Off**, broadcast frames will not propagate. This may result in a network failure to establish connections to endpoints that are plugged into the switching infrastructure.

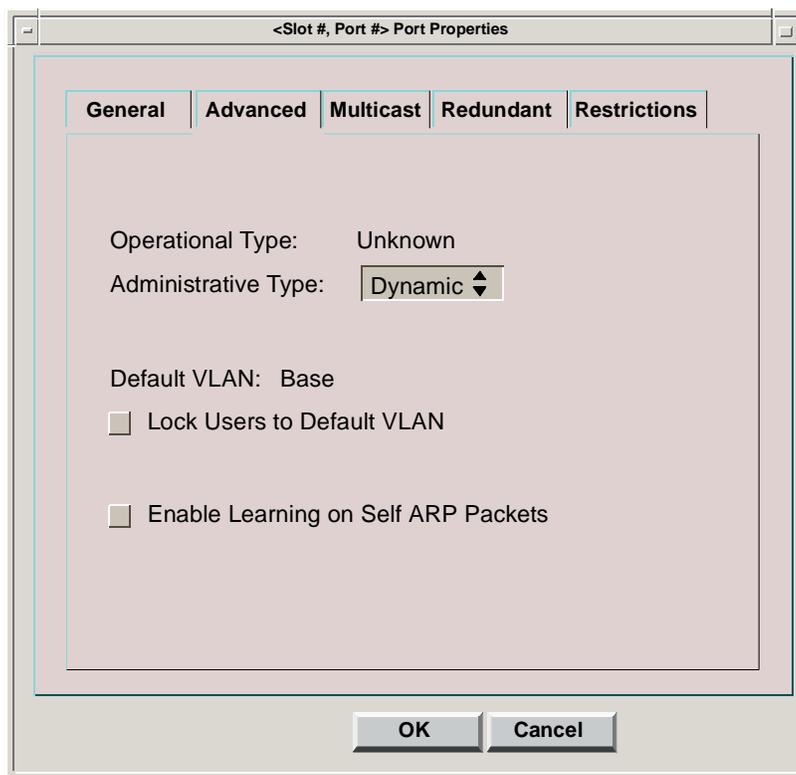
Flooding should only be turned **Off** under special circumstances (e.g., when a highly secure environment is required).

- **On** - Broadcast packets are flooded to ports of the same VLAN.
- **Off** - Broadcast packets are not flooded to ports of the same VLAN.
- **VLAN ID** - A unique number assigned to a VLAN. Allows for the assignment of an ID to a VLAN, defining whether a switch or set of switches needs to process flood channel traffic or forward it at wirespeed through the ASIC-based hardware. You can use any decimal number between 0002 and 4080 as a VLAN ID. The default is 4080. AMR VLANs are assigned VLAN IDs automatically.
- **DHCP Relay Agent** - A reserved IP address associated with the scope of a VLAN as defined at the DHCP server. This address must fall within the range of IP addresses assigned to the VLAN. Refer to [Appendix B, SecureFast DHCP Relay Agent](#) for more information about the DHCP Relay Agent.

VLAN Port Properties

VLAN Port Properties are found on the Advanced Port Properties tab. To get to this tab, select a port, right click it, and then click the Advanced tab. The VLAN properties allow you to lock all users on the selected port to the port's default VLAN (Figure 9-4).

Figure 9-4. VLAN Port Properties



- **Default VLAN** - Default VLAN for the port.
- **Lock/Unlock** - Mode assigned to a port: **Locked** or **Unlocked**.

Locked ()- All users attached to a locked port will only be members of the port's default VLAN. A lock icon is displayed to the right of a locked port.

Unlocked ()- All inherited users will be members of the port's default VLAN. All statically assigned users will be members of the VLAN(s) to which they have been assigned.

Displaying VLAN Details

The VLAN details window provides information about each user with membership in the selected VLAN. The VLAN details window lets you edit certain VLAN attributes from the VLAN Properties tabbed folder and remove users from the selected VLAN. You can drag and drop users from the VLAN Details window to VLANs in the VLAN Manager Main window. The search/filter feature accessible from this window allows you to find a particular user or group of users quickly without having to scroll through the entire list.

To display VLAN details (Figure 9-5), click on the name of a VLAN and then select **Details** from the **View >VLAN** menu or select  (VLAN Details) from the Toolbar.



You can use the pop-up menu to perform this operation by clicking on a VLAN icon, holding down the right mouse button to display the pop-up menu, dragging the cursor down to **VLAN Details**, and then releasing the button.

The VLAN Details window is composed of the general information area and **Users** area. The general information area describes the characteristics of the selected VLAN. The **Users** area provides specific information about each user with membership in the selected VLAN.

In addition to viewing VLAN details, this window lets you:

- View VLAN membership for a selected user.
- Launch the Connection Table for a selected user.
- Remove selected users from the VLAN.
- Edit the **User Name** and **Description** fields for a selected user.
- Add and remove user aliases.

General Information Fields

- **VLAN Name** - Name of the VLAN for which user statistics are being displayed.
- **Status** - Enabled or Disabled. Refer to [Creating VLANs](#), on page 9-2, for information about Enabled and Disabled VLANs.



You can use Advanced VLAN Policy to fine tune connection and flooding policy for VLANs that already exist in the domain. Refer to [Chapter 15, Advanced VLAN Policy](#).

- **Policy - Open or Secure.** Refer to *Creating VLANs*, on page 9-2, for information about Open and Secure policy.
- **Flooding - On or Off.** Refer to *Creating VLANs*, on page 9-2, for information about flooding settings.
- **Users** - Number of users that have membership in the selected VLAN.
- **Total Entries** - Number of entries in the VLAN Details table. It is possible to have more entries than users, since multiple Network Addresses for a single Physical Address will occur under certain circumstances, such as a router with multiple endpoints behind it or an endpoint running multiple protocols.

Users List

The Users List displays information about all users with membership in the selected VLAN. Each line in the User List provides information associated with a specific source endpoint (user). A scroll bar to the right of the table lets you scroll through the table.

- **Physical Address** - Physical address of the endpoint.
- **Switch** - Name of the switch to which the endpoint is connected. If DNS is not being used, this will be the network address of the switch or the name assigned to the switch in the Switch Details window.
- **Port** - Port label of the interface of the switch on which the endpoint is heard.
- **Network Address** - Network address of the endpoint.
- **Network Type** - **IP, IPX, AppleTalk, NetBIOS, or Other.**
- **DHCP Create Date** - Date the DHCP IP address was issued to the endpoint.
- **Host** - Name assigned to an endpoint. Hosts are resolved through the yellow pages from the IP address.
- **User** - Name you assign to an endpoint.
- **Restrictions - Yes or No.**
 - **Yes** - User is restricted to one port.
 - **No** (default) - User is not restricted to a specific port.

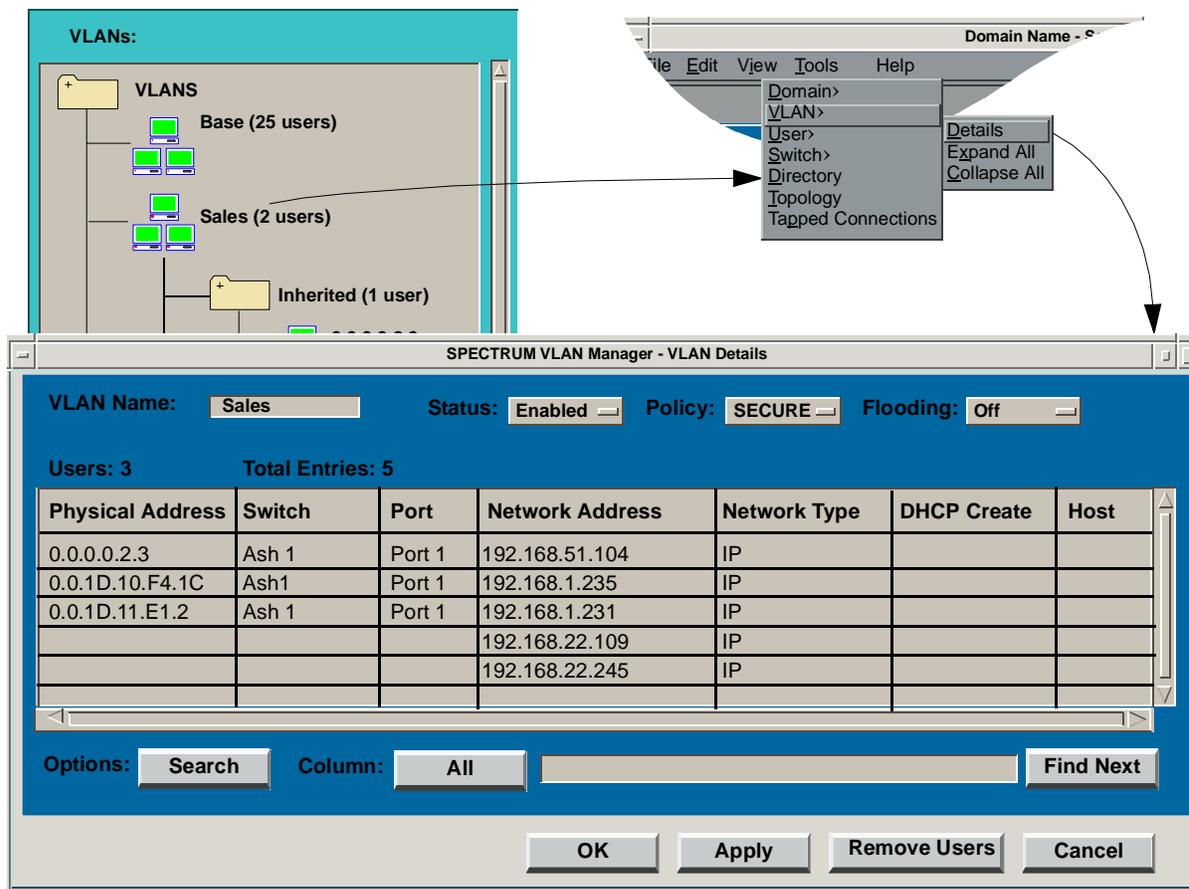


This information is also displayed when **View ? Directory** is selected. In this instance, all users are shown, since the view is not filtered for a specific VLAN.

- **Create Date** - Date user was originally created in the VLANServer database.

- **Duplicate Allowed** - Determines if a duplicate MAC address for this user should be allowed in more than one domain. This value is set from General User Properties. Valid entries are True or False.

Figure 9-5. Displaying VLAN Details



NOTE Multiple Network Addresses for a single Physical Address will occur under certain circumstances such as a router with multiple endpoints behind it or an endpoint running multiple protocols.

Editing User Properties

To modify user properties:

1. Double-Click on the user entry to display the User Properties tabbed folder. Refer to *User Properties*, on page 10-6 for more information about editing user properties.



You can also initiate this operation from the **Edit >User** menu in the Main window, the VLAN Details pop-up menu, the **Directory >Edit** menu, and the Directory pop-up menu.

Using Search/Filter

Use the **Search/Filter** button to find a particular user or group of users. You can Search or Filter by any column of the table or **All** columns. You can also Filter by **None**, which returns the table to the non-filtered state.

To use **Search/Filter**:

1. Select **Search** or **Filter** from the **Options** list and the selection criteria from the **Column** list.
2. Click anywhere in the text box to the right of **Column**, and then enter the text to be matched. Press Enter to start the Search/Filter.
 - **Search** - Finds and highlights the first instance of a user that matches the search criteria. Click **Find Next** to find subsequent instances of users that match the same criteria.
 - **Filter** - Selectively eliminates entries from the VLAN **Users** list that do not match the filter criteria. Only users that match the filter criteria are displayed.



To set filter to IP when filtering on **Network Type**, type IP and then press space bar followed by the RETURN key. This eliminates all protocols except IP.

Toggle VLAN Status/Policy

To change the status or policy of a VLAN, click on the name of the VLAN whose policy you want to change, and then choose **Toggle Enable/Disable** or **Toggle Open/Secure** from the **Edit >VLAN** menu, the VLANs pop-up menu, or the **Enable/Disable, Open/Secure** buttons from the **Properties** window. A key icon  is displayed next to each

VLAN set to SECURE mode. Refer to [Creating VLANs](#), on page 9-2, for information about VLAN status and policy.



You can use the pop-up menu to perform this operation by clicking on a VLAN entry, holding down the right mouse button to display the pop-up menu, dragging the cursor down to **Toggle Enable/Disable** or to **Toggle Open/Secure**, and then releasing the button.

Assigning Membership in VLANs

User membership in a VLAN can be accomplished in three ways: statically configured, inherited, or automatically configured.

- **Statically Configured** - Users are assigned to a VLAN manually, using the drag and drop feature provided by the VLAN Manager's graphical user interface.
- **Inherited** - Users inherit the default VLAN configuration for the port they are attached to.
- **Automatically Configured** - When Automatic Membership Registration (AMR) is enabled, VLANs are dynamically created, endpoints are joined to those VLANs, and packets are flooded to those VLANs according to the criteria rules. Refer to *AMR VLAN Administration*, on page 9-19 for more information about AMR VLANs.

VLAN Membership Rules

VLAN membership is determined in order of precedence as follows:

- Locked Port
- Secure
- AMR
- Statically Configured
- Inherited

Assigning Membership to All Users Connected to a Switch



When dragging a switch to a target VLAN, users connected to locked switch ports will not be added to the target VLAN. However, if ports are unlocked, the users attached to those ports will automatically be added to the target VLAN.

To assign membership in a VLAN to all users connected to a switch ([Figure 9-6](#)):

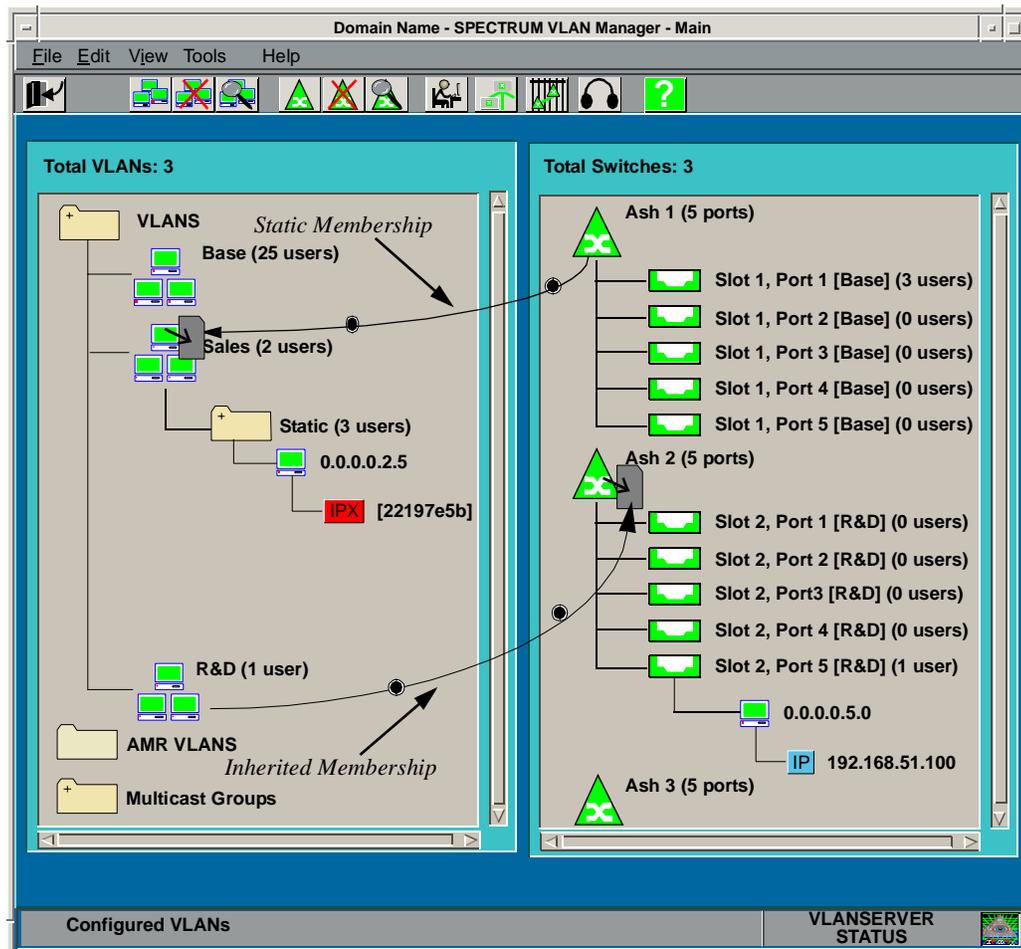
Static Membership

1. Click and hold any selected switch icon. To select multiple switches, refer to *Selecting Icons*, on page 3-25.
2. Drag the cursor over the VLAN icon to which you want to add the users of the selected switch, then drop it into the VLAN. The number of users with membership in the VLAN will increase by the number of users connected to each of the selected switch's ports.

Inherited Membership

Membership in a VLAN can also be assigned by dragging a VLAN over a switch icon and then dropping the VLAN into the switch. All users connected to that switch become members of that VLAN (unless statically configured). The default VLAN for all access ports on the switch change to that VLAN, so any users connecting to any access port on the switch will inherit membership in that VLAN.

Figure 9-6. Assigning VLAN Membership to All Users Connected to a Switch



Assigning Membership to All Users Connected to a Port

To assign membership in a VLAN to all users connected to a port (Figure 9-7):

Static Membership

1. Click and hold any selected port icon. To select multiple ports, refer to *Selecting Icons*, on page 3-25. Note that network ports cannot be selected.
2. Drag the port(s) over the desired VLAN and then drop it/them into that VLAN. All users connected to selected port(s) become members of that VLAN. The default VLAN(s) of the port(s) remains unchanged. Note that a port can only have one default VLAN.

Inherited Membership

Membership in a VLAN can also be assigned by dragging a VLAN over a switch port and then dropping the VLAN into the port. All users connected to that port become inherited members of that VLAN unless previously statically configured. The default VLAN for the port changes to that VLAN, so any users connecting to that port will assume membership in that VLAN.

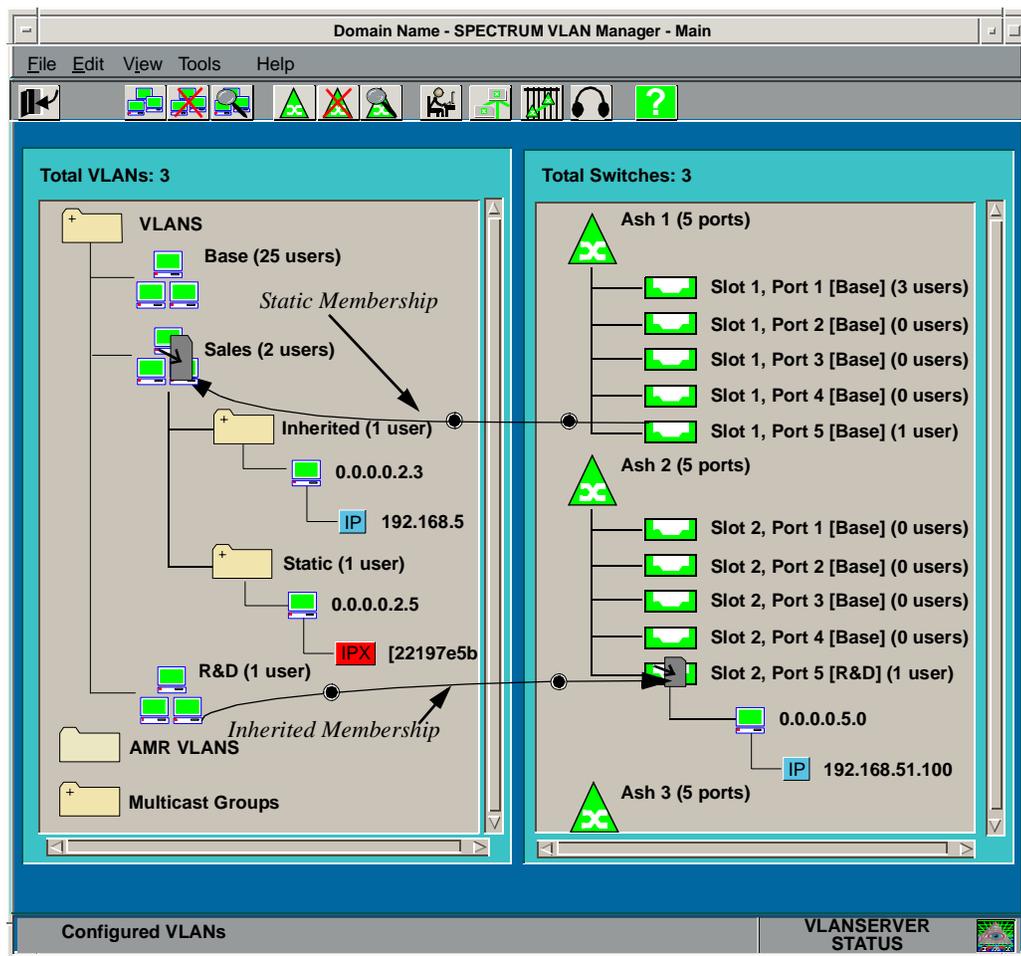


You can use the Assign Default item from the **Edit >VLAN** menu or the **Assign Default VLAN** item from the VLAN pop-up menu to initiate this operation for a single port or to multiple ports. Refer to *Assigning a Default VLAN to Multiple Switch Ports*, on page 9-18 for information about how to use this feature.



VLANs cannot be dragged to Network ports, ATM ports, or INB ports.

Figure 9-7. Assigning VLAN Membership to All Users Connected to a Port

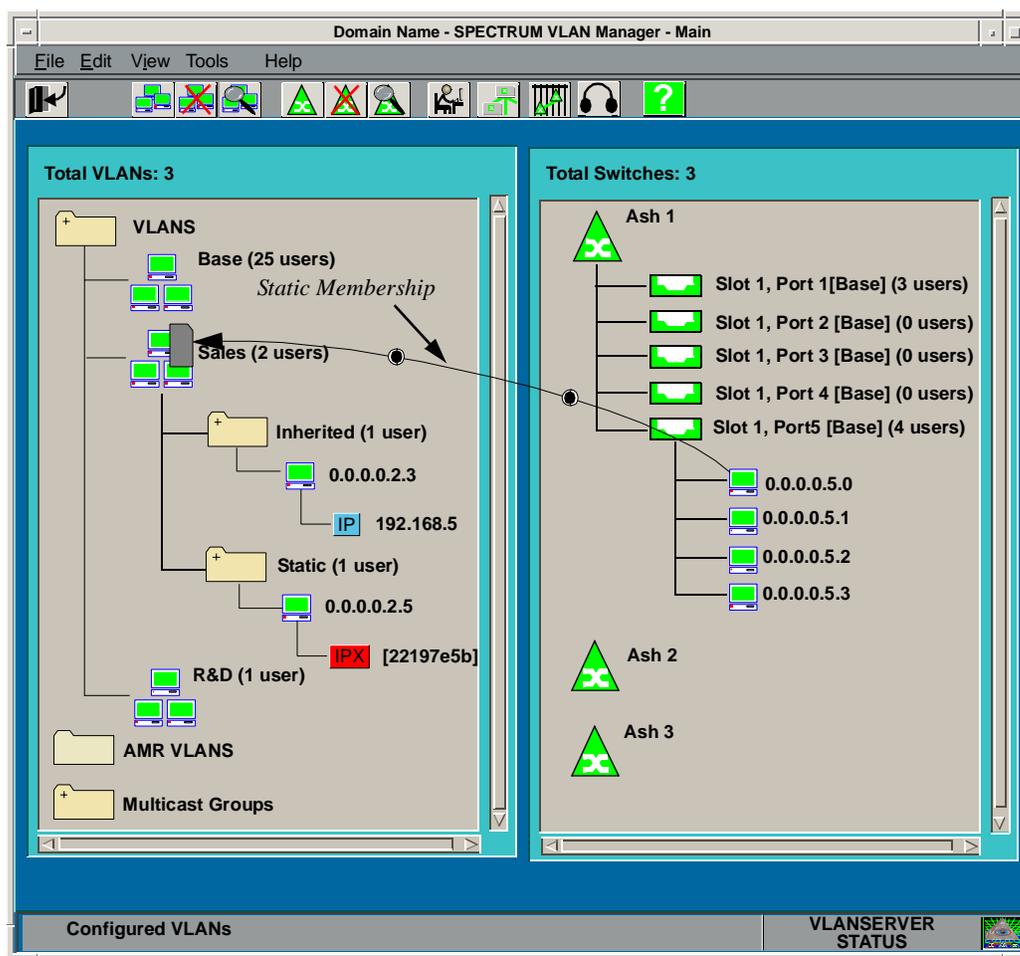


Assigning Membership to Selected Users Connected to a Port

To assign static membership in a VLAN to selected users connected to a port (Figure 9-8):

1. Click and hold any selected user icon. To select multiple users, refer to *Selecting Icons*, on page 3-25.
2. Drag the cursor over the VLAN to which you want to add the selected user(s), and then drop it into that VLAN.

Figure 9-8. Assigning VLAN Membership to Selected Users Connected to a Port

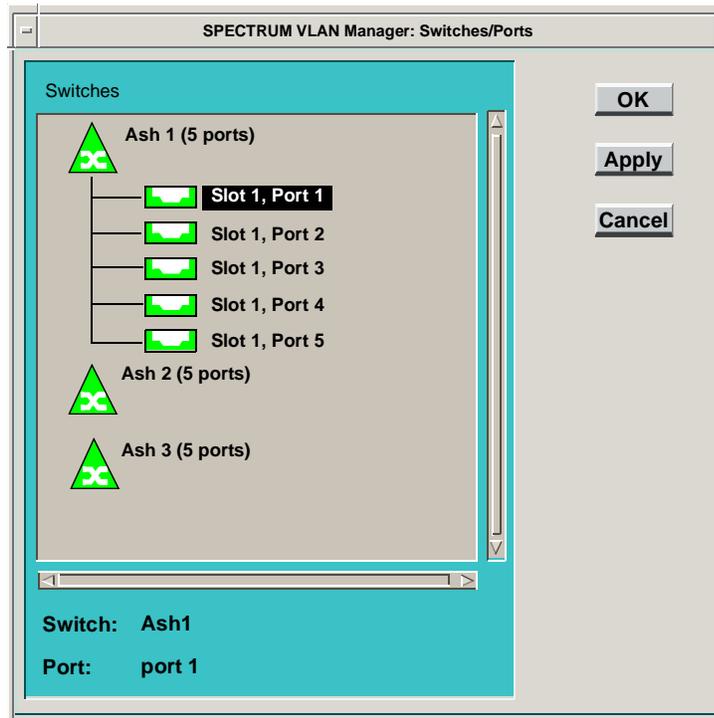


Assigning a Default VLAN to Multiple Switch Ports

To assign a VLAN as the default VLAN for multiple ports (even on multiple switches):

1. Select the VLAN you want to be the default VLAN.
2. Select **Assign Default** from the **Edit >VLAN** menu or select **Assign Default VLAN** from the VLANs pop-up menu. The Switches/Ports window is displayed (Figure 9-9).

Figure 9-9. Assigning a Default VLAN to Multiple Ports



3. Select the switch ports for which you want to have the selected VLAN used as the default VLAN. Use the left mouse button to expand and collapse switches. Use the rubber band technique to select adjacent ports. Use the “control” key in conjunction with the left mouse button to select adjacent or non-adjacent ports. Refer to *Selecting Icons*, on page 3-25, for information about selecting multiple elements.
4. Click **OK** to assign the default VLAN to the ports selected and dismiss the window, **Apply** to assign the default VLAN to the ports selected without closing the window, or **Cancel** to dismiss the Switches/Ports window without making changes.

AMR VLAN Administration

Automatic Membership Registration (AMR) dynamically creates VLANs, joins endpoints to those VLANs, and floods packets to those VLANs. Using AMR to create VLANs makes it easy to group all users of a certain type into a single VLAN without having to manually drag and drop users into a VLAN.

AMR dynamically creates a type-specific VLAN when an endpoint which is broadcasting packets that match the criteria of an enabled type is detected. That endpoint and all other endpoints which are broadcasting packets of an enabled AMR type are made members of the newly created VLAN, effectively segmenting any endpoints sending packets matching the criteria for that type.

An AMR VLAN looks and acts like a regular VLAN with the following exceptions:

- An AMR VLAN cannot be toggled from **Open** to **Secure**. All AMR VLANs are **Open**.
- An endpoint that is deleted from an AMR VLAN will be relearned as soon as it transmits a packet of that type.
- When an endpoint is joined to an AMR VLAN, the endpoint's previous VLAN mappings are not removed or changed in any way.
- If an endpoint is a member of one or more secure VLANs, the packet will be flooded to all of its secure VLANs. AMR VLANs will not be used. Also, the endpoint will not join any AMR VLANs. If the endpoint becomes a member of an AMR VLAN before it becomes a member of a secure VLAN, the AMR VLAN membership will remain, but will not be used. You can manually delete the endpoint from the AMR VLAN if so desired.
- If an endpoint resides on a locked port, the packet will be flooded only to the port's default VLAN, and will only become a member of the port's default VLAN. AMR VLANs are not used.
- If an endpoint does not reside on a locked port, and is not a member of any secure VLANs, the packet is flooded to the best matching AMR VLAN, and the source endpoint may join one or more AMR VLANs.
- If an endpoint is not a member of any AMR VLANs or the packet being sent does not match any of the endpoint's AMR VLANs, the packet is flooded to all open, non-AMR VLANs of which the endpoint is a member. Also, the endpoint will not become a member of any additional VLANs.



The maximum number of VLANs in which a user can have membership is eight. Users learned by an AMR VLAN do not count towards that limit. For example, if a user has statically gained membership in eight VLANs and then that same user is learned by an AMR VLAN, the maximum number of VLANs in which that user can have membership has not been exceeded.

The following AMR VLAN types are supported: IP-Subnet, NetBIOS, IPX RIP/SAP, AppleTalk, DECNet, Banyan VINES, and BPDU. The specific behavior of each type is described below.

Specific Behaviors of AMR Types

IP-Subnet

Enabling the IP-Subnet type requires more than just turning it on. An IP-address mask must also be specified. This mask should not be confused with a subnet mask. The mask simply dictates how much of the IP addresses to look at when creating AMR VLANs. The number of possible AMR VLANs depends on the address mask. For example, if the locally connected network uses a “192.168.subnet.endpoint” format, a mask of 255.255.255.0 would successfully divide the IP endpoints by subnet. A mask of 255.255.0.0 would create only one AMR VLAN and put all IP endpoints in it.

Joining Behavior

The AMR VLAN to join is determined by looking at the source IP address in the packet and then applying the IP-address mask. The resulting AMR VLAN is created and the endpoint is added to that VLAN.

Flooding Behavior

Broadcast packets are flooded to those ports with users who have gained membership in the same AMR VLAN using AMR, static, or inherited membership.

NetBIOS

Enabling the NetBIOS type consists simply of turning it on. Three possible AMR VLANs can be created when this type is selected:

- **NetBEUI**
- **IPX-NetBIOS**
- **IP-NetBIOS**

Joining Behavior

If a NetBEUI packet is detected, a NetBEUI AMR VLAN is created and the endpoint that transmitted the NetBEUI packet is joined to the NetBEUI AMR VLAN. Other endpoints that transmit NetBEUI packets are also joined to the NetBEUI AMR VLAN. The same is true for an endpoint that transmits an IPX-NetBIOS or an IP-NetBIOS packet, except that an IPX-NetBIOS or an IP-NetBIOS AMR VLAN is created and the endpoint is joined to the IPX-NetBIOS or the IP-NetBIOS AMR VLAN, respectively.

Flooding Behavior

Broadcast packets are flooded to those ports with users who have gained membership in the AMR VLAN automatically or using static or inherited membership.



NetBIOS aliases may not appear immediately under Microsoft NT/Windows endpoints if the NetBEUI protocol is not running. The endpoint broadcasts less often without NetBEUI, so the alias may not be learned by a switch right away.

IPX RIP/SAP

Enabling the IPX RIP/SAP type requires simply turning it on via the VLAN Manager. One possible type can be created when IPX RIP/SAP is selected:

- **IPX_RIP/SAP_<netNum>_<frameType>**

where... **IPX_RIP/SAP** = NetWare Server/Router

<netNum> = 4-byte network number

<frameType> = 802.3, Ethernet_II, 802.2, or SNAP

Joining Behavior

When an IPX RIP/SAP reply packet is detected, the endpoint (server/router) that transmitted that packet is joined to an AMR VLAN, based on its frame type and network number.

For instance, a server endpoint of frame type 802.2 with a network number of 0x11111111 will join the IPX_RIP/SAP_11111111_802.2 AMR VLAN.

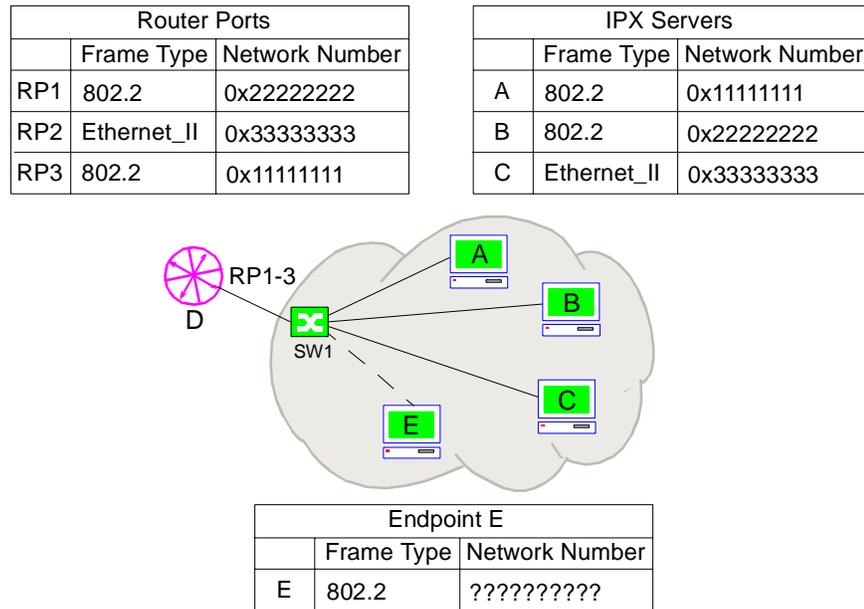
Flooding Behavior

The IPX_RIP/SAP_<netNum>_<frameType> is used for RIP/SAP flooding.

IPX RIP/SAP Example

The sample domain in [Figure 9-10](#) has three IPX servers (A, B, and C) and an IPX router (D) connected to a switch (SW1). Another endpoint (E) will be connected to the switch as this example unfolds.

Figure 9-10. IPX RIP/SAP Example



In this example:

- Endpoint A joins AMR VLAN IPX_RIP/SAP_11111111_802.2, endpoint B joins AMR VLAN IPX_RIP/SAP_22222222_802.2, and endpoint C joins AMR VLAN IPX_RIP/SAP_33333333_Ethernet_II.
- RP1 joins AMR VLAN IPX_RIP/SAP_22222222_802.2, RP2 joins AMR VLAN IPX_RIP/SAP_33333333_Ethernet_II, and RP3 joins AMR VLAN IPX_RIP/SAP_11111111_802.2.
- RP1's RIP/SAP advertisements are flooded to IPX_RIP/SAP_22222222_802.2, RP2's RIP/SAP advertisements are flooded to IPX_RIP/SAP_33333333_Ethernet_II, and RP3's RIP/SAP advertisements are flooded to IPX_RIP/SAP_11111111_802.2.

This arrangement effectively segments the servers and router ports by frame type and network number. A network error will be generated if any endpoint sees advertisements from another router/server with a different network number.

If endpoint E has to communicate with a router/server, it uses the first response it gets and attaches to that server/router using its network number as its own. If endpoint B is the first to respond, endpoint E will use network number 0x22222222 for all further communications. This means that endpoint E is able to communicate with endpoint B directly, but it would have to go through endpoint D, the router, to communicate with endpoints A or C.

Exception to IPX RIP/SAP Rule

When a Windows for Workgroups 3.11 client uses IPX-NetBIOS for sharing resources, it do not follow the standard IPX procedure for determining its IPX network number. Instead of issuing a SAP GNS (Get Nearest Server) request, the client simply uses a network number of 0x00000000 until it hears an IPX RIP/SAP advertisement. If the client never hears an IPX RIP/SAP advertisement, it will continue to use the 0x00000000 network number. An IPX-NetBIOS_00000000 VLAN is created and the client is placed that VLAN. The client can only communicate with other endpoints in the IPX-NetBIOS_00000000 VLAN, not the desired result.

To remedy this, IPX RIP packets are flooded to the IPX-NetBIOS_00000000 VLAN as well as the IPX RIP/SAP_<frame type><netNumber> VLAN allowing Windows for Workgroups 3.11 clients to receive IPX RIP advertisements. In this way, the client will hear an IPX RIP/SAP advertisement and use the valid non-zero network number found in the RIP/SAP packet as its own.

When a SecureFast switch sees that the Windows for Workgroups 3.11 client is no longer using the 0x00000000 network number, it removes the endpoint from the IPX-NetBIOS_00000000 VLAN and adds it to the IPX-NetBIOS_<netNumber> VLAN. The client can now communicate with other members of the IPX-NetBIOS_<netNumber> VLAN, the desired result.

AppleTalk

Enabling the AppleTalk type requires simply turning it on.

Joining Behavior

If an AppleTalk packet is detected by either the AppleTalk ARP Call Processor or the AppleTalk DDP Call Processor (SNAP, types 0x809b and 0x80f3), an AppleTalk AMR VLAN is created and the endpoint that transmitted the AppleTalk packet is joined to the AppleTalk AMR VLAN. Other endpoints that transmit AppleTalk packets are also joined to the AppleTalk AMR VLAN.



Default AppleTalk AMR VLANs will appear in the AMR VLANs folder. Customized AppleTalk AMR VLANs, which are specified via the VLAN Islands tab of Switch Properties will appear in the VLANs folder.

Flooding Behavior

Broadcast packets are flooded to those ports with users who have gained membership in the AMR VLAN automatically or using static or inherited membership.

DECNet

Enabling the DECNet type requires simply turning it on.

Joining Behavior

If a DECNet packet (Ethernet types 0x6000 through 0x6009 or 0x8040 through 0x8042) is detected, a DECNet AMR VLAN is created and the endpoint that transmitted the DECNet packet is joined to the DECNet AMR VLAN. Other endpoints that transmit DECNet packets are also joined to the DECNet AMR VLAN.

Flooding Behavior

Broadcast packets are flooded to those ports with users who have gained membership in the AMR VLAN automatically or using static or inherited membership.

VINES

Enabling the VINES type consists simply of turning it on.

Joining Behavior

If a VINES packet (Ethernet types 0x0bad through 0x0baf) is detected, a VINES AMR VLAN is created, and the endpoint that transmitted the VINES packet is joined to the VINES AMR VLAN. Other endpoints that transmit VINES packets are also joined to the VINES AMR VLAN.

Flooding Behavior

Broadcast packets are flooded to those ports with users who have gained membership in the AMR VLAN automatically or using static or inherited membership.

BPDU

Enabling the BPDU type consists simply of turning it on.

Joining Behavior

If a BPDU packet (Ethernet type 0x4242) is detected, a BPDU AMR VLAN is created and the endpoint that transmitted the BPDU packet is joined to the BPDU AMR VLAN. Other endpoints that transmit BPDU packets are also joined to the BPDU AMR VLAN.

Flooding Behavior

Broadcast packets are flooded to those ports with users who have gained membership in the AMR VLAN automatically or using static or inherited membership.

Enabling AMR VLANs

This section describes how you enable AMR VLANs using the Discovery Wizard or using the **Edit ? Domain ? Properties** window. Each method requires you to choose the type(s) of AMR VLAN to enable and, in the case of IP Subnet, to provide the address mask, which is used by the switches in a domain to determine how many IP AMR VLANs to enable. Refer to *Specific Behaviors of AMR Types*, on page 9-21, for information about IP Subnet AMR VLANs.

Enabling AMR VLANs Using the Discovery Wizard

To enable AMR VLANs using the Discovery Wizard:

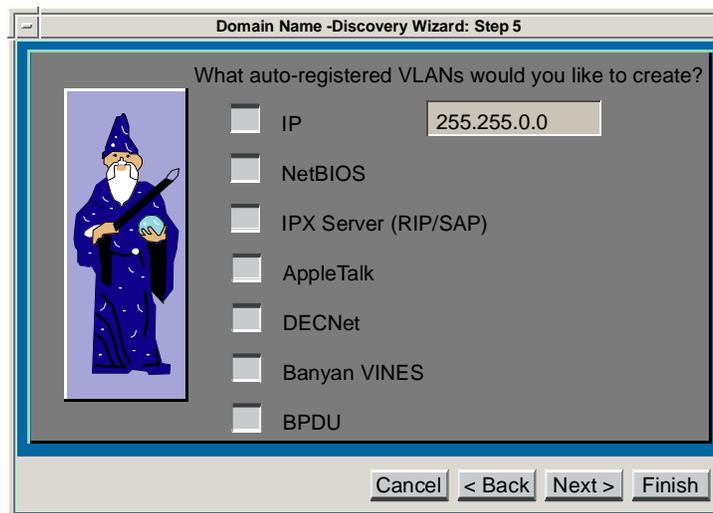
1. Start the Discovery Wizard. Refer to *VLAN Manager Domain Discovery Wizard*, on page 6-1.
2. In Step 5 of the referenced procedure, click the type of AMR VLANs types you want to enable. A type is enabled when its corresponding button is recessed (down).



If you enable the IP-Subnet type, enter an IP-address mask in the text box to the right of “IP-Subnet”.

You can select as many types as you want. [Figure 9-11](#) shows all types selected in this example. Once a type is enabled, VLANs for that type are dynamically created as broadcast packets of that type are heard.

Figure 9-11. Enabling AMR VLANs



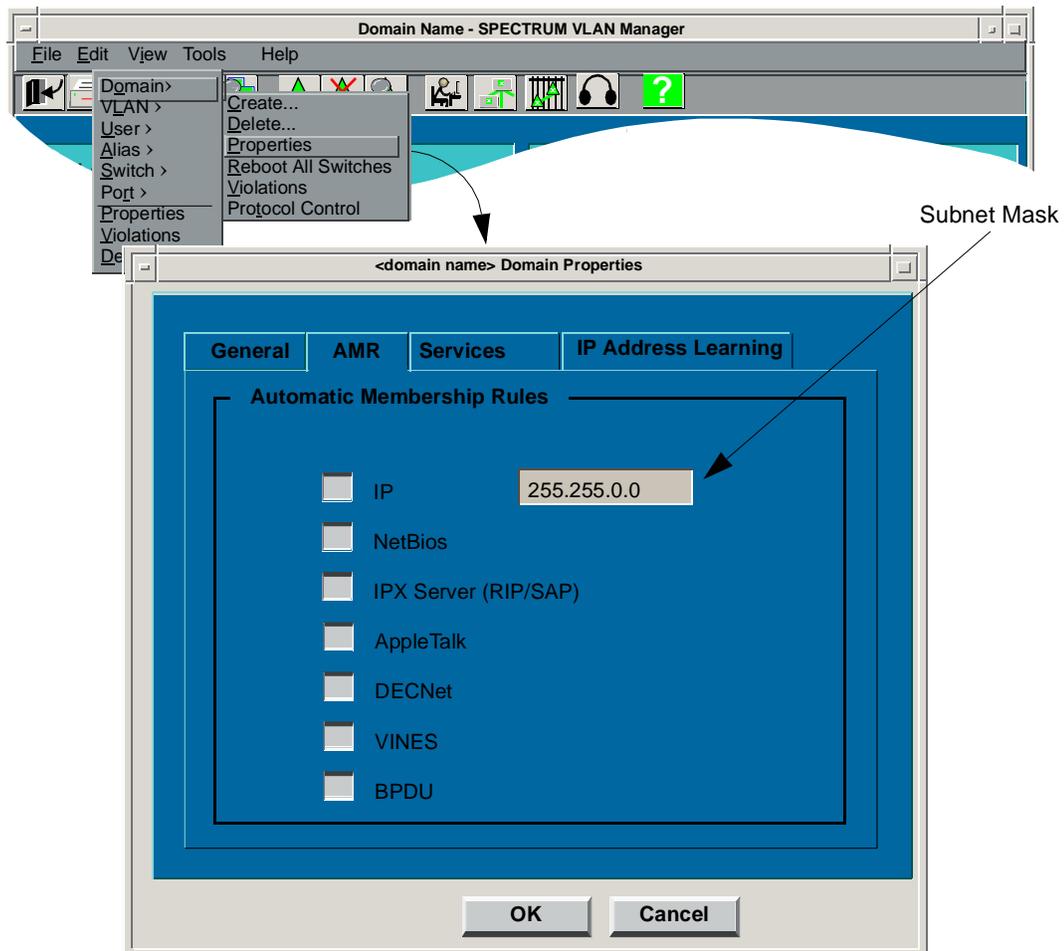
3. Continue the Discovery Wizard procedure. Refer to *VLAN Manager Domain Discovery Wizard*, on page 6-1.

Enabling AMR VLANs Using Domain Properties

To enable AMR VLANs by using the Domain Properties tabbed folder:

1. Select **Properties** from the **Edit > Domain** menu.
2. Click the **AMR** tab to display the AMR tabbed page (Figure 9-12).

Figure 9-12. AMR Configuration



3. Click the type of AMR VLANs you want to enable. A type is selected when its corresponding button is recessed (down). You can select as many types as you want. [Figure 9-12](#) shows all types selected. Refer to [Enabling AMR VLANs](#), Step 2, for information about dynamically creating AMR VLANs.
4. Click another tab to set additional domain properties, **OK** to set domain properties and dismiss window, or **Cancel** to dismiss the SPECTRUM VLAN Manager's Domain Properties window without making domain property changes.

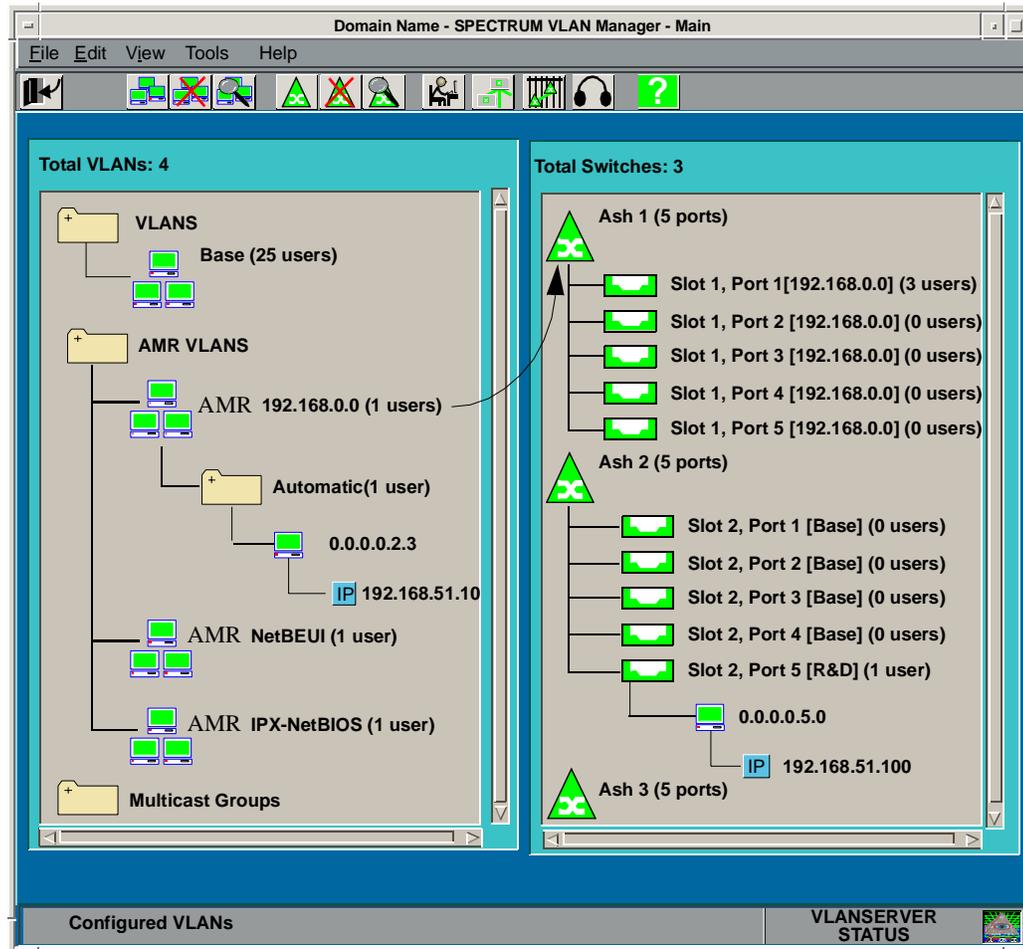
Displaying AMR VLANs

[Figure 9-13](#) shows the VLAN Manager's Main window with three AMR VLANs in the left window pane. The  AMR icon is used to distinguish AMR VLANs from other VLANs.



1. A user learned by an AMR VLAN is not removed from the Base VLAN.
2. You can drag a user (regardless of AMR type) into any VLAN. When you do this, the user does not get removed from its AMR VLAN. It gets removed from its inherited VLAN. For example, a user in an IP AMR VLAN is also in the Base VLAN. If the user is dragged from the IP AMR VLAN into another VLAN, for instance, a Red VLAN, it is not removed from the IP AMR VLAN. It is however removed from the Base VLAN.
3. An AMR VLAN is not deleted automatically. You must use VLAN Manager's VLAN Delete function to delete it. If you delete an AMR VLAN, it will be re-created automatically if a broadcast packet of that type is detected and if that type of AMR VLAN is enabled.
4. By default, only related aliases are displayed for a particular AMR VLAN. You can choose to have all aliases displayed. Refer to [Main Preferences on Page 5-3](#).

Figure 9-13. Displaying AMR VLANs



You can drag an AMR VLAN icon onto a switch or port icon, changing the default VLAN for the switch or port to that of the AMR VLAN. For instance, if you drag the AMR 192.168.0.0 icon onto the ASH 1 switch icon (Figure 9-13), the default VLAN for all the ports on that switch becomes AMR 192.168.0.0. All endpoints connected to that switch or port inherit the properties of that AMR VLAN.

Managing Users

This chapter provides step-by-step instructions for performing user administration tasks, using SPECTRUM VLAN Manager's graphical user interface. It also contains reference information and helpful tips to help you to perform these tasks.

Overview

You manage users (and user Layer 3 aliases) from the **Edit** menu, the **View >User** menu, the **Directory**, the pop-up menus available from the VLAN and Switch window panes, and the VLAN Details window.

The first part of this chapter provides information about managing users from the **Edit** and **View >User** menus. The remainder of the chapter provides information about managing users from the **Directory**. Alternate ways of initiating user management tasks are provided where applicable.

Creating a User

Normally, users are discovered automatically when discovery runs at its regular poll intervals, however, there may be times when you want to create users before the users are actually physically connected to the network. The **Create User** function lets you do this.

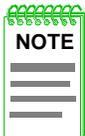
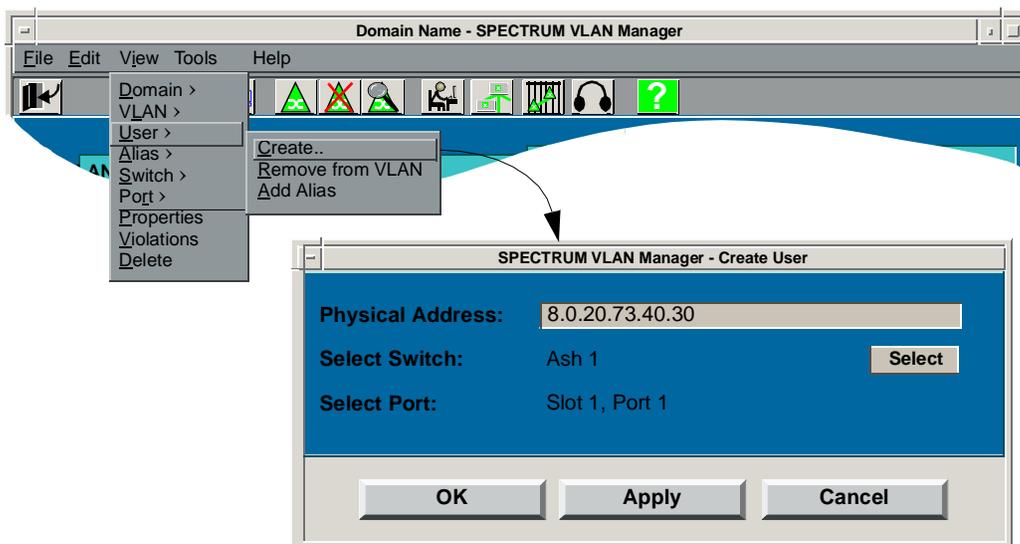
To create a user (Figure 10-1):

1. Select **Create** from the **Edit >User** menu to display the SPECTRUM VLAN Manager - Create User dialog box.



This operation can also be initiated from the Directory's **Edit** menu.

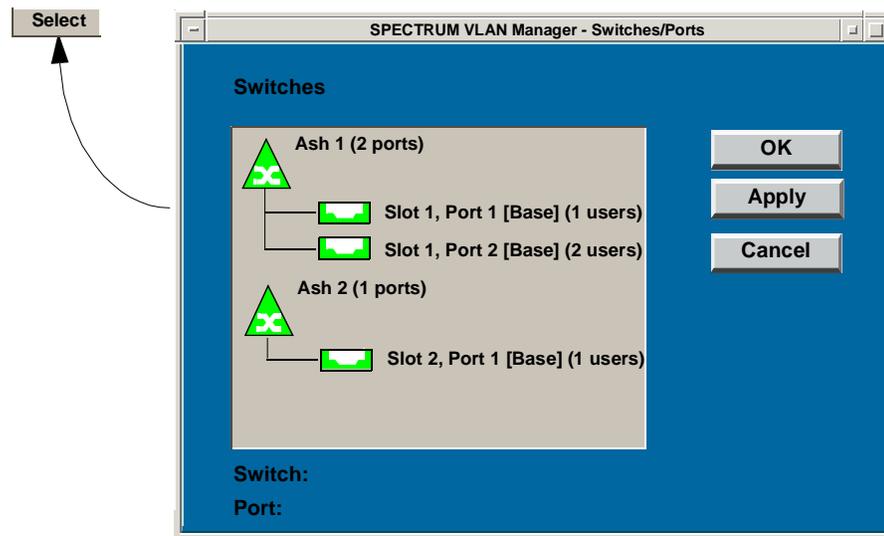
Figure 10-1. Creating a New User



Duplicate user MAC addresses are not allowed within the same domain. When duplicate user MAC addresses are detected on more than one switch in a domain, both users are deleted by the VLANServer. The user that is actually generating data will be relearned.

2. Enter the MAC address of the new user in the **Physical Address** text box. Use a period (.) to delimit the address.
 - To select the switch to which the user is attached:
 - a. Click **Select**. The Switches/Ports dialog box is displayed (Figure 10-2).
 - b. Choose a switch and port from those shown in the **Switches/Ports** tree. The highlighted switch and port are identified at the bottom of the window.
 - c. Press **OK** to select the switch and port and close the window, **Apply** to select the switch and port and leave the window open, or **Cancel** to dismiss the SPECTRUM VLAN Manager's Switches/Ports dialog box.

Figure 10-2. Switch Selection List



3. Press **OK** to create a new user and close the window, **Apply** to create a new user and leave the window open, or **Cancel** to dismiss the SPECTRUM VLAN Manager: Create User dialog box without adding a user.

Removing a User from a Switch

To remove a user from a switch (Figure 10-3):

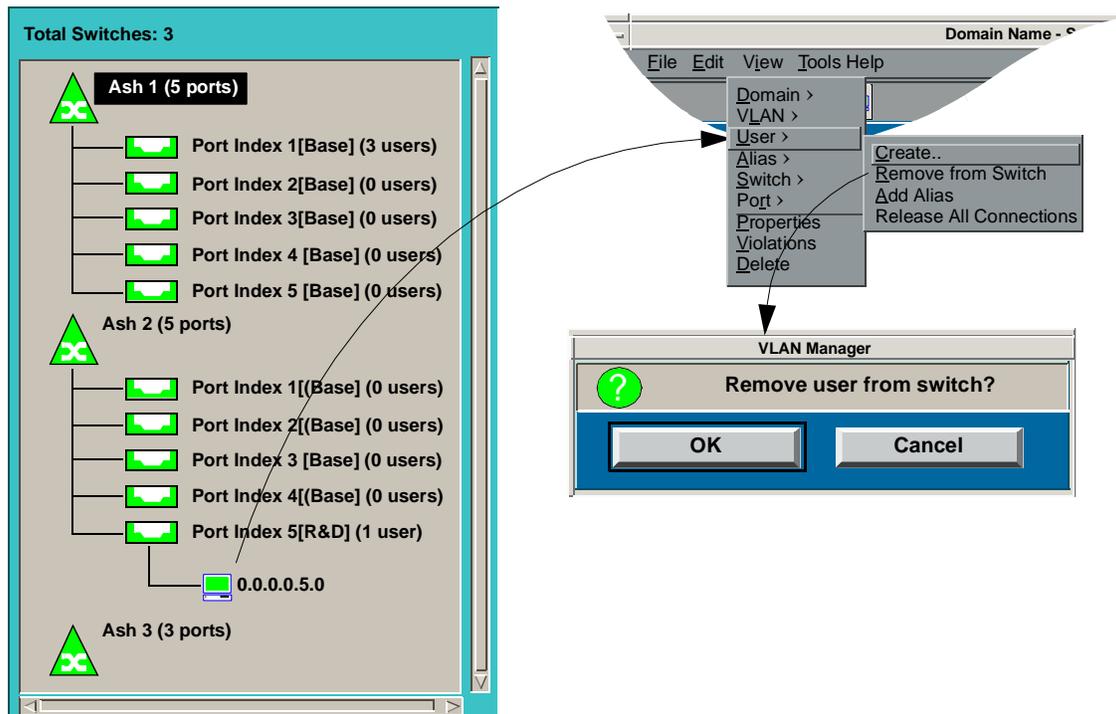
1. In the switch window pane, click on the user you want to remove.
2. Select **Remove from switch** from the **Edit > User** menu.



This operation can also be initiated from the User pop-up menu.

3. Click **OK** in the VLAN Manager confirmation box to confirm that you want to remove the selected user. The user(s) is greyed-out of all VLANs in which that user has membership and removed from the physical pane. Since the VLANServer remembers which VLANs the user has membership in, VLAN membership is automatically reestablished when the user is re-discovered. If you press the **Cancel** button, you will return to the VLAN Manager window without making any changes.

Figure 10-3. Removing a User from a Switch



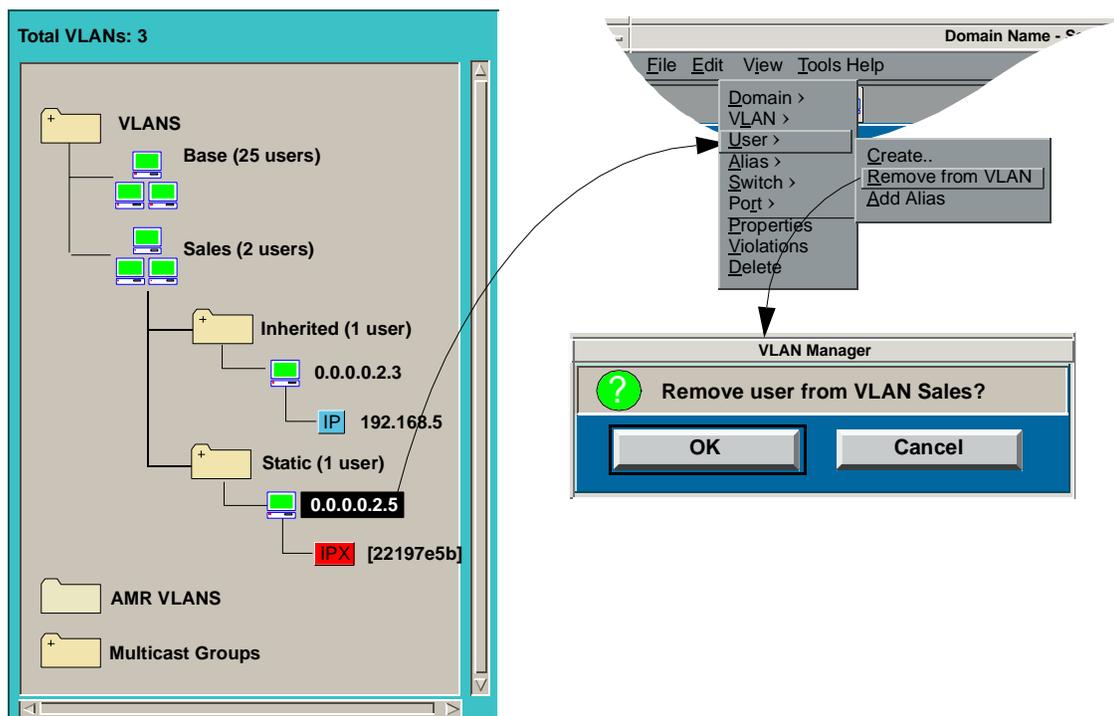
Removing Users from a VLAN

To remove users from a VLAN (Figure 10-4):



1. You cannot remove a user from the Base VLAN.
 2. This operation can also be initiated from the VLAN Details window.
-
1. In the VLAN window pane, click on the name of the user you want to remove from the VLAN it is a member of.
 2. Select **Remove from VLAN** from the **Edit > User** menu. Confirm that you want to remove the selected user by pressing the **OK** button in the VLAN Manager confirmation box. A user that is removed is returned to the port's Default VLAN unless it has membership in other VLANs. If you press the **Cancel** button, you will return to the VLAN Manager window without making any changes.

Figure 10-4. Removing a User from a VLAN



Deleting a User



All user and alias restrictions must be removed before a user can be deleted. If you attempt to delete a user without first removing all of its user and alias restrictions, VLAN Manager will display a message indicating that the user or one of its aliases is restricted. If you continue, all restrictions for the user and its aliases will be removed before the user is deleted.



If you are deleting a user or users configured as persistent, you will see a message informing you of this, letting you know that deleting the user(s) disables persistence for those users, and giving you the option of backing out. Deleting the user(s) disables the persistence feature for the deleted users only.

To delete a user (Figure 10-5):

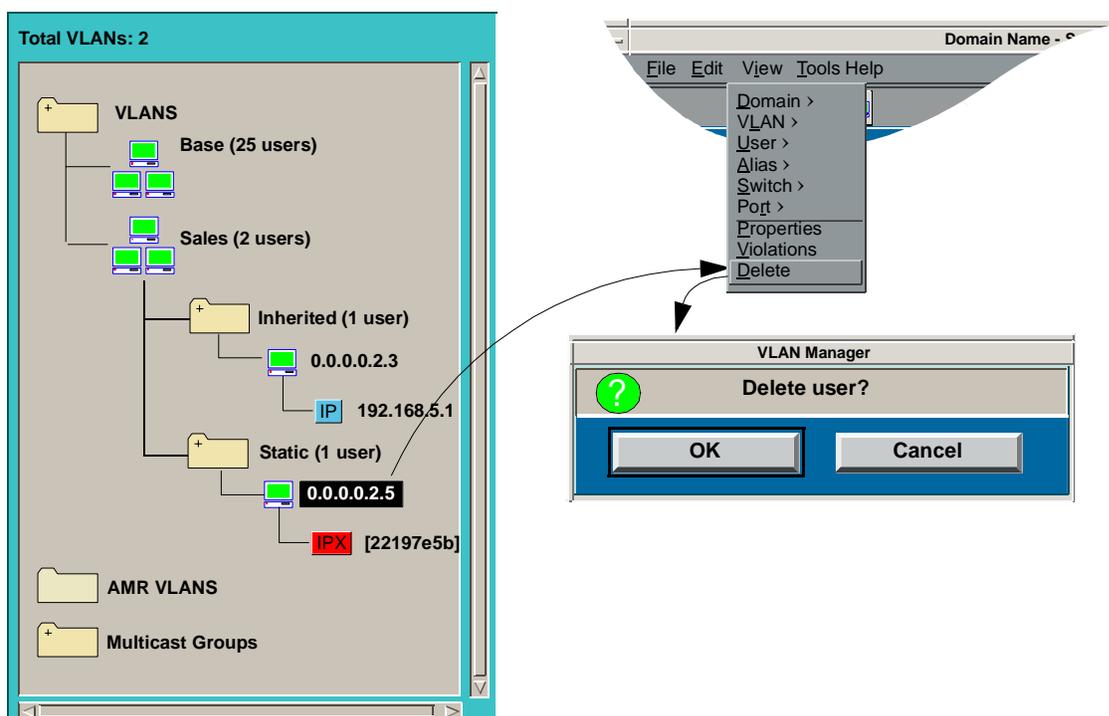
1. In the logical or physical window pane, click on the name of the user you want to delete.

2. Select **Delete** from the **Edit** menu. Click **OK** in the VLAN Manager confirmation box to confirm that you want to delete the selected user. All information about the user is deleted from the VLANServer database and from the switch and all connections the user is part of are torn down. If you press the **Cancel** button, you will return to the VLAN Manager window without making any changes.



This operation can also be initiated from the VLAN pop-up menu, the Switch pop-up menu, VLAN Details, or from the Directory.

Figure 10-5. Deleting a User



User Properties

The User Properties tabbed folder (Figure 10-6) consists of three tabbed pages: **General**, **VLAN Membership**, and **Restrictions**. These pages give you a snapshot of a selected user's attributes. You can edit many of the attributes displayed for a particular page.

To display the User Properties tabbed folder:

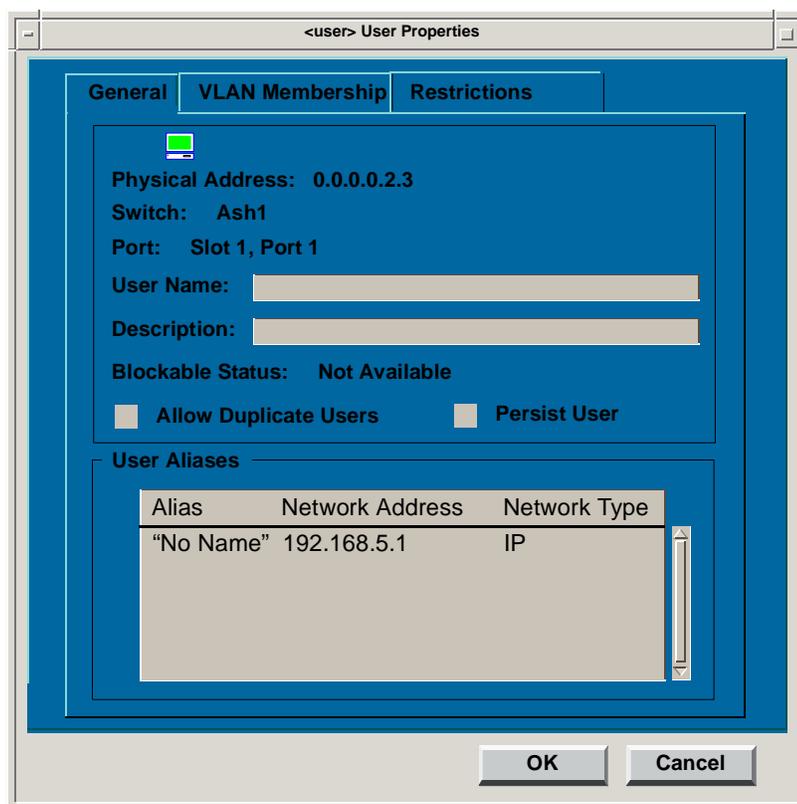
1. Click on a user entry in the VLAN Manager Main window, the Directory, or the VLAN Details window.

2. Select **Properties** from the **Edit** menu.
3. To display a particular tabbed page, click on its corresponding tab. **General** is displayed by default.

General

The **General** tabbed page (Figure 10-6) displays general information about the selected user.

Figure 10-6. User Properties



The screenshot shows a window titled "<user> User Properties" with three tabs: "General", "VLAN Membership", and "Restrictions". The "General" tab is active. It contains a green status indicator, a "Physical Address" field with the value "0.0.0.0.2.3", a "Switch" field with "Ash1", a "Port" field with "Slot 1, Port 1", a "User Name" text box, a "Description" text box, and a "Blockable Status" field with "Not Available". Below these are two checkboxes: "Allow Duplicate Users" and "Persist User", both of which are unchecked. A "User Aliases" section contains a table with three columns: "Alias", "Network Address", and "Network Type". The table has one row with the values "No Name", "192.168.5.1", and "IP". At the bottom of the dialog are "OK" and "Cancel" buttons.

Alias	Network Address	Network Type
"No Name"	192.168.5.1	IP

Physical Address - User's MAC address.

Switch - Switch to which the user is connected.

Port - Port to which the user is connected.

User Name - Name of the user. You can edit this field.

Description - Description of the user. You can edit this field.

Blockable Status - Indicates whether or not source blocking is enabled for this user (the node has been designated as blockable in the Source Configuration Table).

Possible values are:

- Blockable - Source blocking is allowed on the MAC address of this user.
- Not Blockable - Source blocking is not allowed on the MAC address of this user.
- Not Available - User is not in the Source Configuration Table.
- Blank - User is not associated with a switch (i.e., it is a “gray” user).

To set the status as Blockable or Non Blockable, use the Element Management Source Blocker Configuration tool on the **Tools >SecureFast Tools** menu. (See Source Blocker Configuration in the *SecureFast Tools Guide* for more information on this tool.) If the status is not set with this tool, the Blockable Status field displays Not Available.

User Aliases - A list of aliases for the user (see *Adding a User Alias*, on page 10-10 for more information).

To edit the **User Name** or **Description** fields, click anywhere in a field and then enter the desired text, or swipe the text you want to change and type the new text.

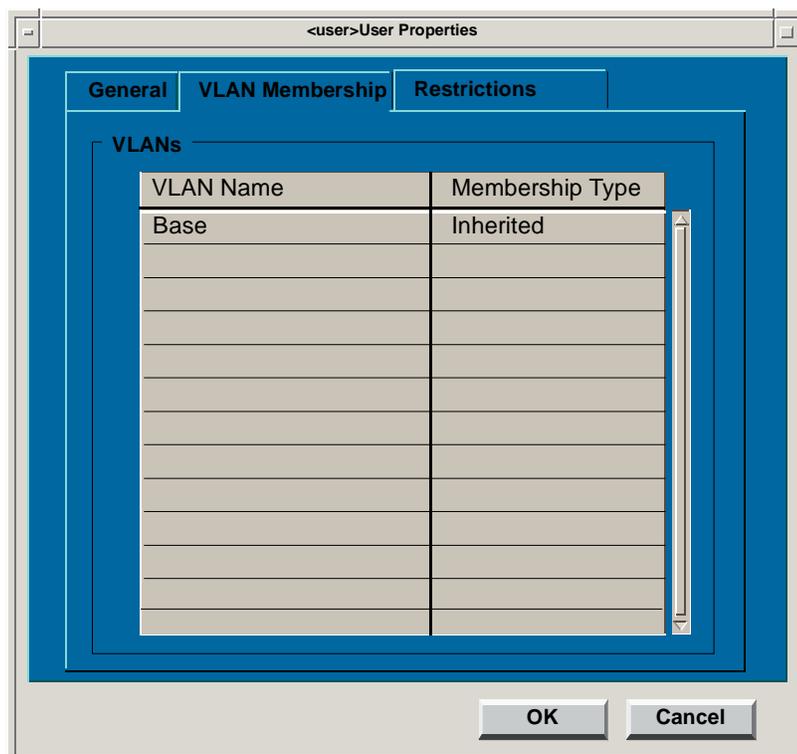
To allow duplicate MAC addresses for this user in other domains, click (depress) the **Allow Duplicate Users** button. To turn this feature off for this user, click the button to raise it.

To enable User Persistence for this user, click (depress) the **Persist User** button. To turn this feature off for this user, click the button to raise it. You can enable and disable User Persistence for multiple users in a domain using the User Persistence tab in the Domain Properties window. See *User Persistence*, on page 6-26, for more information on how to do this, and on User Persistence in general.

VLAN Membership

The **VLAN Membership** tabbed page (Figure 10-7) displays the name and type of each VLAN in which the user has membership. VLAN types are: Inherited, Static, and Automatic.

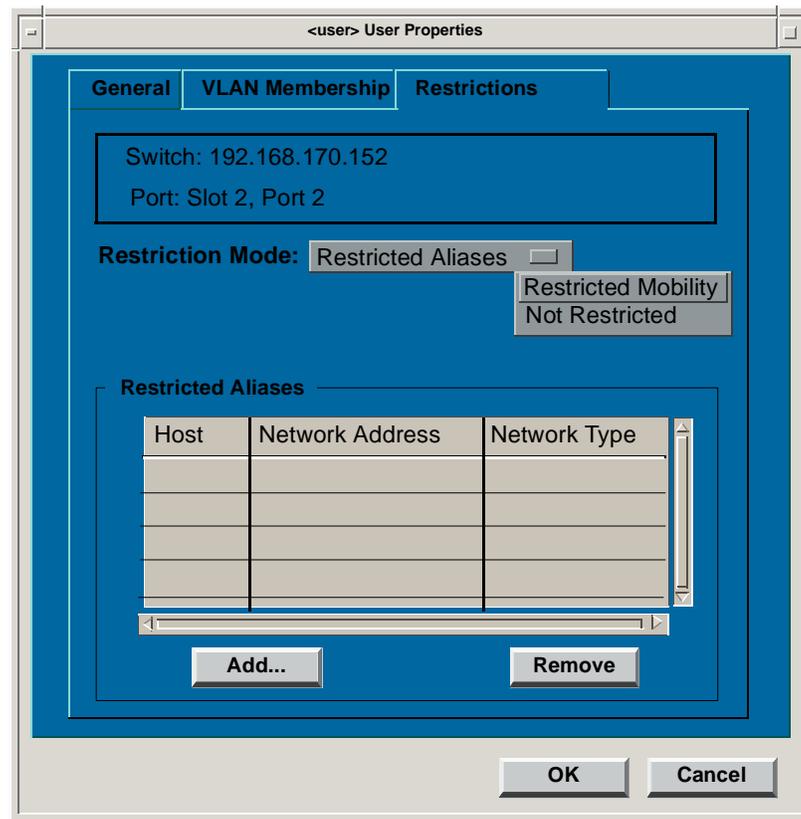
Figure 10-7. User Properties (VLAN Membership)



Restrictions

The **Restrictions** tabbed page (Figure 10-8) displays the following information about a user: the switch and port to which the user is connected, the restriction mode, and a table of aliases and types. From this page you can select one of three user restriction modes, **Restricted Aliases**, **Restricted Mobility**, or **Not Restricted**. For detailed information about how to restrict a user, refer to *User Restrictions*, on page 10-25.

Figure 10-8. User Properties (Restrictions)



Adding a User Alias

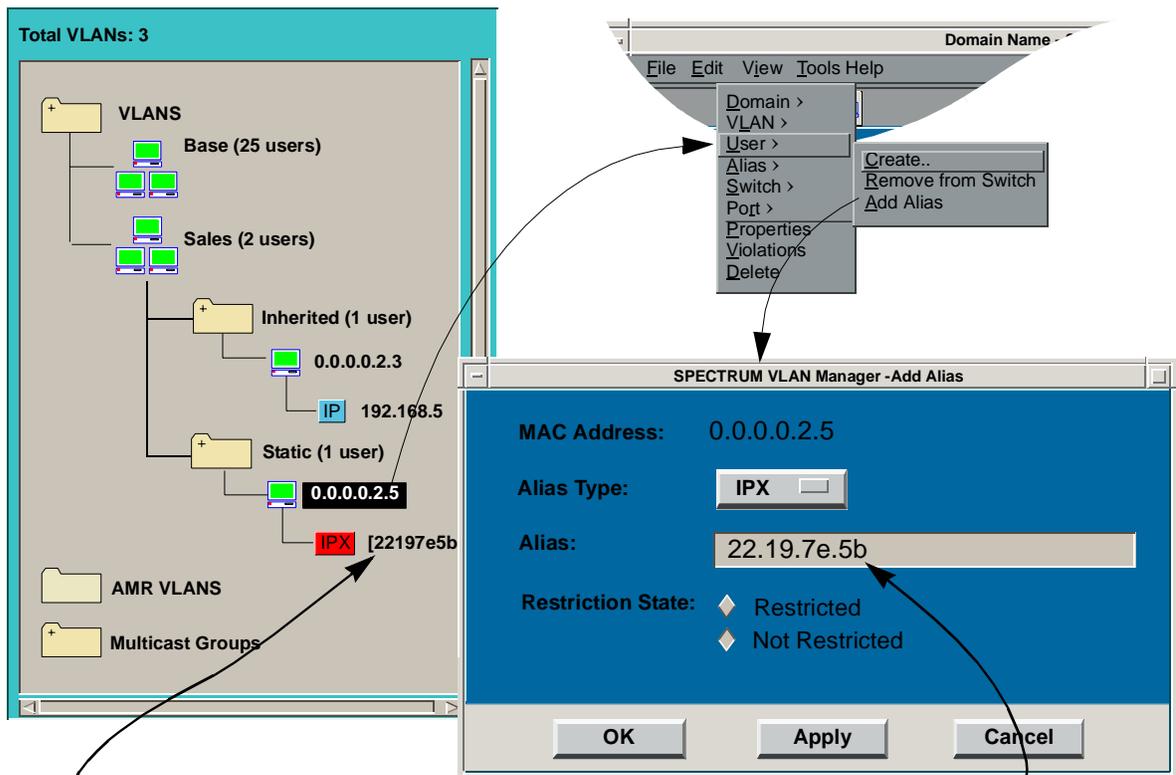
To add a user alias (Figure 10-9):

1. In the logical or physical window pane, click on the user to which you want to add an alias.
2. Select **A**dd **A**lias from the **E**dit > **U**ser menu to display the Add Alias window.



This operation can also be initiated from the Directory's Edit menu, VLAN Details, or Directory pop-up menus.

Figure 10-9. Adding a User Alias



Please note that when adding an alias in the Add Alias window, the network number should be entered in the ##.##.##.## format.

When the alias appears in the logical or physical window pane it is displayed in the ##### format.

3. Select the alias type for the new alias by clicking on the Alias Type button and dragging the cursor to the type of alias you want to add. The default alias type is “**IP**”. Other types are **IPX**, **AppleTalk**, and **NetBIOS**.
4. Enter the address of the alias into the **Alias** text box. The correct syntax for the type of alias selected must be used.



If an alias is restricted to a user, then the user associated with that alias also becomes restricted.

5. Choose whether this alias will be restricted to the port to which it is connected. The default is **Not Restricted**.



You can remove an alias by clicking on a user's alias and then using the Remove Alias pop-up menu. This operation can also be initiated from the Directory's pop-up menu and the **Edit >Alias** menu.

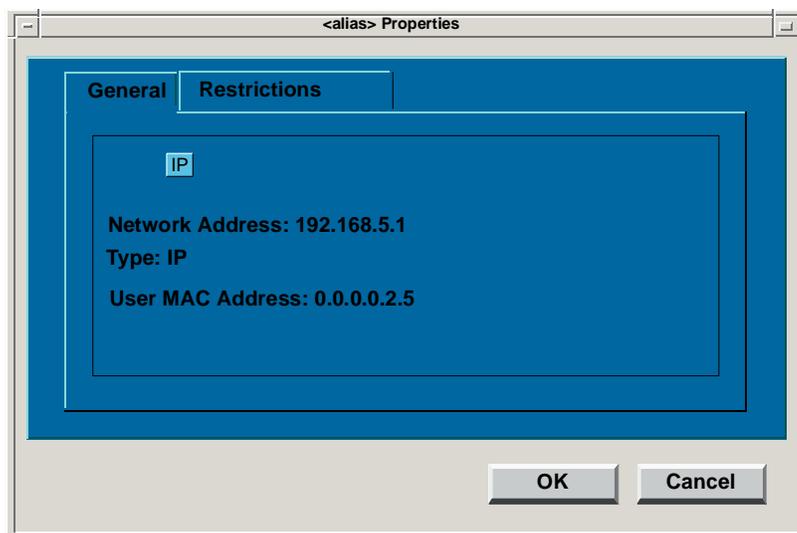
User Alias Properties

The Alias Properties tabbed folder ([Figure 10-10](#)) consists of the following tabbed pages: **General** and **Restrictions**. These pages provide you with a snapshot of a user alias's attributes. Some of the attributes displayed can be edited, others are read-only. To display the Alias Properties tabbed folder, click on a user alias entry in the VLAN Manager Main window and then select **Properties** from the **Edit** menu. To display a particular tabbed page, click on its corresponding tab. **General** is displayed by default.



This operation can also be initiated from the alias pop-up menu.

Figure 10-10. Alias Properties



General

The **General** tabbed page (Figure 10-10) displays the following information about a user: alias name, network address, type, and MAC address. All fields are read-only.

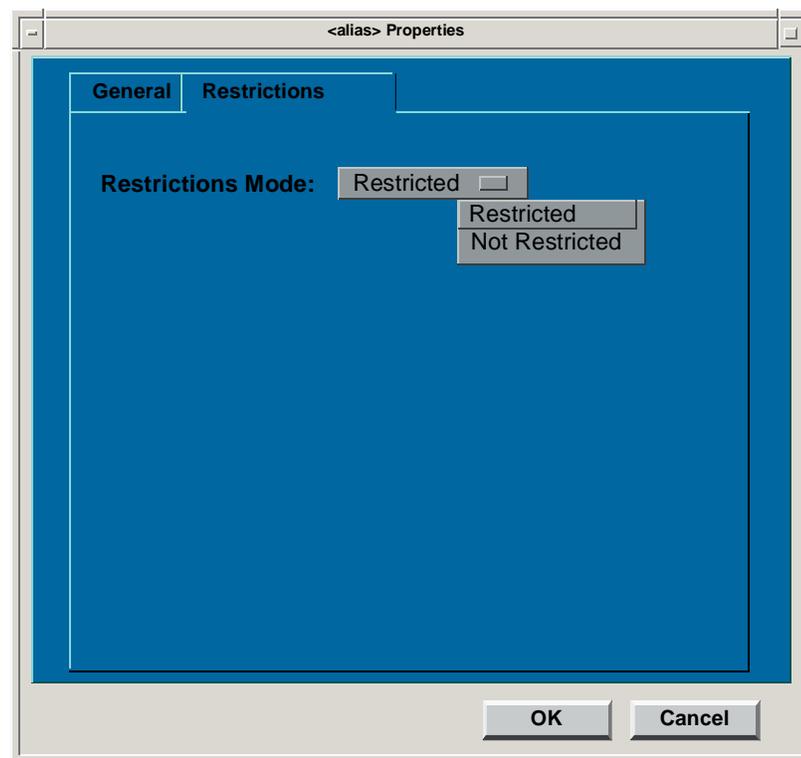
Restrictions

The **Restrictions** tabbed page (Figure 10-11) displays the state of the alias (Restricted or Not Restricted).

To edit alias restrictions:

1. Choose an alias restriction and then click **Restricted/Not Restricted**.
2. Click **OK** to accept changes and close the window, or **Cancel** to dismiss the window without making changes.

Figure 10-11. Alias Properties (Restrictions)



Viewing Connection Information

The **View > User** menu consists of the following item: **Connection Table**.

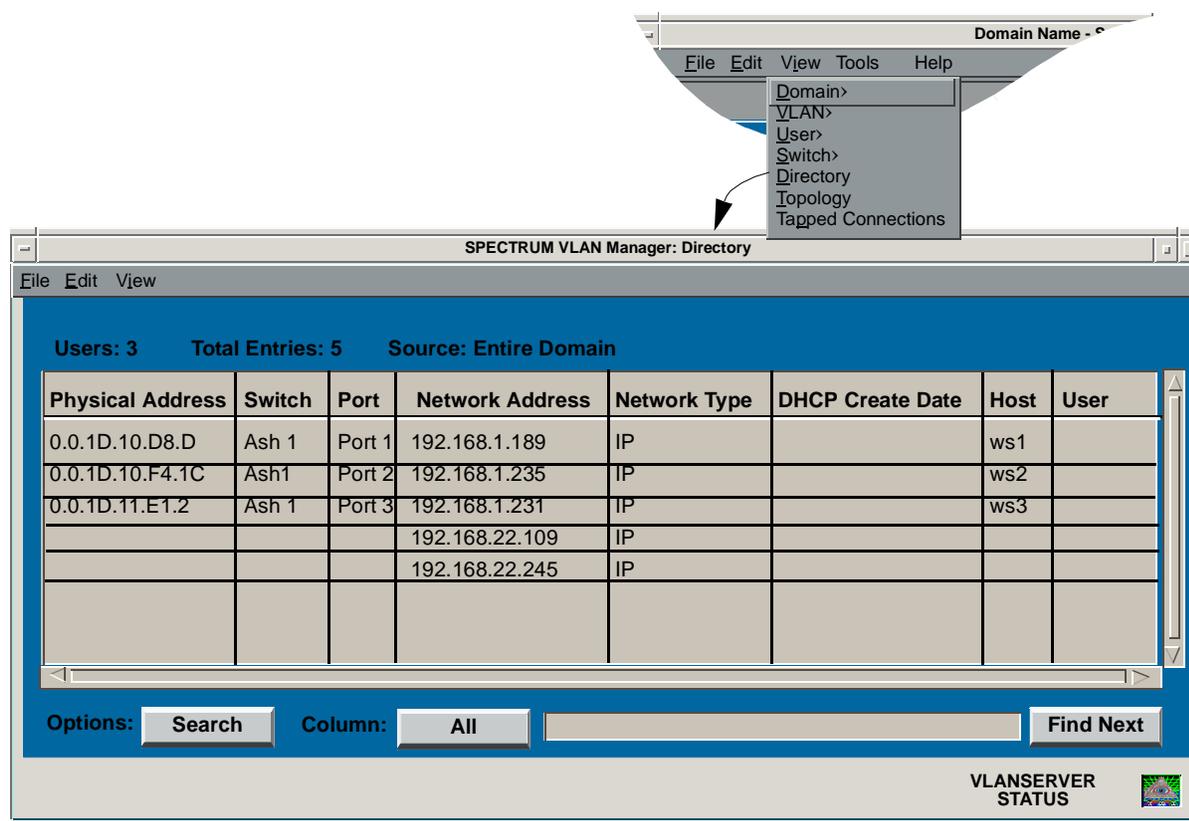
- **Connection Table** - Lets you view connection information for a particular call. Refer to [Chapter 11, *Managing Connections*](#), for detailed information about the Connection Table.

Using the Directory

The Directory provides information about each user having membership in the current domain. Commands launched from the menu bar or pop-up menu let you perform user related operations. A search/filter feature accessible from the window lets you find a particular user or group of users quickly without having to parse through the entire list.

To list all users in a VLAN domain ([Figure 10-12](#)), select **Directory** from the **View** menu or click  in the Tool Bar. The SPECTRUM VLAN Manager's Directory window is displayed.

Figure 10-12. Directory Window



The Directory window consists of a menu bar, a users list, search/filter options, and the VLANServer Status indicator.

Directory Menus

The menu bar consists of three menus: **F**ile, **E**dit, and **V**iew. Each menu provides access to additional selections.

- **F**ile - consists of three selections: **S**ave, **I**mport, and **C**lose.
 - **S**ave - Lets you save the contents of the directory to a file. Refer to [Save, on page 10-20](#).
 - **I**mport - Lets you import user profiles into the VLANServer database. Refer to [Import, on page 10-23](#).
 - **C**lose - Close the Directory view.
- **E**dit - consists of the following selections: **C**reate User, **D**elete User(s), **P**roperties, **R**emove User(s) from Switch, **A**dd Alias, **R**emove Alias, **R**elease All Connections for User, and **U**ser **V**iolations.
 - **C**reate User - Lets you create a new user in the current domain. Refer to [Creating a User](#), on page 10-1.
 - **D**elete User(s) - Lets you delete a user from the current domain. Refer to [Deleting a User](#), on page 10-5.
 - **P**roperties - Lets you view and/or edit user attributes. Refer to [User Properties](#), on page 10-6.
 - **R**emove User(s) from Switch - Lets you remove users in the current domain from their switch associations.
 - **A**dd Alias - Lets you add a network alias (e.g., IP, IPX) to a user. Refer to [Adding a User Alias](#), on page 10-10.
 - **R**emove Alias - Lets you remove a network alias (e.g., IP, IPX) from a user. Refer to [Adding a User Alias](#), on page 10-10.
 - **R**elease All Connections for User - Lets you remove all active calls for the selected user.
 - **U**ser **V**iolations - Displays the Violations Table for the selected user. Refer to [Violations](#), on page 10-32.
- **V**iew - consists of two selections: **C**onnection **T**able and **U**ppdate **D**uplicates.
 - **C**onnection **T**able - Launches the Connection Table filtered for the selected user. Refer to [Chapter 11, Managing Connections](#).
 - **U**ppdate **D**uplicates - Updates the Duplicate Address window.

Users List

The users list displays information about all users with membership in the current domain. Each line in the list provides information associated with a specific source endpoint (user). A scroll bar to the right of the table allows you to scroll through the table.

- **Physical Address** - MAC address of the endpoint.
- **Switch** - Name of the switch to which the endpoint is connected. If DNS is not being used, this will be the network address of the switch or the name you have assigned through Switch Details.
- **Port** - Port label of the switch on which the endpoint is heard.
- **Network Address** - Network address of the endpoint.
- **Network Type** - IP, IPX, AppleTalk, or other.
- **DHCP Create Date** - Date dynamic IP address for this user was issued.
- **Host** - Name assigned to the endpoint. Hosts are resolved through DNS from the IP address.
- **User** - Name you assign to the endpoint.
- **Restrictions** - Yes or No.
 - **Yes** - User is restricted to one port.
 - **No** - User is not restricted to a specific port.



If any of a user's aliases are restricted, the user is restricted to its port and the **Restrictions** would be **Yes**.

- **Create Date** - Date user was originally created in the VLANServer database.
- **Persisted** - Indicates whether or not the user is persisted. (See *User Persistence*, on page 6-26 for more information on persisted users.)
 - **Yes** - User is persisted.
 - **No** - User is not persisted

Creating a User

To create a user, select **Create User** from the Directory's **Edit** menu and then refer to *Creating a User*, on page 10-1.

Deleting a User

To delete a user:

1. Click on the user entry for the users that you want to delete in the Directory window. (Hold down the **Control** key, and then click on users to select multiple users.)



You can use the Filter feature to quickly isolate a group of users to delete.

2. Select **Delete Users** from the Directory's **Edit** menu to delete selected users.



This operation can also be initiated from the Directory pop-up menu.

Editing User Properties

3. To edit user property information, click **Properties** from the Directory's **Edit** menu and then refer to *User Properties*, on page 10-6.



This operation can also be initiated from the Directory pop-up menu.

Removing Users from a Switch

To remove users from a switch:

1. Click on the user entry for the user that you want to remove in the Directory window. (Hold down the **Control** key, and then click on users to select multiple users.)



You can use the Filter feature to quickly isolate a group of users to remove.

2. Select **Remove Users from Switch** from the Directory's **Edit** menu to remove the selected users.



This operation can also be initiated from the Directory pop-up menu and the Switch User pop-up menu.

Adding/Removing a User Alias



All user alias restrictions must be removed before an alias can be removed. If you attempt to remove an alias without first removing all of its restrictions, VLAN Manager will display a message indicating that the alias is restricted. If you continue, all restrictions for the alias will be removed before the alias is removed.

To add or remove a user alias, click **Add Alias** or **Remove Alias** from the Directory's **Edit** menu and then refer to *Adding a User Alias*, on page 10-10.



Add Alias can also be initiated from the Directory pop-up menu. Remove Alias can also be initiated from the Directory pop-up menu.

Directory Pop-up Menu

The Directory pop-up menu lets you perform the following operations: view and edit user properties, delete users, add and remove aliases, display the Connection Table, view user violations.

- **Properties** - Lets you view and/or edit user attributes. Refer to *User Properties*, on page 10-6.
- **Add Alias** - Lets you add a network alias (e.g., IP, IPX) to a user that is running more than one protocol. Refer to *Adding a User Alias*, on page 10-10.
- **Remove Alias** - Lets you remove a network alias. Refer to *Adding a User Alias*, on page 10-10.
- **Remove User(s) from Switch** - Lets you remove selected users from a switch. Refer to *Removing Users from a Switch*, on page 10-17.
- **Connection Table** - Displays the Connection Table for the selected user. Refer to [Chapter 11, Managing Connections](#).
- **User Violations** - Displays the Violations Table for the selected user. Refer to *Violations*, on page 10-32.
- **Delete User(s)** - Lets you delete selected users from the VLANServer database and switch. Refer to *Deleting a User*, on page 10-17.

Using the Search/Filter Options

Use the **Search/Filter** button to find a particular user or group of users. You can search or filter by any column of the table. You can also filter by **None**, which returns the table to the non-filtered state.

To use **Search/Filter**:

1. Select **Search** or **Filter** from the **Options** list and then select the search or filter criteria from the **Column** list.
2. Click anywhere in the **Column** text box and then enter the text to be matched.
 - **Search** - Finds and highlights the first instance of a user that matches the search criteria. Click **Find Next** to find subsequent instances of users that match the same criteria.
 - **Filter** - Selectively eliminates entries from the Directory that do not match the filter criteria. Only users that match the filter criteria are displayed.



To filter to IP when filtering on Network Type, press the space bar or type IP, and then press the space bar and then the RETURN key. This eliminates all protocols except IP.

Finding Duplicate Network Addresses

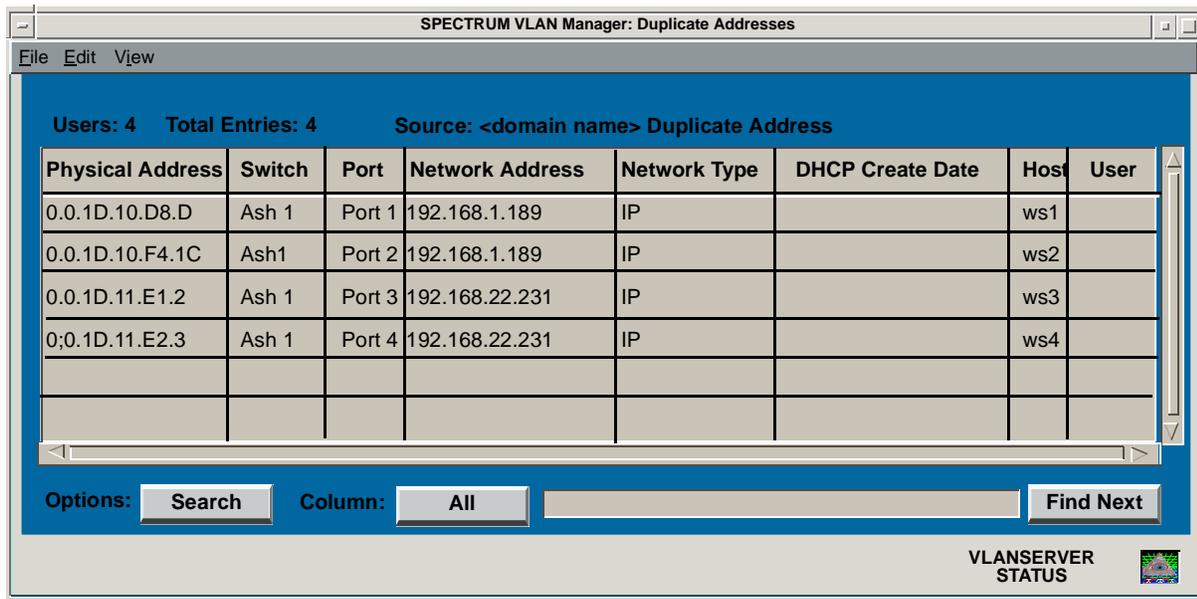
Finding and eliminating duplicate network addresses is essential to ensuring trouble-free operation of your network. Endpoints on your network using the same network address will have problems communicating with other endpoints and the reason is often not obvious. VLAN Manager lets you quickly identify duplicate network addresses. You can view all duplicate network addresses or use the filter and search option to find duplicate network addresses for a particular protocol.

To find duplicate addresses, select **Duplicate Addresses** from the **View >Domain** menu. The Duplicate Addresses window ([Figure 10-13](#)) is displayed. It contains information about all endpoints in the current domain with identical network addresses. This window is a filtered version of the Directory view. All fields are the same as those in the Directory.



Use **Search** or **Filter** to filter the duplicate address list to an address type.

Figure 10-13. Duplicate Network Addresses



Save

Save lets you copy the contents of the Directory, Connection Table, or Duplicate Address Table to a file in either of two formats, *Space Delimited* or *Comma Delimited*. Each format is described below.

Space Delimited

The Space Delimited format produces an ASCII tabular text file (Figure 10-14). It is intended to be used when you want to print the file to a printer. You may have to modify print parameters such as font, size, or format to produce the desired output.

Figure 10-14. Space Delimited Format

```
Physical Address Switch Port Network Address Network Type DHCP Create Date Host User Restrictions .....
0.0.1D.10.D8.D Ash 1 Port 1 192.168.1.189 IP ws1
0.0.1D.10.F4.1C Ash 1 Port 1 192.168.1.235 IP ws2
0.0.1D.11.E1.2 Ash 1 Port 1 192.168.1.231 IP ws3
192.168.22.109 IP
```

Comma Delimited

Comma Delimited format produces an ASCII comma delimited text file (Figure 10-15). It is intended to be used when you want to import the file into a spreadsheet. For instance, you may want to import the file into an Excel spreadsheet with the import delimiter set to comma. From there you can use the features of the spreadsheet program to produce a report in whatever format you desire.

Figure 10-15. Comma Delimited Format

Physical Address,Switch, Port,Network Address,Network Type, DHCP Create Date, Host,User, Restrictions,.....

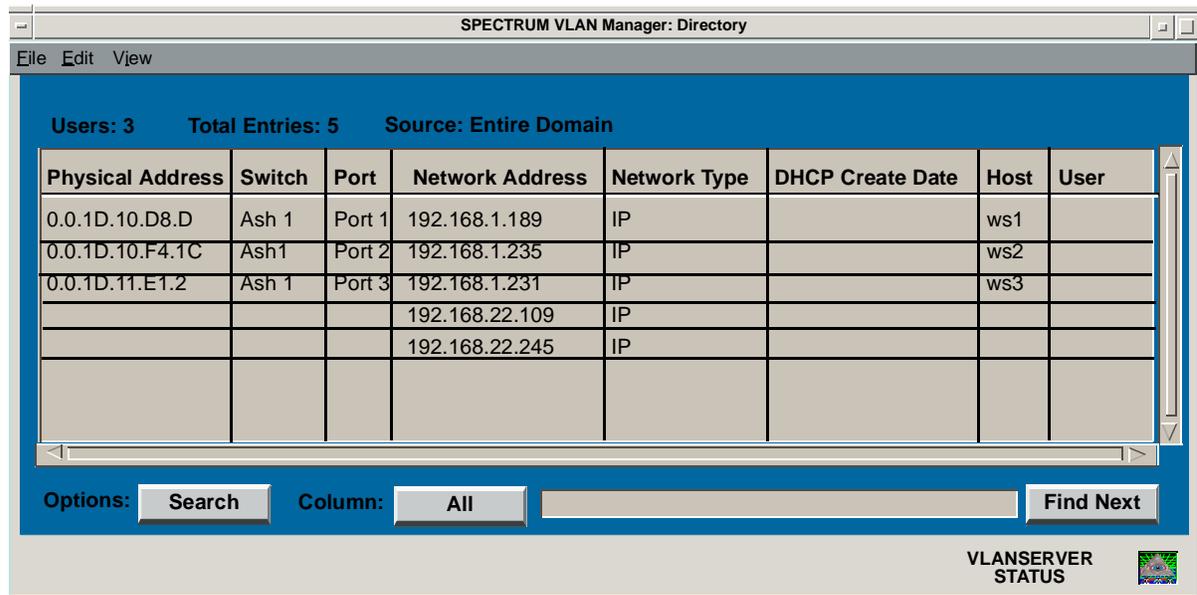
```
0.0.1D.10.D8.D,Ash 1,Port 1,192.168.1.189,IP,,ws1,,,
0.0.1D.10.F4.1C,Ash1,Port 1,192.168.1.235,IP,,ws2,,,
0.0.1D.11.E1.2,Ash 1,Port 1,192.168.1.231,IP,,ws3,,,
,,,192.168.22.109,IP,,,,,
,,,192.168.22.245,IP,,,,,
```

Using Save

To use **Save**:

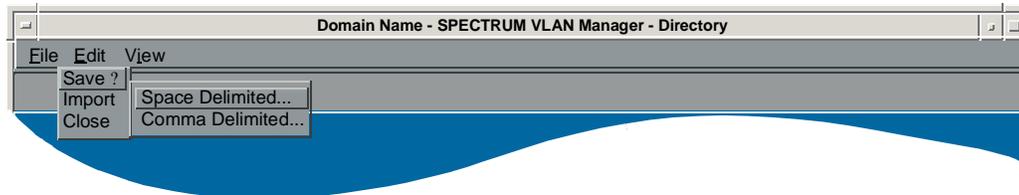
1. Open the Directory or Connection Table. The Directory is shown in Figure 10-16 as an example.

Figure 10-16. Save: Directory Window



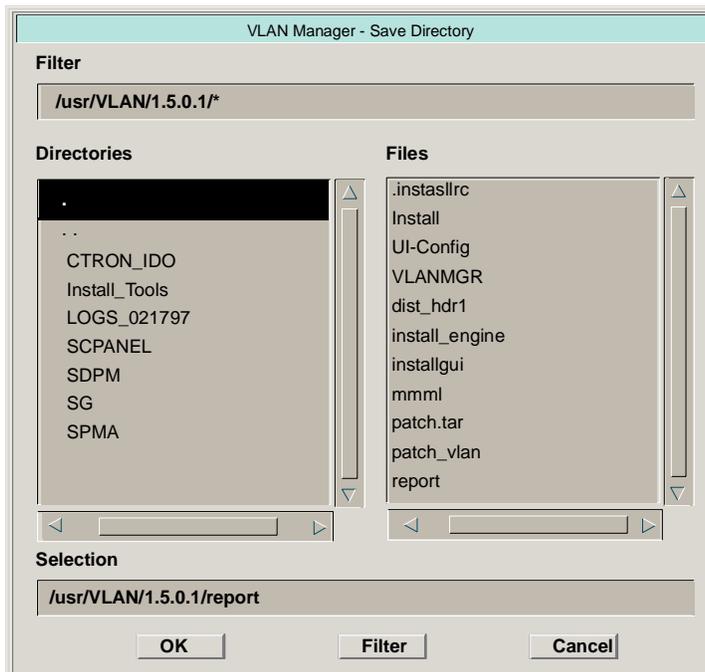
2. Select **Save >Space Delimited** or **Comma Delimited** from the **File** menu. [Figure 10-17](#) shows **Space Delimited** as an example.

Figure 10-17. Save: Space Delimited Menu Selection



The Save Directory window is displayed ([Figure 10-18](#)). This window contains a **Filter** field, a **Directories** list, a **Files** list, a **Selection** field, and **OK**, **Filter**, and **Cancel** buttons.

Figure 10-18. Save Directory Window



- **Filter** - Path you want to use as your filter criteria. You can enter the path directly or build the path by clicking on entries in the directory list. If you enter the path directly, click the **Filter** button to apply the filter. Only directories which match the filter criteria will be displayed in the **Directories** list. Files contained in the filtered path are displayed in the **Files** list.
- **Directories** - All directories in the filtered path. Click an entry to modify the **Filter** field. Double-click an entry to display the contents of a directory.
- **Files** - All files in a selected directory. Click a file name to enter it into the **Selection** field. Double-click an entry to enter it into the **Selection** field and perform the copy.
- **Selection** - Path (including the file name) to which Directory or Connection Table information will be saved. If you want to use a new file name, enter it in this field.



If you save to a file that already exists, its contents will be overwritten. No warning is given. No undo is available.

3. Select or specify the file into which you want to save the contents of the Directory, Connection Table, or Duplicate Address Table. You can use the filter function ([Figure 10-18](#)) to help you find the file.
4. Click **OK** to perform the save or **Cancel** to exit the Save operation without saving the information.

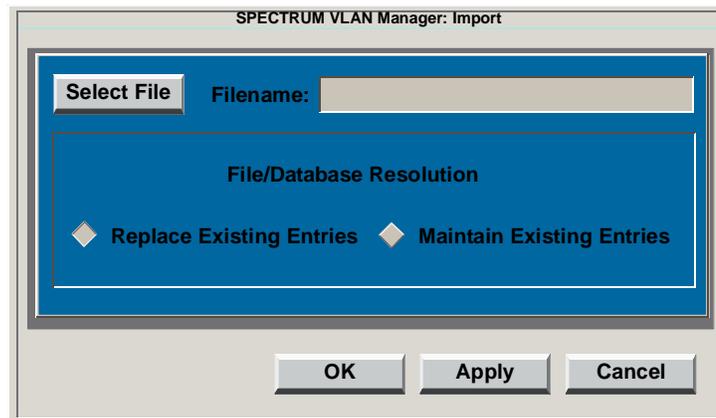


1. You must have write permission for the directory in which you want to save Directory, Connection Table, or Duplicate Address data.
2. Set Preferences to Physical Address before saving Connection Table data. Refer to [Chapter 5, Managing Preferences](#).
3. **Save** saves the current contents of the view. If the information has been filtered or sorted, the resulting file will also be filtered or sorted.

Import

Import lets you copy information about a user or users from an external file into the directory database. This feature lets you add User Name information for users currently in the database without having to add each User Name individually. To launch the import function, click **Import** from the Directory windows **File** menu. The SPECTRUM VLAN Manager's Import window is displayed ([Figure 10-19](#)).

Figure 10-19. File Import



This window consists of the following fields and buttons:

- **Select File** - Lets you browse your file system to find the import file.
 - **Filename** - Import file name field. Type in the file name or use the **Select File** button to browse for the file name.
- **File/Database Resolution** - Determines write behavior in regard to existing entries in the database, as follows:
 - If **Replace Existing Entries** is selected, writes import file information over existing database information.
 - If **Maintain Existing Entries** is selected, ignores import file information and keeps existing database information.
- **OK** - Accepts changes and closes Import window.
- **Apply** - Accepts changes and leaves Import window open.
- **Cancel** - Dismisses Import window without making changes.

Using Import

To read an import file into the directory database:

1. Save the current Directory as a comma-delimited file. Refer to *Using Save*, on page 10-21.



You can manually create the comma-delimited file using your favorite text editor.

2. Import the comma-delimited file into a database or spreadsheet application such as Microsoft Access or Microsoft Excel. The application must support comma delimited import and export.
3. Remove all columns except for Physical Address (MAC) and User Name.
4. Make all Physical Address entries dot (.) delimited.
5. Modify User Name entries.
6. Export to a comma-delimited file. **Do not** include a header line.
7. Import the file into the Directory using **Import**.
 - a. Select **Import** from the Directory's File menu.
 - b. Select the import file. Type the file name into the **Filename** field or click **Select File** to browse for the file name.
 - c. Click **Replace Existing Entries** and then click **OK**.

User Restrictions

VLAN Manager lets you restrict a port using Port Restrictions or a user using User Restrictions. *Restricting a Port*, on page 8-42 explains how you can use Port Restrictions to restrict a port to a certain user(s). This section explains how you can use User Restrictions to restrict users to any number of specified ports (Restricted Mobility) or restrict any or all of a user's aliases to the port to which the user is connected (Restricted Alias).

[Table 10-1](#) provides a short description of each type of restriction and illustrates how each type of restriction affects a user's alias(es) and a user's mobility.

Table 10-1. Types of Restrictions

Type of Restriction	Description	User Alias(es)	User Mobility
Port Restriction	Restricts a port to certain MAC addresses.	User aliases are not considered	User mobility is allowed. Only the users on a port's Port Restriction list can move to the port; however, a user on the list can move to any non-restricted port or to any other port which is restricted to that user's MAC address.

Type of Restriction	Description	User Alias(es)	User Mobility
User Restriction (Restricted Mobility)	Restricts a user (MAC address) to certain ports.	All user aliases associated with the user are locked to the user's MAC address. No other MAC address can use any of the user's aliases.	Some user mobility is allowed. User can move to any port to which it is restricted.
User Restriction (Restricted Alias)	Restricts a user alias to the user.	Any selected user alias associated with the user can be locked to the user's MAC address. No other MAC address can use any of the user's locked aliases.	No user mobility is allowed. User's MAC address is restricted to the port to which the user is connected.

Types of User Restrictions

There are three types of User Restriction modes: **Restricted Alias**, **Restricted Mobility**, and **Not Restricted**.



When a user is restricted, regardless of the type of user restriction, any alias restricted to the user cannot be used by any other device in the domain and will not be learned by any other switch in the domain.

Restricted Alias

Restricted Alias mode prevents a user (MAC address) from using an IP address, or any other alias, that has been restricted to another user. If another user tries to use an alias which has been restricted to another MAC, a restriction violation will be generated. Refer to *Violations*, on page 10-32.

When an alias is restricted to a user, that user is automatically restricted to the port to which it is connected and cannot be moved to another port in the domain. For example, if you restrict IP alias 1.2.3.4 to User A (MAC A.A.A.A.A.A) on Switch 1, Port 1, User A is automatically restricted to Switch 1, Port 1. It cannot be moved to another port and no other device can use IP alias 1.2.3.4.

The information about ports to which a user has been restricted is persistent in the VLANServer database.



1. If Restricted Mobility is re-selected, the user's restrictions will revert to those configured using Restricted Mobility.
2. If a user was restricted using Restricted Alias, but had previously been restricted using Restricted Mobility, when all alias restrictions are removed from the user, the user's restrictions will revert back to those that were previously configured using Restricted Mobility.
3. If a user was restricted using Restricted Alias, but no previous Mobility Restrictions had been configured for the user, the user's restrictions will revert to Not Restricted.

Restricted Mobility

Restricted Mobility mode prevents a user (MAC address) from connecting to ports on the network other than those ports to which the user is restricted. If a user tries to move to a port that it is not restricted to, a restriction violation will be generated. Refer to *Violations*, on page 10-32.

When a user is restricted using Restricted Mobility, all aliases associated with the user are restricted to the ports to which the user is restricted and the user can only move to the ports to which it is restricted. Any previously restricted aliases will be lost since all aliases associated with the user are locked to the restricted mobility ports. For example, if you restrict User A (MAC A.A.A.A.A.A) to Switch 1, Ports 1 and 2, User A cannot move to any ports other than ports 1 and 2 and User A's alias (IP address 1.2.3.4) cannot be used by any other device in the domain.



Mobility restrictions are not enforced across domains.

Not Restricted

All restrictions for the user are removed.



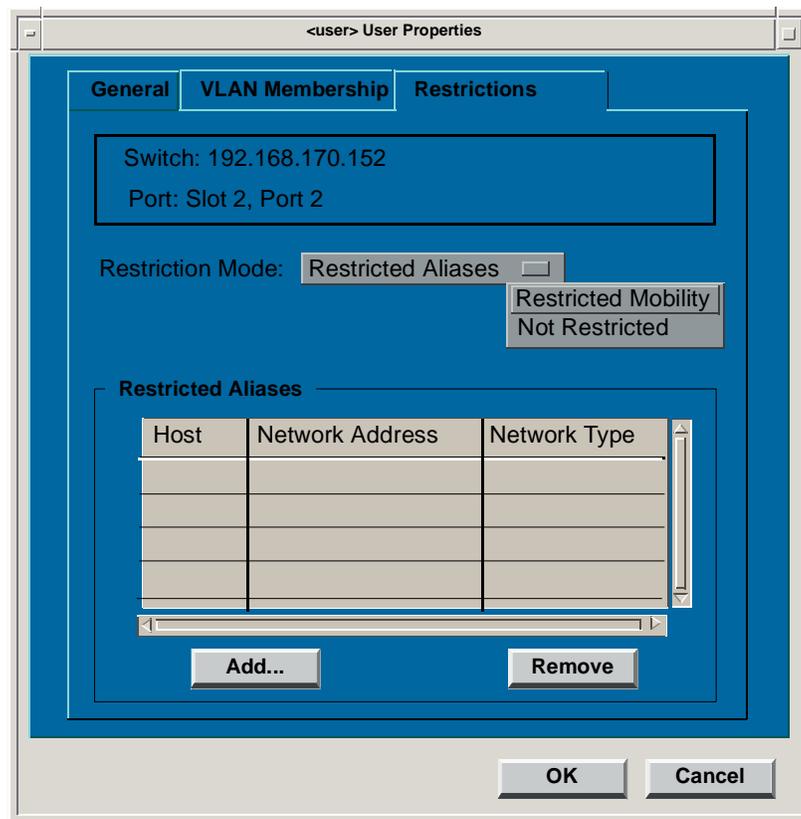
If you use Redundant Access User Restrictions, do not restrict users or ports for redundant users using the user or port restrictions available from user or port properties. Doing so may cause unpredictable results.

Using User Restrictions to Restrict a User

To restrict a user:

1. Select a user (MAC address) from the VLAN Manager Main window and then select Properties from the user pop-up menu.
2. Select the **Restrictions** tabbed page (Figure 10-20). This page displays the following information about a user: the switch and port to which the user is connected, drop-down list that lets you select what mode will be used to restrict the user, and a dialog box containing information relating to selected restriction mode.

Figure 10-20. User Properties (Restrictions)

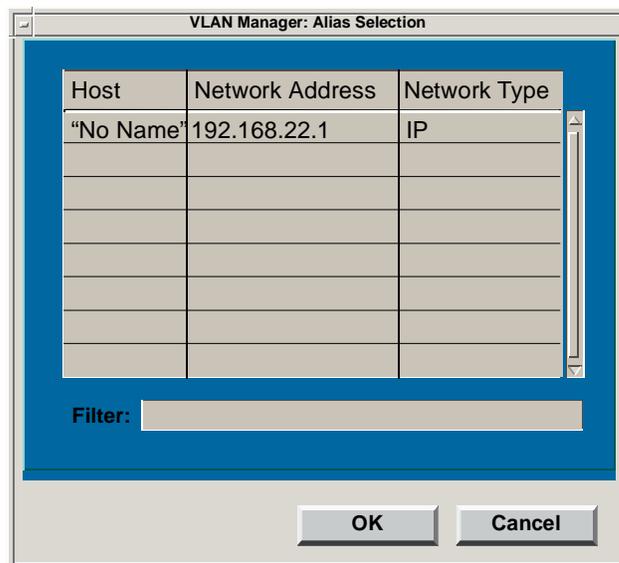


3. Select a restriction mode from the drop-down list, Restricted Alias(es), Restricted Mobility, Not Restricted. If you select Restricted Alias(es), continue with Step 4. If you select Restricted Mobility, continue with Step 5. If you select Not Restricted, no restrictions are placed on the user.
4. The Restricted Aliases table contains the host name (Host), Network Address, and Network Type of each alias that is restricted to the current user. Add or delete aliases from this table as required.

Add Alias

- a. To add a user alias restriction, click **Add** to display the Alias Selection dialog box (Figure 10-21).

Figure 10-21. Add User Alias Restriction



- b. Select the alias(es) you want to add. Click on an alias entry to select it. To select multiple aliases, click the alias entries you want to select.



You can use the filter feature to find an alias(es) quickly. As you type characters in the **Filter** text box, only those aliases that match your criteria are displayed.

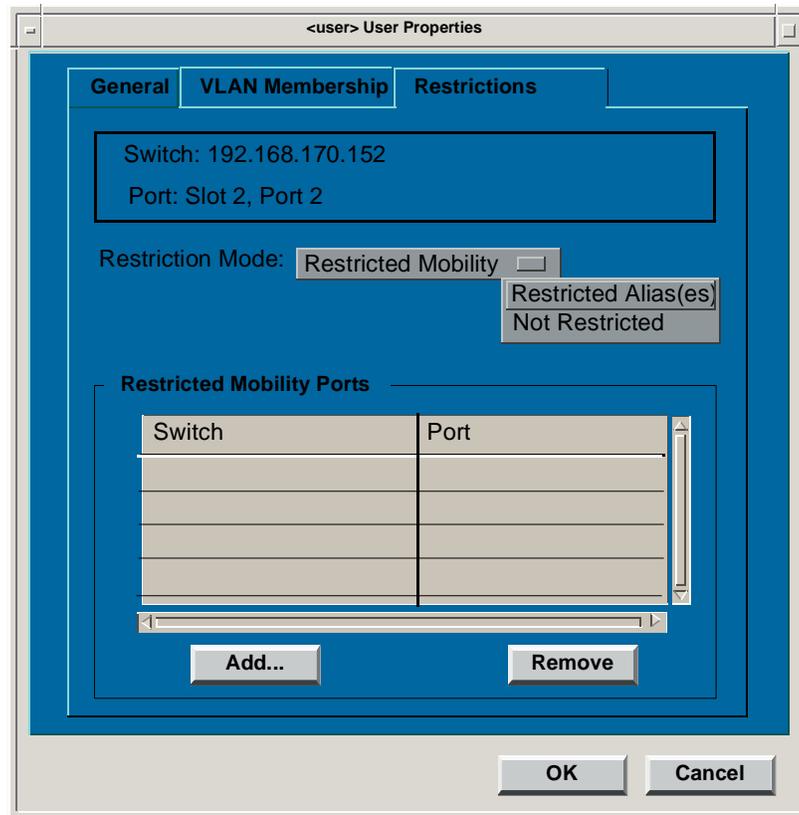
- c. Click **OK** to restrict the selected alias(es) or **Cancel** to close the Alias Selection dialog box without restricting any selections. Aliases you add are displayed in the Restricted Aliases table.

Remove Alias

- a. Select the alias(es) you want to remove from the Restricted Aliases table. Click on an alias entry to select it. To select multiple aliases, click the alias entries you want to select.
- b. Click **Remove** to remove the alias(es). Aliases you remove are deleted from the Restricted Aliases table.

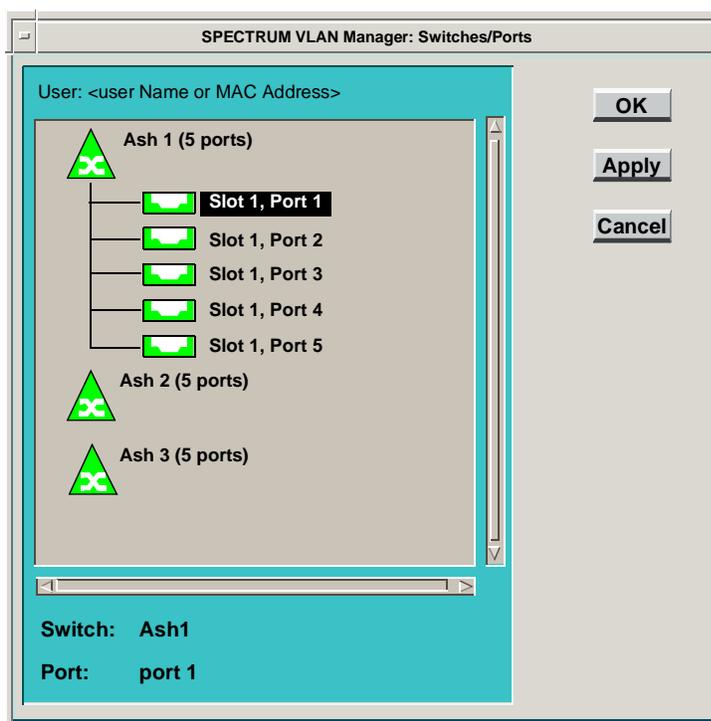
5. Each entry in the Restricted Mobility Ports table (Figure 10-22) contains a list of switch ports to which the user and its aliases are currently restricted. Add or delete switch ports from this table as required.

Figure 10-22. Restricted Mobility Ports Table



Add Port

- a. To add a user mobility restriction, click **Add** to display the Switches/Ports dialog box (Figure 10-23).

Figure 10-23. Add User Port Restriction

- Select the ports to which you want to restrict the user and its aliases. Click on a port entry to select it. To select multiple ports, click the port entries you want to select.
- Click **OK** to restrict the user and its aliases to the selected port(s) and close the window, or **Cancel** to close the window box without making any restrictions. Ports you add are displayed in the Restricted Mobility Ports table.

Remove Port

- Select the port(s) you want to remove from the Restricted Mobility Ports table. Click on a port entry to select it. To select multiple ports, hold the **Control** key and click the port entries you want to select.
- Click **Remove** to remove the port(s). Ports you remove are deleted from the Restricted Mobility Ports table.

Violations

- The following types of violations can occur: Restricted Port, Restricted Mobility, Restricted User, Restricted User (same port), Invalid IP - IP Not Learned, Invalid IP - Packet Discarded, or Disabled Protocol.
 - **Restricted Port** - A user not on a restricted port's list of MAC addresses tries to connect to the port.
 - **Restricted Mobility** - A user tries to connect to a port not on the list of ports to which it can connect.
 - **Restricted User** - A user tries to connect to a port other than the one to which it is restricted or a user tries to use an IP address restricted to another user on a different port.
 - **Restricted User (same port)** - A user tries to use an IP address restricted to another user on the same port.
 - **Invalid IP - IP Not Learned** - A user in a subnet that is not being serviced by the current domain tries to access the network. Connections to and from the user will be established but the Layer 3 address will not be cached in the switch's local directory.
 - **Invalid IP - Packet Discarded** - A user in a subnet that is not being serviced by the current domain tries to access the network. Connections to the user will not be established. Subnets which are allowed are configured as Internals of a Default Gateway Router MAC or through the IP Address Learning tab of Domain Properties; users of all other subnets will cause this violation.
 - **Disabled Protocol** - A user attempts to use a protocol that is not enabled in the current domain.

Violation Notification

Violations are identified at the port level in the VLAN Manager's Main window. The icon of any port for which at least one violation exists will be colored Yellow.

Identifying the Cause of a Violation

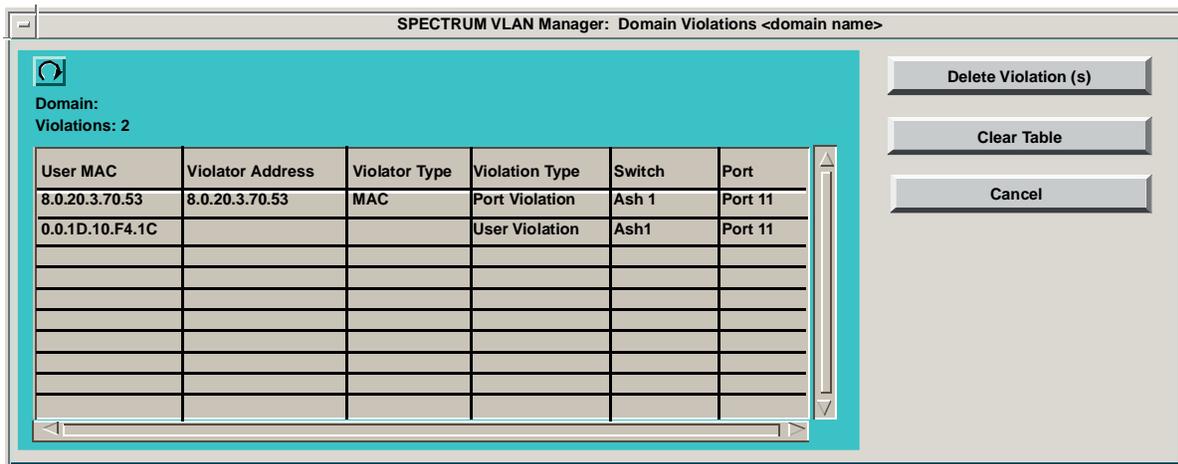
To find the cause of a violation, you open the Violations window (Figure 10-24). This window consists of the following fields and buttons: **User MAC**, **Violator Address**, **Violator Type**, **Violation Type**, **Switch**, **Port**, **First Seen**, **Last Seen**, and **Count** fields and **Delete Violation(s)**, **Clear Table**, and **Cancel** buttons. Data is filtered in the Violations window depending on how you open the window. If you opened the window at the domain level, no filtering is done, and all violations for the domain are displayed. If you opened the window at the switch, port, or user level, data is filtered to the selected level.

Violation Window Fields

- **User MAC** - MAC address of the violating endpoint.
- **Violator Address** - For a Violation Type of Restricted Port, Restricted Mobility, or Restricted User with a Violator Type of MAC, the MAC address of the violator. For a Violation Type of Restricted User with a Violator Type of IP, IPX, AppleTalk, or NetBIOS, the Layer 3 address that is in violation.
- **Violator Type** - Protocol (MAC, IP, IPX, AppleTalk, NetBIOS) associated with the Violator Address.
- **Violation Type** - Valid violation types are: Restricted Port, Restricted User, Restricted User (same port), Restricted Mobility, Invalid IP - IP Not Learned, and Invalid IP - Packet Discarded.
- **Switch** - Switch where the violation occurred.
- **Port** - Port where the violation occurred.
- **First Seen** - First time the violator was heard relative to when the switch was reset.
- **Last Seen** - Time when the violator was most recently heard relative to when the switch was reset.
- **Count** - Number of times the violation has occurred.

Violation Window Buttons

- **Delete Violation(s)** - Remove all selected entries from the violations table.
- **Clear Table** - Remove all entries from the violations table for the domain, switch, port, or user currently displayed.
- **Cancel** - Dismiss the Violations window and return to the VLAN Manager's Main view.

Figure 10-24. Violations Window

Opening the Violations Window

The violations displayed in the Violations window depend on whether you have opened the window for a domain, switch, port, or user.

Opening the Violations Window for a Domain

To open the Violations window for a domain, select **Violations** from the **Edit >Domain** menu.

Opening the Violations Window for a Switch, Port, or User

To open the Violations window for a switch, port, or user, select the switch, port, or user and then select **Violations** from the **Edit** menu.

Remedying a Violation

The following sections provide information about how to remedy different violation types.

Remedying User and Port Restrictions



A user or port violation must be remedied and removed from the Violations table before restriction changes you make to remedy a violation take effect.

If you choose not to remedy a violation:

- The violating endpoint will be ignored and all packets dropped
- No call processing will take place for that endpoint
- The VLAN Manager's Main window will continue to indicate a violation for the port to which the violator is connected
- The Violations window entry you delete for an unremedied violation will reappear when the violation is rediscovered.

The following table provides you with suggested procedures for remedying user and port violations based on violation type. The examples provide you with typical scenarios of how user and port violations might be remedied.

Table 10-2. User and Port Violation Remedies

Violation Type	Cause	Remedy
Restricted Port	A user not on the restricted ports' list of MAC addresses tried to use the port.	<ol style="list-style-type: none"> 1. Display the Port Properties' Restrictions tabbed page for the port shown in the Port column. 2. Note that the user shown in the User MAC column is not listed. 3. Add the User MAC to the list of users that are allowed to use the port, remove all restrictions from the port, or disconnect the user from the port. 4. Remove the entry from the Violations Table.
Restricted Mobility	A user tried to use a port which it is not allowed to use.	<ol style="list-style-type: none"> 1. Display the User Properties' Restrictions tabbed page for the MAC address shown in the User MAC column. 2. Note that the port which the user tried to use is not listed. 3. Add the port to the list of ports which the user can use, remove all restrictions from the user, or disconnect the user from the port. 4. Remove the entry from the Violations Table.

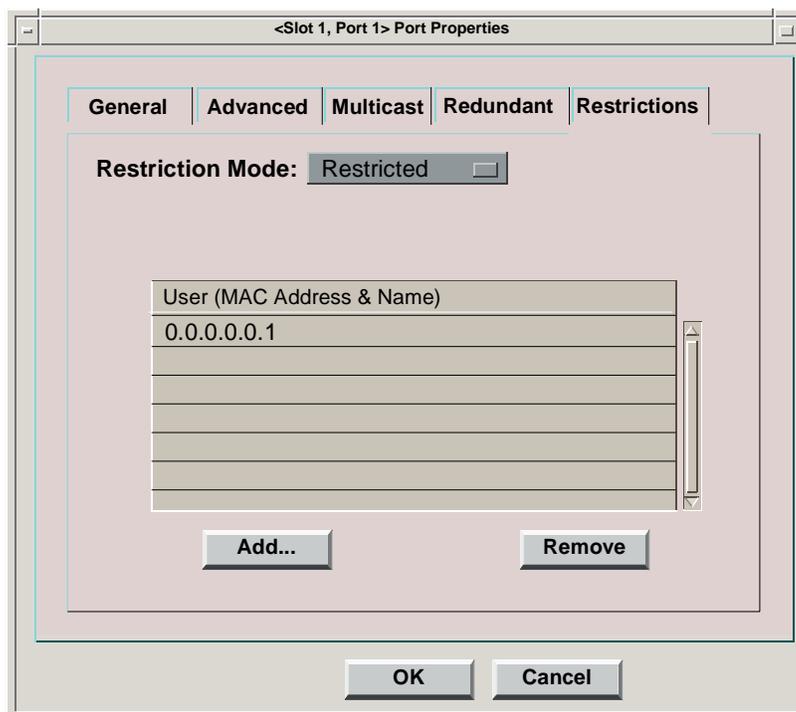
Table 10-2. User and Port Violation Remedies

Violation Type	Cause	Remedy
Restricted User	A user with a restricted alias has tried to use another port.	<ol style="list-style-type: none"> 1. Display the User Properties' Restrictions tabbed page for the MAC address shown in the User MAC column. 2. Note that the port to which the user tried to connect is not the port to which its alias is restricted. 3. Remove all restrictions from the user, or disconnect the user from the port. 4. Remove the entry from the Violations Table.
	A user tried to use an alias restricted to another user which is on a different port.	<ol style="list-style-type: none"> 1. Display Directory View and search for the Alias shown as the Violation Address. 2. Display the User Properties Restrictions tabbed page for that MAC Address 3. Note the Violator Address is restricted to this MAC. 4. Remove the restriction on the alias which the user tried to use, remove all alias restrictions from the user, use another address. 5. Remove the entry from the Violations Table.
Restricted User (same port)	A user tried to use an IP address restricted to another user which is on the same port.	<ol style="list-style-type: none"> 1. Display Directory View and search for the Alias shown as the Violation Address. 2. Display the User Properties Restrictions tabbed page for that MAC Address 3. Note the Violator Address is restricted to this MAC. 4. Remove the restriction on the alias which the user tried to use, remove all alias restrictions from the user, use another address. 5. Remove the entry from the Violations Table.

Example #1 (Restricted Port Violation)

In this example, suppose you have restricted the port in Conference Room B (Switch 1, Port 1) to MAC address 0.0.0.0.1 because you want to control who can connect to the network from this port.

Figure 10-25. Example 1



You notice that the port icon for Switch1, Port 1 changes from the color Green to the color Yellow. Realizing that this indicates that a violation has occurred, you bring up the Violation window for that port.

The violation entry for Switch 1, Port 1 provides you with the following information:

- **User MAC** - 0.0.0.0.2
- **Violator Address** - 0.0.0.0.2
- **Violator Type** - MAC
- **Violation Type** - Restricted Port
- **Switch** - 1
- **Port** - 1
- **First Seen** - 3+21:08:26
- **Last Seen** - 3+21:08:44
- **Count** - 2

From the **User MAC** information, you can tell that the violation was caused by MAC address 0.0.0.0.2. In this case, the **Violator Address** information provides the same information as the User MAC information.

You bring up the **Port Properties' Restrictions** tabbed page for the switch and port where the violation was heard (Switch 1, Port 1) and find that this port is restricted to MAC address 0.0.0.0.1.

You have identified the problem: the device with MAC address 0.0.0.0.2 should not be using Switch 1, Port 1.

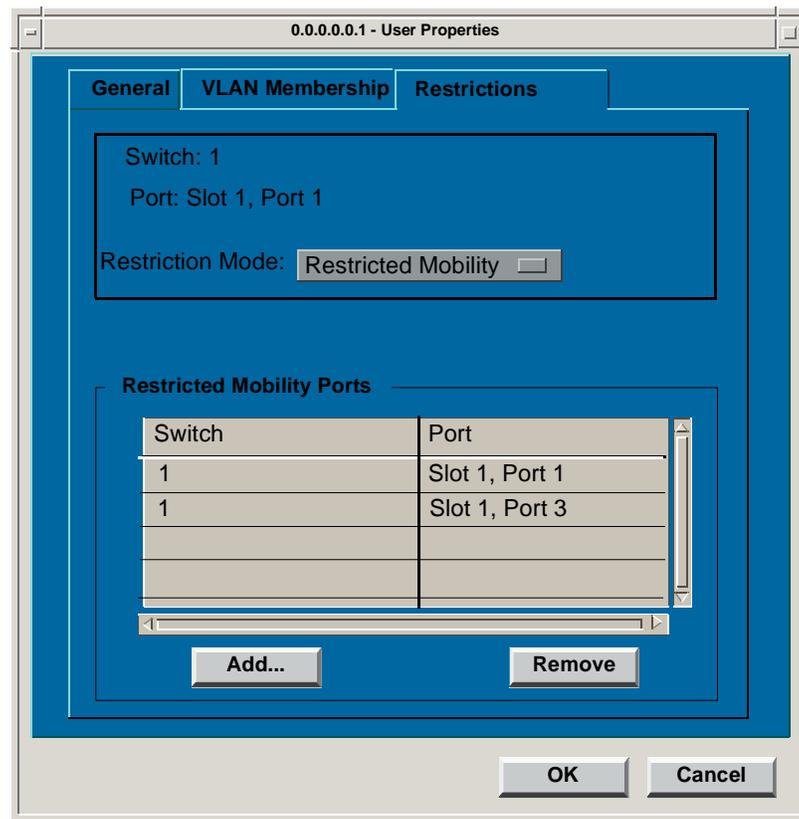
You can add MAC address 0.0.0.0.2 to the port's list of restricted MAC addresses, disconnect 0.0.0.0.2 from Switch 1, Port 1, or remove all restrictions from the port.

Since it's not critical that this port be restricted to one device, but you want to have control over who can connect to the port, you decide to add MAC address 0.0.0.0.2 to the list of restricted users.

You then remove the entry for this violation from the Violations window. The port icon will change to the color Green if there are no other violations on the port.

Example #2 (Restricted Mobility Violation)

In this example, suppose you have restricted the mobility of Endpoint 1 (0.0.0.0.1) to Switch 1 (installed in Slot 1), Ports 1 and 3; however, you inadvertently connect this endpoint to Switch 1, Port 2.

Figure 10-26. Example 2

All aliases associated with Endpoint 1 are also restricted to Switch 1, Ports 1 and 3 so if you tried to assign Endpoint 1's IP address to another endpoint, a violation of type 'Restricted User' would occur.

You notice that Switch1, Port 2, is flagged with a violation icon (Yellow), so you bring up the Violation window for that port.

The entry in the window provides you with the following information:

- **User MAC** - 0.0.0.0.1
- **Violator Address** - 0.0.0.0.1
- **Violator Type** - MAC
- **Violation Type** - Restricted Mobility
- **Switch** - 1

- **Port** - 2
- **First Seen** - 3+21:08:26
- **Last Seen** - 3+21:08:44
- **Count** - 2

From the **User MAC** information, you can tell that MAC address 0.0.0.0.1 has caused the violation. In this case, the **Violator Address** information provides the same information as the User MAC information.

You bring up the **User Properties' Restrictions** tabbed page for the MAC address causing the violation (0.0.0.0.1), and find that this user is restricted to Switch 1, Ports 1 and 3 using Restricted Mobility.

You have identified the problem: Endpoint 1 is connected to Switch 1, Port 2 and it is restricted to Switch 1, Ports 1 and 3.

At this point, you can move the user to a port to which it is restricted, change the port restrictions of Endpoint 1 to include Switch 1, Port 2, disconnect Endpoint 1 from Switch 1, Port 2, or remove all restrictions from the user.

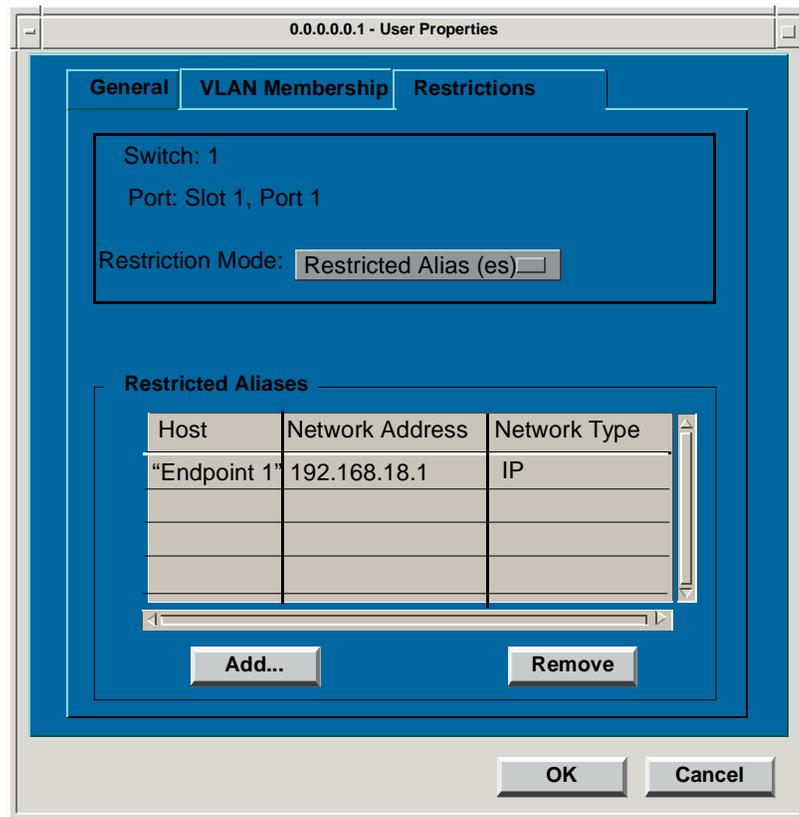
You physically move the user to Switch 1, Port 1.

You then remove the entry for this violation from the Violations window. The port icon will change to the color Green if there are no other violations on the port.

Example #3 (Restricted User Violation)

In this example, suppose you have restricted Endpoint 1's IP alias (192.168.18.1) to Endpoint 1 (0.0.0.0.1); however, Endpoint 2 (0.0.0.0.2) tries to use this IP address. By default, Endpoint 1 is restricted to Switch 1, Port 1, and Endpoint 2 is using Port 2.

Figure 10-27. Example 3



Restricting Endpoint 1's IP address to Endpoint 1 also restricts Endpoint 1 to Switch 1, Port 1 so if you try to connect Endpoint 1 to another port, a violation of type 'Restricted User' will occur. The violation type is 'Restricted User' and not 'Restricted Mobility' because 'Restricted Mobility' violations only occur if the restriction was set using Restricted Mobility.

You notice that Switch1, Port 2, the port to which Endpoint 2 is connected, is flagged with a Violation icon (Yellow), so you bring up the Violation window for that port.

The entry in the window provides you with the following information:

- **User MAC** - 0.0.0.0.2
- **Violator Address** - 192.168.18.1
- **Violator Type** - IP
- **Violation Type** - Restricted User
- **Switch** - 1
- **Port** - 2
- **First Seen** - 3+21:08:26
- **Last Seen** - 3+21:08:44
- **Count** - 2

From the User MAC, you can tell that MAC address 0.0.0.0.2 has caused the violation, and from the Violator Address, you can tell that a restriction involving IP address 192.168.18.1 has been violated.

You bring up the Directory View and search for alias 192.168.18.1. You notice that this IP address is an alias for MAC address 0.0.0.0.1, so you bring up the **Restrictions** tabbed page for MAC address 0.0.0.0.1. At this point you can tell that alias 192.168.18.1 is restricted to MAC address 0.0.0.0.1.

You have identified the problem: Endpoint 2 is trying to use an IP address (192.168.18.1) that is restricted to another user (Endpoint 1).

At this point, you can assign Endpoint 2 a different IP address, remove the IP alias restriction from user Endpoint 1 or change the user to which IP address 192.168.18.1 is restricted to Endpoint 2.

You assign Endpoint 2 a different IP address.

You then remove the entry for this violation from the Violations window. The port icon will change to the color Green if there are no other restrictions on the port.

Invalid IP Violations



Invalid IP violations must be remedied and removed from the Violations table before restriction changes you make to remedy a violation take effect.

If you choose not to remedy a violation:

For an Invalid IP - IP Not Learned violation:

- Call processing will take place for that endpoint but the endpoint's IP address will not be cached in the switch's local directory
- The VLAN Manager's Main window will continue to indicate a violation for the port to which the violator is connected
- The Violations window entry you delete for an unremedied violation will reappear when the violation reoccurs.

For an Invalid IP - Packet Discarded violation:

- The violating endpoint will be ignored
- No call processing will take place for that endpoint
- The VLAN Manager's Main window will continue to indicate a violation for the port to which the violator is connected
- The Violations window entry you delete for an unremedied violation will reappear when the violation reoccurs.

The following table provides you with suggested procedures for remedying Invalid IP violations based on violation type. The examples provide you with typical scenarios of how Invalid IP violations might be remedied.

Table 10-3. Invalid IP Violation Remedies

Violation Type	Cause	Remedy
Invalid IP - IP Not Learned	A user in a subnet not being serviced by the current domain tried to use the domain.	<ol style="list-style-type: none"> 1. Display the Domain Properties' IP Address Learning tabbed page 2. Note that the subnet for the user shown in the Violator Address column is not listed. 3. Add the subnet of the user to the list of subnets in IP Address Learning tab, or in Router Wizard for Default Gateway MAC change the user's address so it is in a subnet that is serviced by the domain. 4. Remove the entry from the Violations Table.
Invalid IP - Packet Discarded	A user in a subnet not being serviced by the current domain tried to use the domain.	<ol style="list-style-type: none"> 1. Display the Domain Properties' IP Address Learning tabbed page 2. Note that the subnet for the user shown in the Violator Address column is not listed. 3. Add the subnet for the user to the list of subnets in IP Address Learning tab, or in Router Wizard for Default Gateway MAC change the user's address so it is in a subnet that is serviced by the domain. 4. Remove the entry from the Violations Table.

Example (Invalid IP - IP Not Learned)

You remedy a violation of type **Invalid IP - Packet Discarded** the same way you remedy a violation of type **Invalid IP - IP Not Learned**.

In this example, an endpoint 0.0.0.0.1 with a network address of 192.168.19.1 on Switch 1, Port 1 tries to make a connection to endpoint 0.0.0.0.2, IP 192.168.18.1 on Switch 1, Port 2. The domain is servicing subnet 192.168.18.0 but is not servicing subnet 192.168.19.0.

You notice that Switch1, Port 1 is flagged with a Violation icon (Yellow), so you bring up the Violation window for that port.

The entry in the window provides you with the following information:

- **User MAC** - 0.0.0.0.1
- **Violator Address** - 192.168.19.1
- **Violator Type** - IP
- **Violation Type** - Invalid IP - IP Not Learned
- **Switch** - 1
- **Port** - 1
- **First Seen** - 3+21:08:26
- **Last Seen** - 3+21:08:44
- **Count** - 2

From the User MAC, you can tell that MAC address 0.0.0.0.1 has caused the violation, and from the Violator Address, you can tell that a restriction involving IP address 192.168.19.1 has been violated.

You bring up the **Domain Properties' IP Address Learning** tabbed page and notice that the 192.168.19.0 subnet is not one of the subnets being serviced by this domain.

You have identified the problem: the user with IP address 192.168.19.1 is trying to use a domain that is not servicing the 192.168.19.0 subnet.

At this point, you can add the 192.168.19.0 subnet to the list of subnets being serviced by the domain, change the IP address for user MAC 0.0.0.0.1 to an address in the 192.168.18.0 subnet, or do nothing. You decide to add the 192.168.19.0 subnet to the list of subnets being serviced by the domain.

You bring up the **Router Wizard** and add the 192.168.19.0 subnet to the list of internal subnets for the Default Gateway.

Finally, you remove the entry for this violation from the Violations window. The port icon will change to the color Green if there are no other restrictions on the port.

Disabled Protocol Violation

The following table and examples illustrate a typical way to remedy a Disabled Protocol violation.

Table 10-4. Disabled Protocol Violation Remedies

Violation Type	Cause	Remedy
Disabled Protocol	A user uses a protocol that is not enabled on the current switch.	<ol style="list-style-type: none"> 1. Display the Domain Protocol Control window or the Switch Protocol Control window. 2. Note that the protocol listed in the Violator Type column is not listed as enabled. 3. Enable the protocol. 4. Remove the entry from the Violations Table.



The settings applied in the Domain Protocol Control window can be overridden by the settings in the Switch Protocol Control window, therefore the settings displayed in the Domain Protocol Control window may not be accurate for all switches on the domain. For information on Domain Protocol Control, see *Protocol Control*, on page 6-38. For information on Switch Protocol Control, see *Switch Protocol Control*, on page 7-19.

Example (Disabled Protocol Violation)

In this example, an endstation uses a protocol that is not enabled on that domain.

You notice that the Slot 4, Port 3 is flagged with a Violation icon (yellow), so you bring up the Violation window for that port.

The entry in the window provides you with the following information:

- **User MAC** - 0.0.0.0.1
- **Violator Address** - 192.168.19.1
- **Violator Type** - cp.inet.igp
- **Violation Type** - Disabled Protocol
- **Switch** - 2
- **Port** - slot 4, port 3
- **First Seen** - 0+00:00:18

- **Last Seen** - 48+11:31:42
- **Count** - 46785

From the Violation Type, you can tell that a Disabled Protocol violation occurred and from the Violator Type, you can see the protocol that was used. The packet sent by the user has already been intercepted and dropped by the switch.

At this point, you can enable the protocol on the domain or just on the switch. To enable a protocol on a switch, open the **Switch Protocol Control** window from the **Tools** menu (see *Switch Protocol Control*, on page 7-19). To enable a protocol on the domain level, open the **Protocol Control** window from the **Edit >Domain** menu.

Once you have enabled the protocol, remove the entry for this violation from the Violations window. The port icon will change to the color Green if there are no other violations on the port.

Managing Connections

This chapter provides step-by-step instructions for performing connection administration tasks using SPECTRUM VLAN Manager's graphical user interface. It also contains reference information and helpful tips to help you perform these tasks.

Overview

You perform most connection management tasks from the **Connection Table**. A few tasks can be initiated from the **Edit >Switch** menu, the **View >Switch** menu, or the **View >Tapped Connections** command. Tasks that can be performed from these menus include:

- Launching the Connection Table
- Configuring Call Aging Parameters
- Provisioning Calls
- View and manage tapped connections for the current domain.

The Connection Table ([Figure 11-4](#)) provides detailed information about all active calls associated with a source and destination, lets you add and release call taps, and lets you release calls.

Launching the Connection Table

To launch the Connection Table, select a switch or user from the Switches window pane and then choose **Connection Table** from the **View >Switch** menu. You can also launch the **Connection Table** from the:

- Toolbar 
- **View >User** menu
- **View >VLAN >Details** pop-up menu
- **Directory >View** menu

- Directory pop-up menu
- VLAN User pop-up menu (when a user is selected)
- Switch User pop-up menu (when a user is selected)



Since the time required to read and display connection information varies depending on the number of connections, a progress meter, which shows the percentage of the total connection information read, is displayed each time you launch the Connection Table.

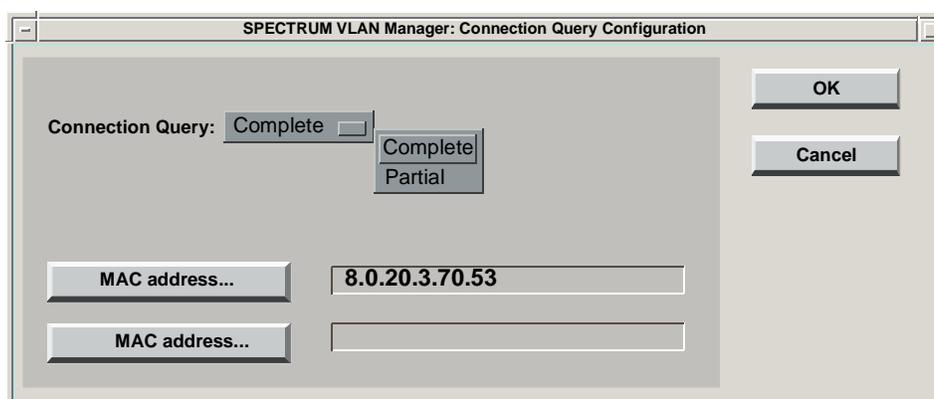
Connection Table statistics are gathered for a specific user. When you select a user, the SPECTRUM VLAN Manager Connection Query Configuration window is displayed. This window lets you query the Connection Table in two ways: **Complete** or **Partial**. The default is **Complete**. **Complete** requires that the source user MAC and destination user MAC be specified. **Partial** only requires the MAC address of a user.

Complete Connection Table Query

To display the connection information for a specific source/destination user pair:

1. Select a user from the Logical window pane and then select Connection Table from the user pop-up menu. The SPECTRUM VLAN Manager: Connection Query Configuration window is displayed (Figure 11-1). Note that the contents of the bottom half of this window depends on the type of query you select: **Complete** or **Partial**. **Complete** is the default.

Figure 11-1. Connection Table Query Configuration (Complete Query)



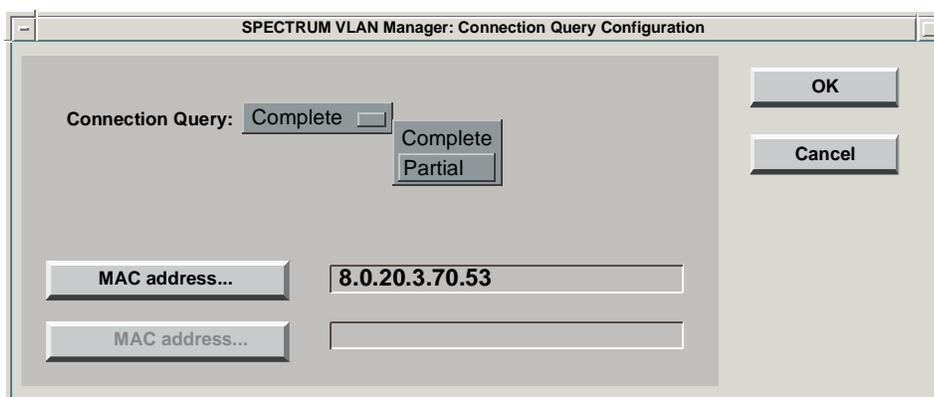
2. The source address of the selected user is automatically entered into the top MAC address user field. To select a different source user, click the associated **MAC address** button. Refer to *Selecting a Source User, Destination User, or MAC Address, on page 11-4* for information about selecting a different MAC Address.
3. Click anywhere in the bottom MAC address user text field and then enter the MAC address of the destination user. If you don't know the MAC address of the destination user, click the associated **MAC address button**. Refer to *Selecting a Source User, Destination User, or MAC Address, on page 11-4* for information about selecting a different MAC Address.
4. Click **OK** to display connection information about the selected source and destination or click **Cancel** to dismiss the Connection Query Configuration window.

Partial Connection Table Query

To display all connection information for a specific user:

1. Select a user from the Logical window pane and then select Connection Table from the user pop-up menu. The SPECTRUM VLAN Manager: Connection Query Configuration window is displayed. Note that the contents of the bottom half of this window depends on the type of query you select: **Complete** or **Partial**. **Complete** is the default.
2. Select **Partial** from Connection Query. The SPECTRUM VLAN Manager: Connection Table Query Configuration window is displayed as shown in [\(Figure 11-2\)](#).

Figure 11-2. Connection Table Query Configuration (Partial Query)



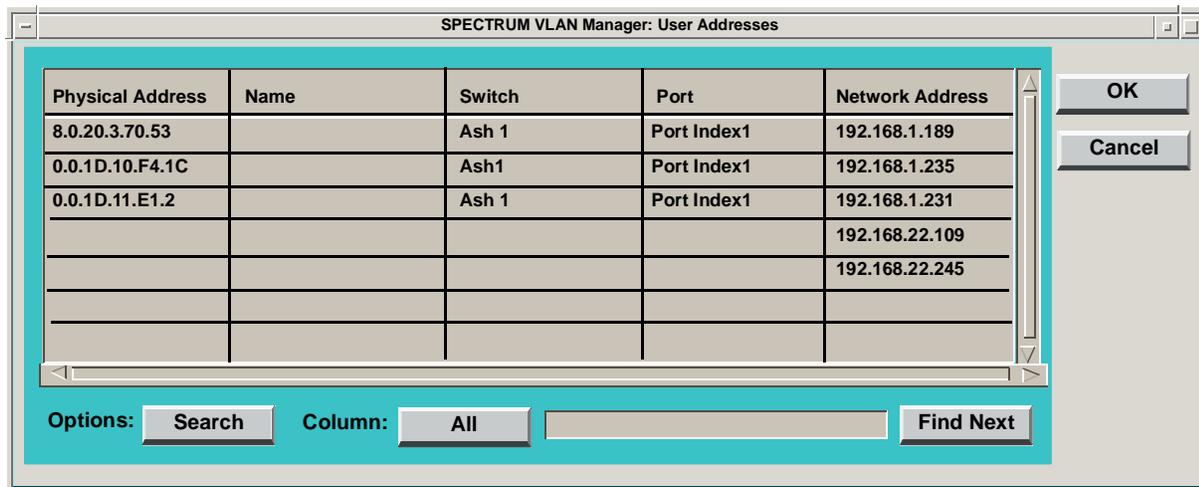
3. The MAC address of the selected user is automatically entered into the MAC address field. To select a different MAC address, click the associated **MAC Address** button. Refer to *Selecting a Source User, Destination User, or MAC Address, on page 11-4* for information about selecting a different MAC Address.
4. Click **OK** to display connection information about the selected user or click **Cancel** to dismiss the Connection Query Configuration window.

Selecting a Source User, Destination User, or MAC Address

The SPECTRUM VLAN Manager: User Addresses window is displayed (Figure 11-3) if you click **MAC address** from the Connection Query Configuration window while performing a connection query.

Click anywhere in the record displaying connection information about the user you want to select and then click **OK** to select that user. The user's MAC address is entered into the appropriate Connection Query Configuration window text field. Click **Cancel** to dismiss the User Addresses window.

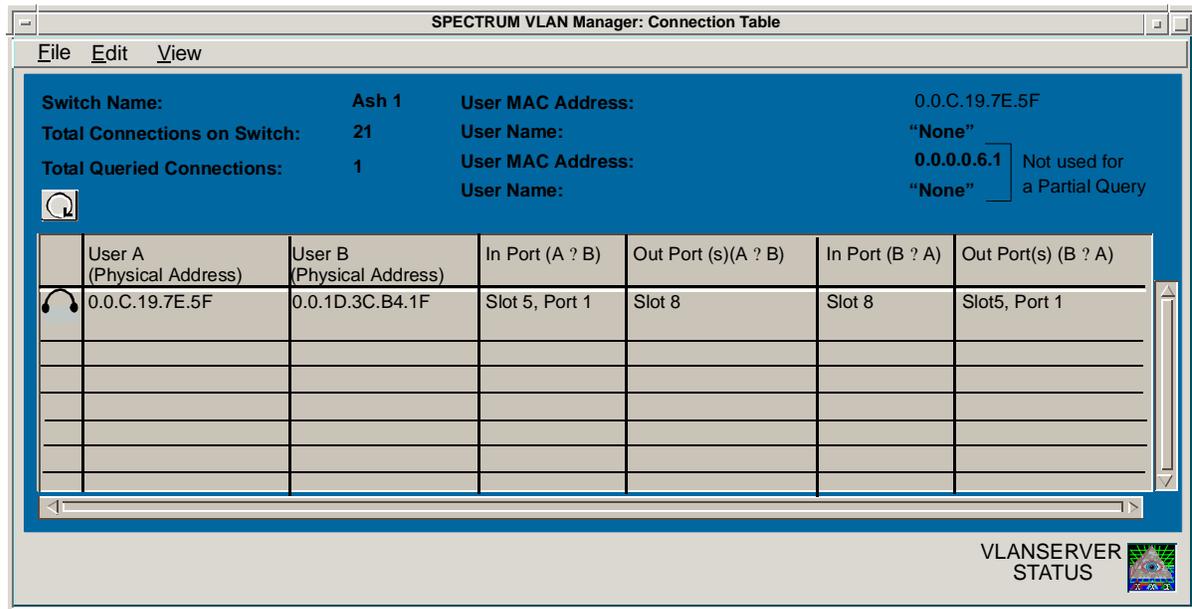
Figure 11-3. User Addresses



Elements of the Connection Table

The Connection Table window consists of a Menu bar, an update button, general information fields, the connection table, and several support functions.

Figure 11-4. Connection Table



Connection Table Menu Bar

The Connection Table menu selections let you perform all connection-related tasks. The features and functions available from the Connection Table menus are summarized in this section and discussed in greater detail in the sections covering how to use each selection.

File Menu

The **File** menu lets you define preferences for viewing the Connection Table, save the contents of the Connection Table, and Exit the Connection Table. Selections from the **File** menu include:

- **P**references - Lets you to define Connection Table settings. Refer to [Chapter 5, Managing Preferences](#), for information about setting these preferences.
- **S**ave - Lets you save the contents of the Connection Table to a file. Refer to [Save, on page 10-20](#).

- **C**lose - Closes the Connection Table window.

Edit Menu

The **Edit** menu consists of the following selections: **A**ging Configuration, **P**rovision Connection, **C**onnection, and **R**elease **A**ll Connections - User A.

- **A**ging Configuration - Lets you set the call aging parameters. Refer to *Aging Connections*, on page 11-14.
- **P**rovision Connection - Lets you set up provisioned connections. Refer to *Provisioning Calls*, on page 11-18.
- **C**onnection - Displays the Connection submenu. This menu consists of the following commands: **C**all Tap, **R**elease Tap, and **R**elease Call.
 - **C**all Tap - Lets you add taps to calls listed in the connection table. Taps can be unidirectional, monitoring either the source or destination endpoint, or bidirectional, monitoring all traffic between two endpoints.
 - **R**elease Tap - Lets you tear down taps on demand.
 - **R**elease Call - Lets you tear down automatically programmed calls (switched connections) or manually programmed calls (PVCs) on demand. Calls only time out when a switch associated with a call resets or the call aging threshold is reached.
 - **R**elease **A**ll Connections - User A - Lets you tear down all calls involving User A.

View Menu

The **View** menu consists of the following selections: **C**onnection Query, **U**ppdate, **E**xplode/**C**ollapse Router Connections, and **S**ort.

- **C**onnection Query - Lets you filter connection table information. Refer to *Launching the Connection Table*, on page 11-1 for information about Connection Query.
- **U**ppdate - Lets you refresh the contents of the Connection Table.
- **E**xplode/**C**ollapse Router Connections - Lets you toggle between showing all endpoints known to the router and only showing the router information. The word “COLLAPSED” appears in table fields to indicate collapsed connections.
- **S**ort - Lets you arrange the entries in the Connection Table according to the sort field you choose.
- **P**ath Trace - Lets you view the end-to-end connectivity of a selected call within a domain.

Connection Table Update Button



- Update the contents of the Connection Table.

General Information Fields

Fields displayed vary depending on the type of connections (i.e., switch, user) for which information is being collected.

- **Switch Name**- Switch name for which active call statistics are being displayed.
- **Total Connections on Switch** - Current number of active calls on the selected switch.
- **Total Queried Connections** - Current number of active filtered connections.
- **User MAC Address (User A)** - MAC address of the user for which active call statistics are being displayed.
- **User Name (User A)** - Name of the user for which active call statistics are being displayed.
- **User MAC Address (User B)** - MAC address of the user for which active call statistics are being displayed.
- **User Name (User B)** - Name of the user for which active call statistics are being displayed.
- **VLAN SERVER STATUS** - Uses color to indicate the operational status of the VLANServer. If the VLANServer icon's background color is Green, normal operation is indicated. If the background color is Red, a server failure condition exists.

Connection Table Fields

The Connection Table displays information about all active calls for a user. Each line on the Connection Table provides information associated with a specific call. A scroll bar to the right of the table lets you scroll through the table.

- **Untitled** - Tapped call (). A small icon of a telephone handset with a curved line above it, indicating a missed or tapped call.
- **User A**- Network address (e.g., IP, IPX), MAC address, User Name, or Hostname of the endpoint that initiated the call. The type of information displayed is determined by the User Display selection set from the Preferences menu Connection Table tab.
- **User B**- Network address (e.g., IP, IPX), MAC address, User Name, or Host name of the endpoint to which the call is directed. The type of information displayed is determined by the User Display selection set from the Preferences menu Connection Table tab.

- **In Port (A ? B)** - On a call from endpoint A to endpoint B, the switch port on which the call is received.
- **Out Port(s) (A ? B)** - On a call from endpoint A to endpoint B, the switch port(s) on which the call is transmitted.
- **In Port (B ? A)** - On a call from endpoint B to endpoint A, the switch port on which the call is received.
- **Out Port(s) (B ? A)** - On a call from endpoint B to endpoint A, the switch port(s) on which the call is transmitted.
- **Duration** - The length of time (in seconds) that the call has been in progress. Timing starts as soon as an end-to-end connection between endpoints has been established. Time is shown in days, hours, minutes, and seconds. For example, 2+14:9:45 represents 2 days, 14 hours, 9 minutes, and 45 seconds.
- **Type** - The type of connection. Valid entries are: **Filter**, **Provisioned**, **Switched**, **Self-Programmed Non-Filter**, **Self-Programmed Filter**, **VLAN**, **Tap**, **Mcast**, and **Non-critical VLAN**.
 - **Filter** - connection goes out the same port it came in on (source address and destination address are on the same port).
 - **Provisioned** - manually established connection.
 - **Switched** - dynamically established connection.
 - **Self-Programmed Non-Filter** - switch to switch connection.
 - **VLAN**- normal connection.
 - **Tap** - tapped connection.
 - **Mcast** - multicast connection.
 - **Non-critical VLAN** - connections considered to be non mission critical. If connections need to be dropped, this type of connection will be dropped first. Other types of connections will be dropped starting with the oldest connections.
- **Control Status** - This attribute is always set to “Activate.”
- **Admin Status** - This attribute is always set to “Enabled.”
- **Packets** - The number of packets transmitted for this connection.
- **Bytes** - The number of bytes transmitted for this connection.



You can adjust the widths of the columns in the Connection Table by positioning the cursor over one of the vertical lines separating columns, and then dragging the line to the left or right.

Sorting the Connection Table

To use the sort feature:

1. Choose the **Sort** selection from the Connection Table's **View** menu. A list of sort fields is displayed.



You can also initiate the sort feature by double-clicking a column header.

2. Click on any sort field. The Connection Table is rearranged according to the sort field you chose. Text entries are arranged alphabetically. Numeric entries are arranged from lowest to highest.

The selected sort field is used for all subsequent sorts until you choose a different field or you exit the Connection Table.

Tapping a Connection

You can add or release call taps using Call Tap.

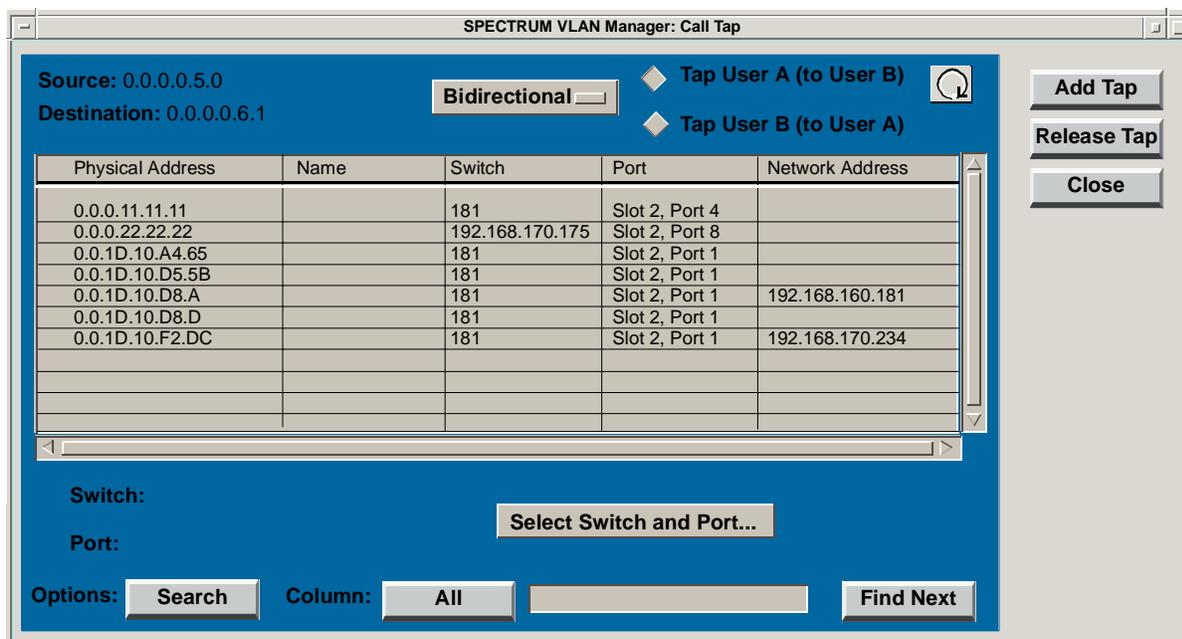


To view tapped calls, select **Tapped Connections** from the VLAN Manager **View** menu or click the Tapped Connections tool.

Adding a Call Tap

1. In the Connection Table, select a call to be tapped by clicking anywhere on the entry.
2. Select **Call Tap** from the Connection Table's **Edit > Connection** menu or from the Connection Table pop-up menu to display the SPECTRUM VLAN Manager's Call Tap window (Figure 11-5).

Figure 11-5. Call Tap



This window identifies the call to be tapped by its source and destination physical address, and provides buttons that let you select the mode used to tap a call: unidirectionally or bidirectionally. All users in a domain which can be selected as the tap point are listed. You can use the search/filter feature to find a particular user quickly without having to manually search the entire list. Buttons on the right side of the window let you add a tap, release a tap, or close the window. To refresh the data in the table, click the Update button: 

3. To select the way the call tap will operate, select **Unidirectional** or **Bidirectional**. If you select **Bidirectional**, the call tap will operate in both directions, meaning that all data will be seen by the tap point (a.k.a. probe). If you select **Unidirectional**, the call tap will operate in whichever direction is selected. Click on the button to the left of **Tap User A (to User B)** or **Tap User B (to User A)** to select which data will be seen. If you select **Tap User A**, data sent by the source will be seen at the tap point. If you select **Tap User B**, data sent by the destination will be seen at the tap point.

4. Select the tap point.

If the tap point has not registered with a switch, that is if it is passively listening, not speaking, click the **Select Switch and Port** button to display the **Switches/Ports** dialog box. Select the switch and port of the tap point, click **OK** to enter the switch and port information into the **Switch** and **Port** text fields, and then close the window or **Close** to dismiss the window without accepting switch and port selections.

If the tap point has registered with a switch (i.e., is speaking):

- a. Use the scroll bar to find the tap point, and then click anywhere on the entry to select it.

or

- b. Use the **Search/Filter** feature to find the tap point.

5. Click **Add Tap**. An additional port number is added to the **Out Port** field for the call being tapped and the call tap icon (📞) is displayed to the left of the **User Physical Address**.

Releasing a Call Tap

1. Select the call with the tap to be released from the **Connection Table**.
2. Select **Release Tap** from the **Connection Table**'s **Edit > Connection** menu or from the **Connection Table** pop-up menu. The port name of the tap point is removed from the **Connection Table Out Port** field for the call from which the call tap was released. The call tap icon is also removed.



This operation can also be initiated from the **View > Tapped Connections** window.

Modifying a Call Tap

To modify a call tap, first release the existing tap, then add the new tap.

Tracing a Connection

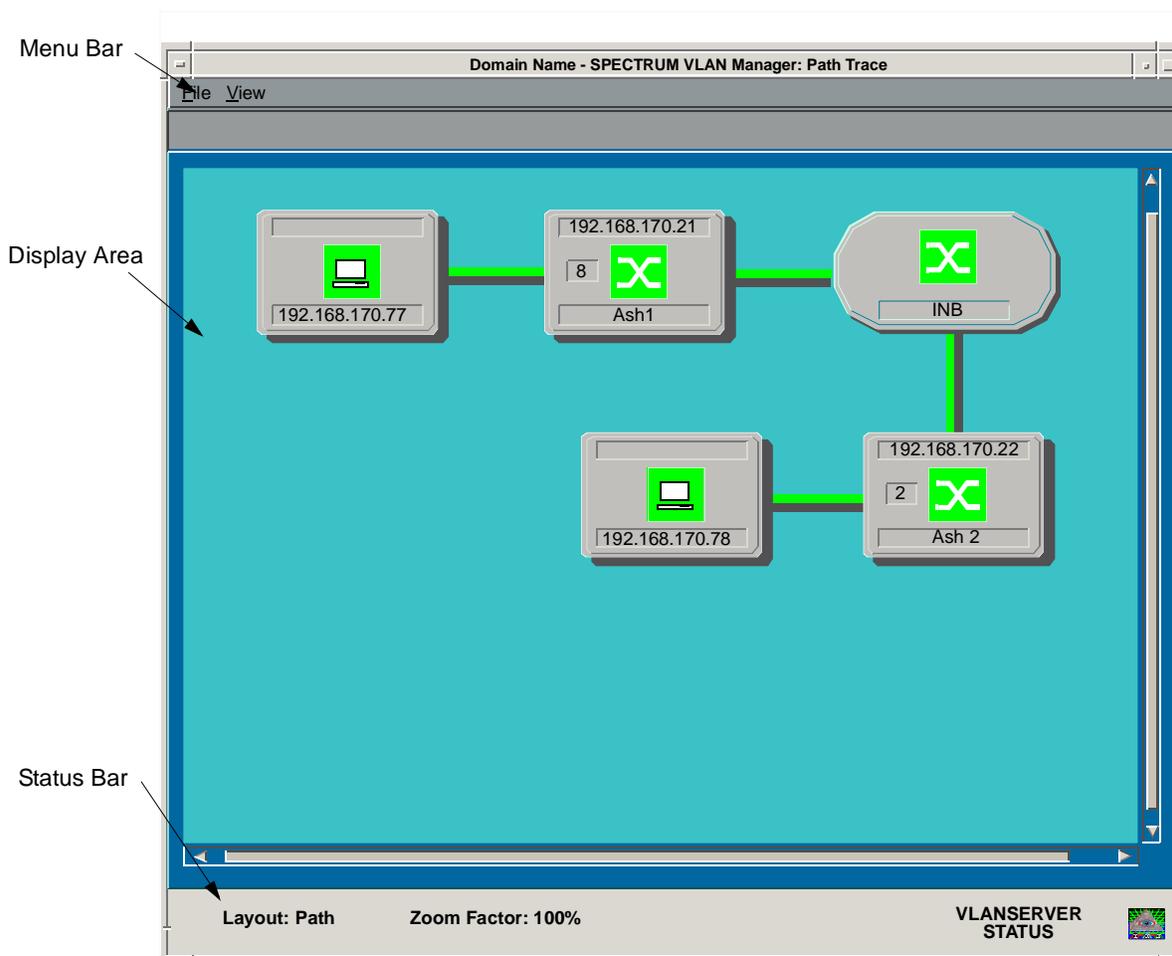
Path Trace lets you view end-to-end connectivity of a call and perform the same tasks that are available from the Topology View.

To display a connection's path:

1. Select the connection you want to display path information about from the connection table by clicking anywhere on the entry.
2. Select **Path Trace** from Connection Table pop-up menu. The selected connection's path is graphically represented in the SPECTRUM VLAN Manager's Path Trace View ([Figure 11-6](#)).



This operation is also available by selecting **Path Trace** from the VLAN Manager's Main **View ? Tapped Connections** window.

Figure 11-6. Path Trace

The SPECTRUM VLAN Manager's Path Trace View consists of a menu bar, a display area, and a status bar.

Path Trace Menu Bar

The menu bar consists of two commands: **F**ile and **V**iew. The **F**ile menu commands are similar to those found in the Topology View's **F**ile menu (Refer to *Topology View File Menu*, on page 13-3). Similarly, the **V**iew >**Z**oom command is similar to the Topology View's **V**iew >**Z**oom command (Refer to *Topology View View Menu*, on page 13-3).

Path Trace Display Area

This area is used to provide a graphical representation of the end-to-end connectivity for a selected connection. Icons show devices such as switches and workstations. A special type of icon shows links between devices. Pop-up menus let you perform many connection related tasks. Refer to *Switch Icon Pop-up Menu*, on page 13-10 and/or *Link Status Pop-up Menu*, on page 13-12.

Path Trace Status Bar

The status bar at the bottom of the view provides layout and zoom factor information. The layout will always be PATH. The zoom Factor will reflect the current zoom percentage being applied to the view.

Releasing a Connection

You can release a call, using **Release Connection**.

To release a call:

1. Select a call to be released from the connection table by clicking anywhere on the entry.
2. Select **Release Connection** from the Connection Table's **Connection** menu or the Connection Table pop-up menu. The selected call is released.



To release all calls for a selected user, select a user from the physical pane and then choose **Release All Connections** from the **Edit >User** menu or select a user from the Directory and then choose **Release All Connections** from the **Edit** menu.

Aging Connections

Aging Connections lets you configure call aging parameters to optimize system performance by releasing connections that have aged out.

Connections are not automatically aged out or removed unless a certain threshold (Age Threshold) is reached.

Aging will occur if the Age Threshold is reached. The number of connections aged out (removed) is determined by the **Number To Age** parameter.

For example, if we set the **Age Threshold** to 70%, and the **Number To Age** to 1000, with the remaining parameters as shown below, the following will happen assuming connection capacity is 8000 connections.

Refer to *Configuring Call Aging*, on page 11-16 for descriptions of all parameters used in this example.

Present Capacity - 70%
Age Pass in Progress - Not Aging Now
Last Age Pass Time - Tue Mar 4 11:10:00 1997
Time Since Last Age Pass - 0+00:04:55
Age Pass Delta - 0+00:00:00
Age Pass Count - 10

Since the **Present Capacity** (70%) (5600 connections) equals the **Age Threshold** (70%), aging will take place. The oldest 1,000 connections will be released from the Connection Table. If any of the calls released were active at the time they were released, they will immediately be reestablished with the next packet the switch receives from the source.

Aging Pass In Progress will change from **Not Aging Now** to **Aging Now**. This happens very quickly and may not even be noticed.

Present Capacity will adjust downward to account for the connections that were removed from the Connection Table. You would think that in our example **Present Capacity** would drop to 58% (4600 connections) immediately: however, that is not the case, since calls are processed 10 at a time and calls that were active when removed will be immediately reestablished. The number would drop gradually as calls were removed until it reached 58% if none of the removed calls were active at the time. If any calls were active, the number might never reach 58%.

Last Age Pass Time will change to 0+11:15:00.

Time Since Last Age Pass will change to 0+00:00:00.

Age Pass Delta will change to 0+00:05:00.

Age Pass Count will change to 11.

When the age pass is completed, **Age Pass In Progress** will change from **Aging Now** to **Not Aging Now**. In this example, connection aging will occur whenever **Present Capacity** reaches 70%.

Configuring Call Aging

Click **Aging Configuration** from the Connection Table's **Edit** menu to display the SPECTRUM VLAN Manager's Aging Configuration window (Figure 11-7). This window identifies which switch call aging information is being collected for, connection aging information, and provides buttons that let you perform several switch aging support functions. If the Enable Aging button is in the (default) deselected (raised) position, aging is not enabled and no connection aging will occur.



Aging Configuration is implemented on a per switch basis. Normally, you probably will want to configure all the switches in a domain with the same parameters.



This operation is also available from the **Edit >Switch** menu.

Figure 11-7. Aging Configuration

SPECTRUM VLAN Manager: Aging Configuration

Switch Name:	192.168.170.125
Maximum Connections Allowed:	8000
Age Threshold(%):	70 (5600 connections)
Number To Age (per age pass):	1000
Statistics Based Aging:	Disabled
Statistics Aging Threshold (%):	

Present Capacity:	70% (# of connections)
Age Pass In Progress:	Not Aging Now
Age Pass Count:	10
Current Time:	Tue Mar 4 11:00:44 1997
Last Age Pass Time:	Tue Mar 4 11:10:00 1997
Time Since Last Age Pass:	0+00:04:55
Age Pass Delta:	0+00:00:00

Buttons: OK, Apply, Age Partial Connections, Age Filter Connections, Age All Connections, Stop Age Pass in Progress, Close

Aging Configuration Attributes

Aging Configuration attributes that can be edited are shown in italics.

- *Age Threshold* - Point at which the connection aging takes effect. The connection aging algorithm computes a percentage value, based on the number of current active calls and the maximum number of connections allowed (16K if unidirectional, 8K if bidirectional). Values can range from 1 to 100. The default value is 95.
- *Number To Age* - Number of connections to age out. The default value is 100.
- *Statistics Based Aging* - Enables or Disables Statistics Based Aging. The default is Disabled.
- *Statistics Aging Threshold* - Point at which the activity based aging takes effect. When the connection count has exceeded the Statistics Aging Threshold, the switch makes a pass through the Connection Table checking the call statistics. One minute later the switch makes another pass through the Connection Table and any connection which has had no change in its call statistics is aged.
- *Present Capacity* - Percentage of maximum connections currently in use. Values can range from 0 to 100.
- *Age Pass in Progress* - Indicates if aging is in progress (**Aging Now**) or not in progress (**Not Aging Now**).
- *Age Pass Count* - The number of aging passes that have occurred.
- *Current Time* - The current time.
- *Last Age Pass Time* - The time that the last age pass occurred.
- *Time Since Last Age Pass* - The time since the last age pass.
- *Age Pass Delta* - The time between the last two age passes.

Aging Configuration Buttons

- **OK** - Accept changes, and then close window.
- **Apply** - Accept changes.
- **Age Partial Connections** - Immediately begin aging process of only Number To Age connections.
- **Age Filter Connections** - Age all filtered calls.

- **Age All Connections** - Immediately begin aging process and continue until all calls that can be aged out are aged out. New calls initiated when the age pass is in progress are not aged out.
- **Stop Age Pass in Progress** - Terminate the current Age Pass.
- **Close** - Return to Connection Table without making changes to the Aging Configuration.

Editing Aging Configuration Attributes

To edit an attribute:

1. Click **Aging Configuration** from the Connection Table's **Edit** menu or the **Edit >Switch** menu. The SPECTRUM VLAN Manager's Aging Configuration window (Figure 11-7) is displayed.
2. Click the attribute field you want to edit (**Age Threshold, Number To Age, Statistics Aging Threshold**).
3. Enter the data for the selected attribute. To overwrite existing data, use the mouse to highlight the old data, and then enter the new data.
4. Click **OK** or **Apply** to make changes or **Close** to close.

Provisioning Calls

You can set up Permanent Virtual Circuits (PVCs) between endpoints within a domain using **Provision Connection**.



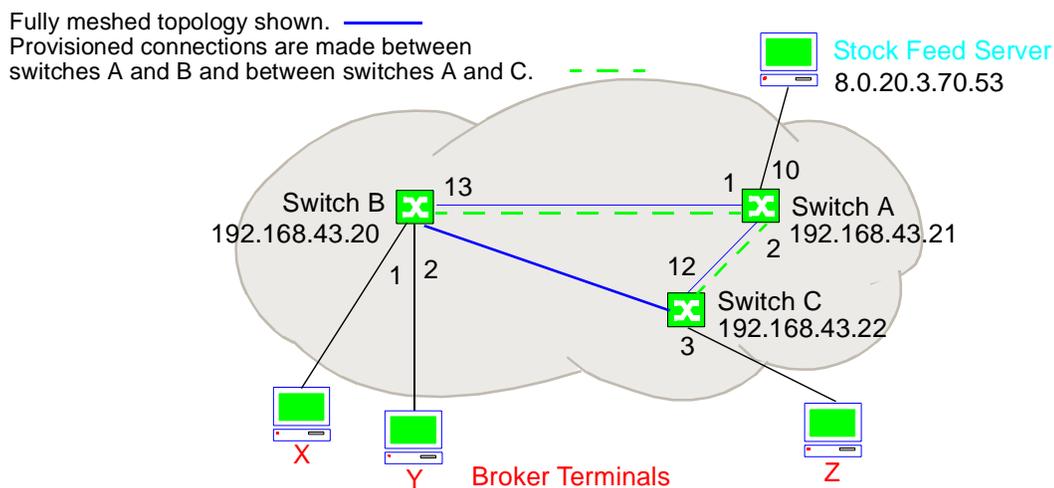
The **ATM/PVC** selection off the Tools menu is used to set up PVCs that traverse ATM networks. Refer to [Chapter 14, Managing VLANs Over ATM Networks](#) for information about setting up PVCs over ATM networks.

Once set up, these permanent connections (calls) are always available. They are not affected by call aging and can only be torn down using Call Release (*Releasing a Connection*, on page 11-14) or resetting the switch.

You may want to send broadcast (or multicast) data from a source node to one or more destination nodes without having to set up (process) new connections each time the data is sent. For instance, you might want to send stock quote information from a stock feed server to brokers terminals at regular intervals. Call provisioning is an ideal tool for this purpose.

Let's say that your stock feed server is connected to switch A and the terminals you want to send stock quote information to are connected to switches B and C, as shown in [Figure 11-8](#). To set up provisioned connections between these devices, you first program switch A, the originating switch, and then program switches B and C, respectively.

Figure 11-8. Call Provisioning Example



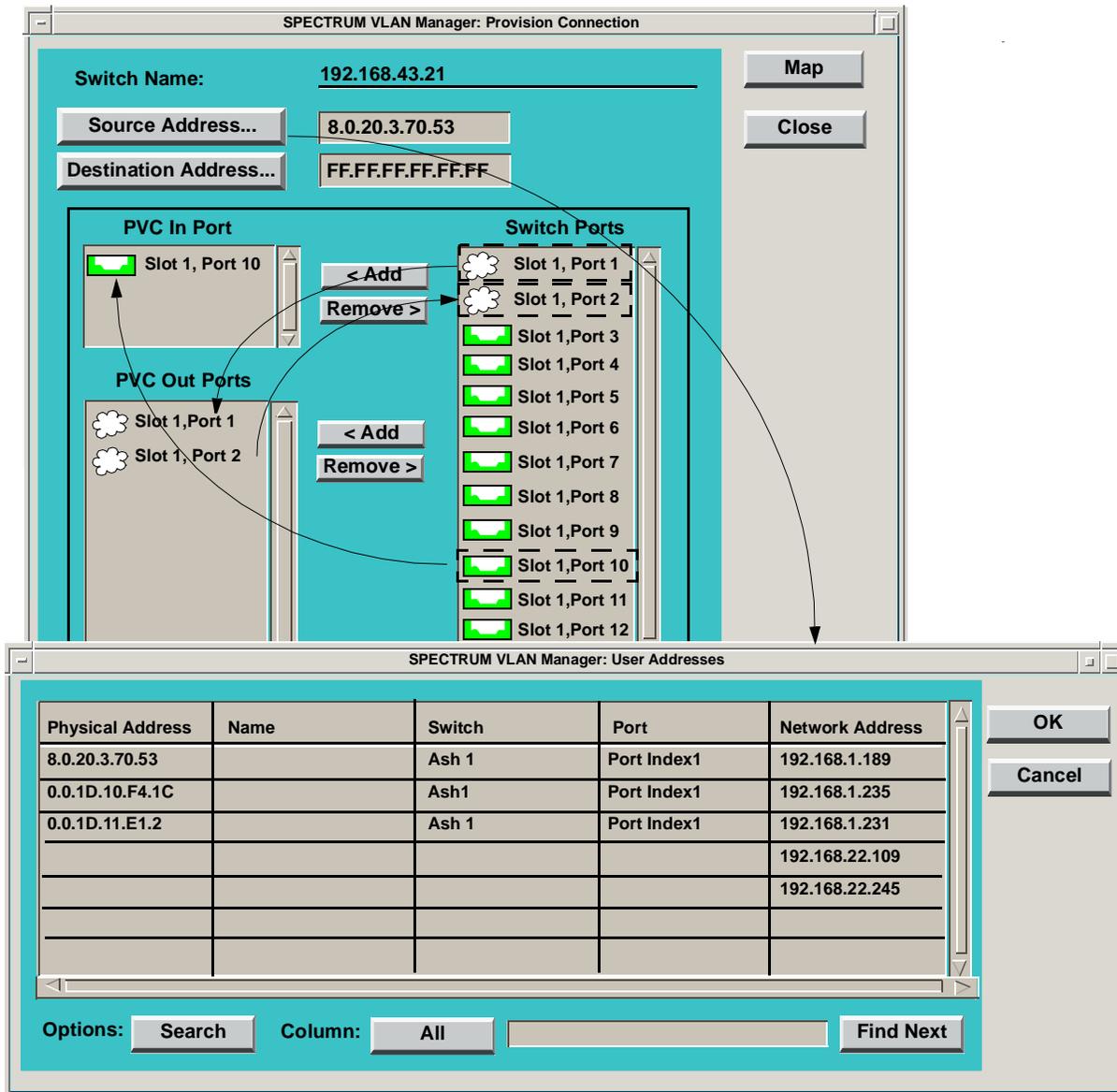
To provision the connections:

1. Select switch A from the VLAN Main window.
2. Select **Provision Connection** from the Connection Table's **Edit >Switch** menu. The Provision Connection window is displayed ([Figure 11-9](#)).



This operation is also available from the Connection Table's **Edit** menu.

Figure 11-9. Call Provisioning



3. Select the source address. In our example, we are using 8.0.20.3.70.53 as the source address, or Stock Feed Server.

Type the source address in the source address field or click the Source Address button to bring up a User Addresses window. Click 8.0.20.3.70.53, and then click OK to enter that source address into the source address field. Click Cancel to return to the Provision window without selecting a source address.

If you don't know the source address, refer to *Using the Directory*, on page 10-14).

4. Select the destination address. In our example, we are using the default FF.FF.FF.FF.FF.FF as the destination address, meaning all endpoints connected to switch B, ports 1 and 2, and switch C, port 3.

Type the destination address in the destination address field or click the Destination Address button to bring up the User Addresses window. If other than FF.FF.FF.FF.FF.FF, enter that address, and then click OK to enter that destination address into the destination address field. Click Cancel to return to the Provision window without selecting a destination address. Multicast and Unicast destination addresses are also allowed. A Multicast destination address would be used to support specific applications such as video conferencing. In this case, you program certain endpoints to listen and respond to the video conferencing applications' multicast address. At this time, there is no practical advantage to setting up a PVC using a Unicast destination address.

5. Select the **PVC In Port**, the switch port that connects the source device to the switch. Click a port in the Switch Ports list and then click **Add**. The port is moved to the **PVC In Port** field (Figure 11-9). In our example, the PVC In port is Port 10.

If you don't know the "in" port, refer to *Using the Directory*, on page 10-14.



When provisioning between two switches that are connected by a PVC, there may be some confusion if there are multiple PVCs on the outgoing switch, as you must choose the exact PVC which connects the two switches. One way to ensure this is to have previously edited the PVC port label.

6. Select the **PVC Out Port(s)**, the ports that connect the switch to the destination devices (or in the case where a call must traverse more than one switch, the next switch or switches in the path). These will be network ports if the provisioned connection will traverse more than one switch. In our example shown in Figure 11-8, we need to enter the network port that connects switch A to switch B, because destinations X and Y are connected to switch B and we need to enter a network port that connects switch A to switch C, because destination Z is connected to switch C. Port 1 connects switch A to switch B and port 2 connects switch A to switch C. Click on Port 1, and then click **Add**. Port 1 is added to the **PVC Out Port** list (Figure 11-9). Click on Port 2, and then click **Add**. Port 2 is added to the **PVC Out Port** list (Figure 11-9). Note that you can select multiple ports by using the "control" key.
7. Click **Map** to create the provisioned connection with the parameters you specified. Your provisioned connection is displayed in the Connection Table. Alternately, you could click **Close** to return to the Provision Connection window without creating a provisioned connection.
8. Repeat steps 1 through 7 to program switches 20 and 22, substituting the values shown below. The source and destination addresses would remain the same.

Switch B

- PVC In Port - 13
- PVC Out Ports - 1,2

Switch C

- PVC In Port - 12
 - PVC Out Port - 3
9. Your provisioned connection is now complete. When the stock feed server sends data out, terminals X, Y, and Z will receive it. There is no need to set up a provisioned connection between switch B and switch C, because we established connections to both switches from switch A.

Tapped Connections

Tapped Connections let you view and manage existing tapped calls for the current domain. Click on **Tapped Connections** from the VLAN Manager **View** menu to display the SPECTRUM VLAN Manager's Tapped Connections window. Except for two additional fields: **Tap Switch** and **Tap Port**, the fields and options in this window are identical to those in the Connection Table.

- **Tap Switch** - Tap point switch
- **Tap Port** - Tap point port

Click on **Release Tap** to remove a tap from a selected call, **Update** to update the current display, or **Close** to dismiss the Tapped Connection window.

Managing IP Multicast Groups

This chapter provides detailed information about creating and administering IP Multicast groups using SPECTRUM VLAN Manager's graphical user interface.

Overview

IP Multicast groups let you set up unidirectional point-to-multipoint connections. Multicasts are most often used when data from a given source must be distributed simultaneously to several destinations (e.g., sending video to a group or disk mirroring). Multicast packets are distributed through the switch cloud using a packet distribution tree rooted at the sender. Only switches in the tree for a particular call get involved with connection setup for that call. The packet distribution tree can add branches without changing the rest of the tree when new receivers join.



The packet distribution tree, the point-to-point connection that gets set up through the switch cloud, is a second tree, independent of the Spanning Tree used for MCSP (Multicast Cabletron Switch Protocol) signaling.

When a multicast connection has been set up, packets are distributed from a sender to all members of a multicast group, using the packet distribution tree from the sender to all receivers in the group.

IP Multicast groups are configured on a port basis. To receive multicasts, the port to which an endpoint is connected must join a multicast group either dynamically, through IGMP (Internet Group Management Protocol) protocol, or statically, using VLAN Manager.

An IP Multicast group is named according to the associated multicast group address, such as ip.224.0.1.2. Ports on which a group is joined through IGMP are also remembered in that group. Any endpoint, whether or not a member of a multicast group, may send to the group unless Allow All Multicast Senders is selected from the **Domain Properties ? Services** tabbed page. Refer to *Services Properties*, on page 6-22.

Endpoints in a switch domain are able to send and join multicast groups that extend beyond the domain. A switch sends IGMP reports to routers to join groups and thereby receive their external multicasts, and then send beyond the switch cloud by sending out on ports with attached routers.

A separate point-to-point connection in a switch is set up for each group sender. When a new source begins to send, the group source information is signaled in a MCSP (Multicast Cabletron Switch Protocol) message along an “all switches” signaling channel which follows the spanning tree links. Any switch that has local receivers for this group then unicasts a connection setup message back to the sender.

An IP Multicast group is created for each multicast address detected. Each IP Multicast group contains all senders and receivers for that multicast address.

IP Multicast groups do not follow and are not restricted by the same rules by which VLANs are regulated. For instance, you cannot drag an IP Multicast group to a switch or port and you cannot apply policy to an IP Multicast group.

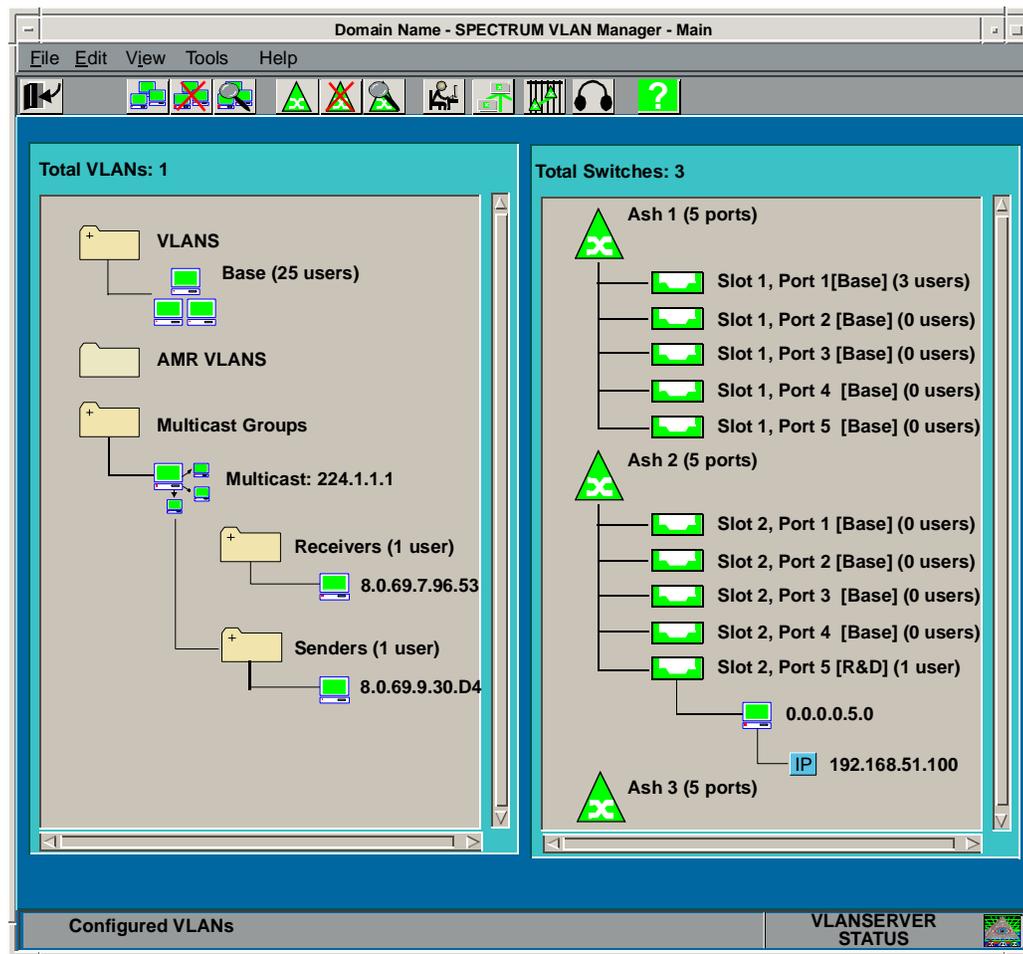
Displaying IP Multicast Groups

Figure 12-1 shows the VLAN Manager’s Main window with one IP Multicast group shown in the left window pane. The  icon is used to distinguish an IP Multicast group from a VLAN. Multicast users are categorized as either receivers or senders. Receivers are placed in the Receivers folder. Senders are placed in the Senders folder.



By default, only related aliases are displayed for a particular IP Multicast group. You can choose to have all aliases displayed. Refer to *Main Preferences*, on page 5-3.

Figure 12-1. Displaying IP Multicast Groups



Editing Multicast Properties

VLAN Manager provides numerous ways to control multicast access using the VLAN Manager Discovery and Router Wizards and the switch and, port properties settings.

- To enable or disable multicast for an entire SFS domain, you use the VLAN Manager Discovery Wizard or the Domain Multicast properties settings.
- To enable or disable multicast for a specific router, you use the VLAN Manager's Router Wizard.
- To control port access to multicast groups, you use the switch multicast properties settings.

Enabling and Disabling Multicast for an Entire Domain.

Refer to *VLAN Manager Domain Discovery Wizard*, on page 6-1, or *Domain Properties*, on page 6-18 for information about enabling or disabling multicast support for an entire domain.



You can enable or disable multicast on an individual switch basis using the **Domain Wide Services** view from the **Edit >Domain** menu.

Enabling or Disabling Multicast for a Router

Refer to *Configuring a Router Port*, on page 8-9, for information about enabling or disabling multicast support for a specific router.

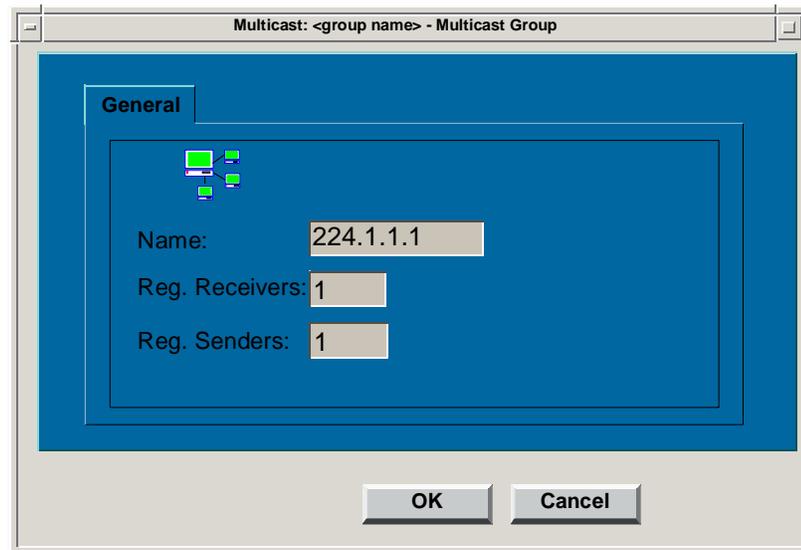
Controlling Access to Multicast Groups

You can view and edit IP Multicast group, switch, and port properties using VLAN Manager's popup menus.

IP Multicast Group Properties

To view IP Multicast group properties, select an IP Multicast group, use the right mouse button to bring up the VLAN User pop-up menu, and then select **Properties**. The Properties tabbed folder is displayed ([Figure 12-2](#)).

Figure 12-2. IP Multicast Group Properties



This folder consists of the following tabbed page: **General**.

- **General** - Provides the following read-only information about the selected IP Multicast group (Figure 12-2).
 - **Name** - The name of this IP Multicast group.
 - **Reg. Receivers** - The total number of registered hosts receiving data from this IP Multicast group. At least one receiver per switch must register for a particular multicast group address in order for that switch to receive data from that address.
 - **Reg. Senders** - The total number of hosts sending data to this Group Address. All senders are registered to send to a particular multicast group address.

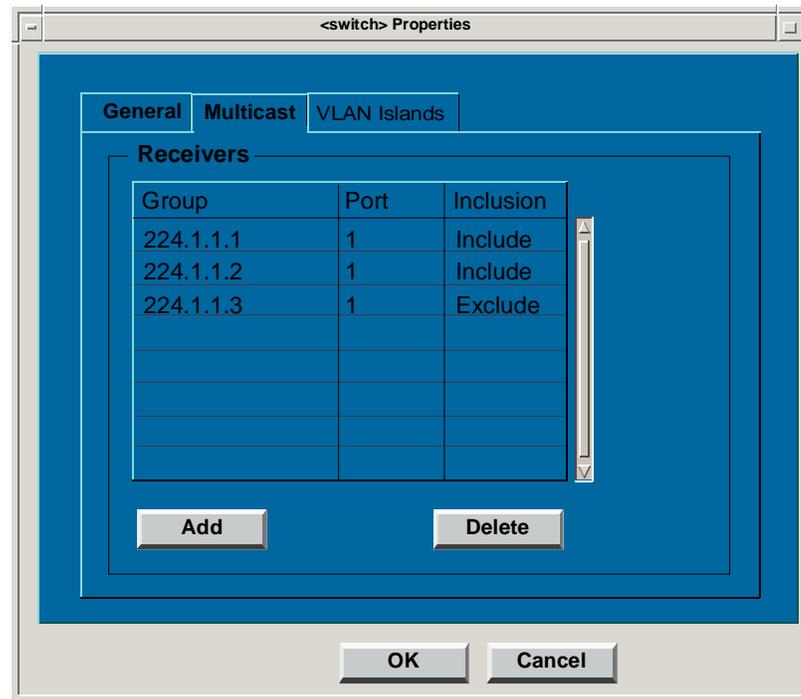
Switch Properties

To view and/or edit switch properties, select a switch, use the right mouse button to bring up the VLAN User pop-up menu, and then select **Properties**. The **Properties** tabbed folder is displayed (Figure 12-4). This folder consists of the following tabbed pages: **General** and **Multicast**.

- **General** - Refer to *General Switch Properties*, on page 7-4 for information about the General Switch Properties View.
- **VLAN Islands** - Refer to *VLAN Islands View*, on page 7-9 for information about the VLAN Islands View.

- **Multicast** - Provides receiver information about IP Multicast groups associated with the selected switch (Figure 12-3). You can also add or delete receivers using this window.

Figure 12-3. Switch Properties (Multicast)



- **Group** - IP Multicast group name.
- **Port** - Access port number.
- **Inclusion** - Include or Exclude.
 - **Include** - Allow IP Multicasts
 - **Exclude** - Do Not allow IP Multicasts
- **Add/Delete** - Since Multicast is port-based, **Add** and **Delete** let you include or exclude certain or all IP Multicast groups on certain or all ports of a switch.

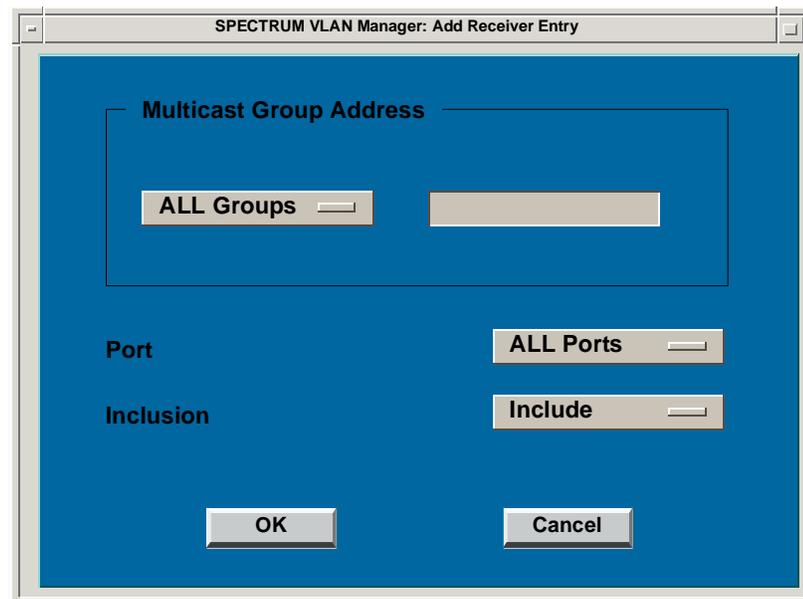
Delete a Receiver

To delete a receiver, select the receiver you want to delete and then click **Delete**.

Add a Receiver

To add a receiver, click **Add** from the **Switch Properties ? Multicast** window. The Add Receiver Entry window is displayed (Figure 12-4).

Figure 12-4. Add Receiver



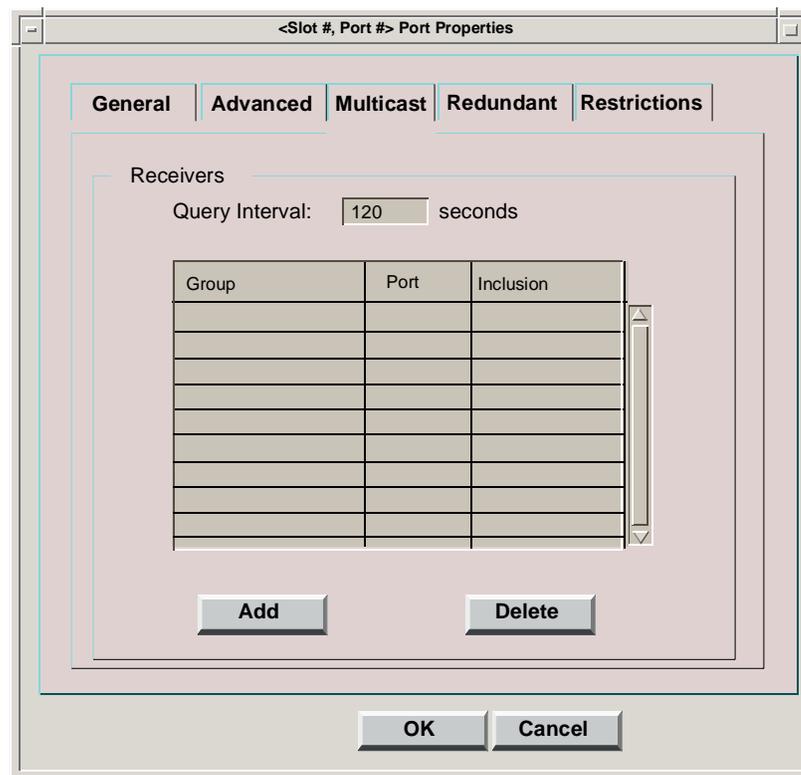
10. Select the Multicast group address to which you want to add a receiver. You may select the “default”, **All Groups**, or select **Custom** or **IGMP Groups** from the drop-down list. If you select **Custom**, enter the IP Multicast address of the group.
11. Select the port you want to add as a receiver to the group you selected in the previous step. You may select the “default”, **All Ports**, or select a port from the drop-down list.
12. Select a policy: **Include** or **Exclude**. If you select **Include**, IP Multicasts will be allowed from the Multicast Group Address to the Port you selected. If you select **Exclude**, IP Multicasts will not be allowed from the Multicast Group Address to the Port you selected.
13. Click **OK** to accept changes and close the window or click **Cancel** to dismiss the window without making changes.

Editing IP Multicast Port Properties

To view and/or edit IP Multicast port properties, select a switch port, use the right mouse button to bring up the switch port pop-up menu, and then select **Properties**. The **Properties** tabbed folder is displayed. This folder consists of the following tabbed pages: **General**, **VLAN**, **Multicast**, and **Redundant**. Refer to *Switch Properties*, on page 7-4 for information about the **General** switch port properties.

- **Multicast** - Provides the following information about the selected Multicast group (Figure 12-5).
 - **Query Interval** - Lets you set the amount of time between IP Multicast queries. Valid values are 60 to 180 and 0. The default is 120 seconds. If you set the query interval to 0, querying is disabled.

Figure 12-5. Multicast Port Properties



Deleting a Multicast Group

To delete a Multicast group:

1. Select the Multicast group you want to delete.
2. Choose **Delete** from the **Edit** menu. The group is deleted.

Viewing Domain Topologies and Managing Switch Links

This chapter provides step-by-step instructions for performing link administration tasks using SPECTRUM VLAN Manager's graphical user interface. It also contains reference information, and helpful tips to help you perform these tasks.

Viewing Domain Topologies

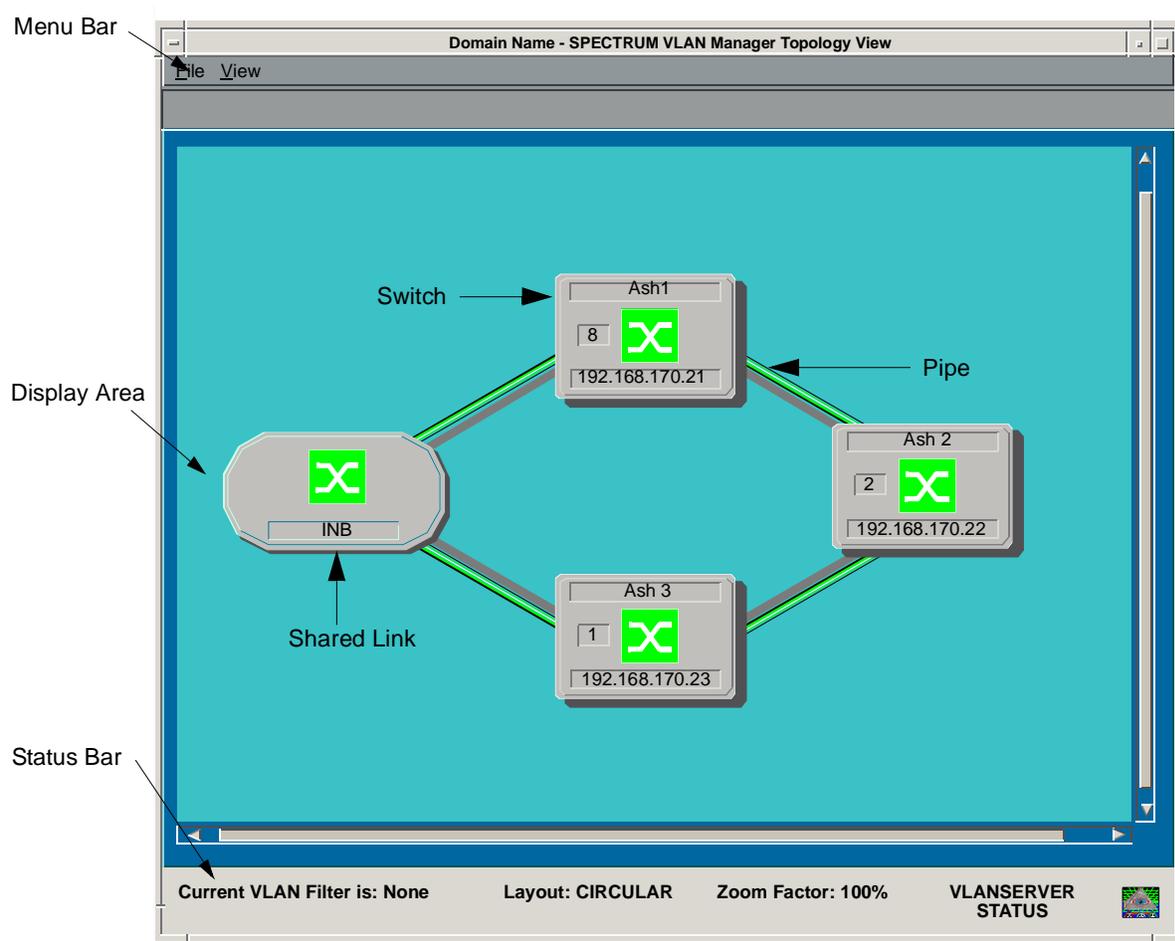
The Topology View provides a live graphical display of all switches and switch links for the current domain.

This view consists of a menu bar, a topology display area, and a status bar (Figure 13-1).

- **Menu Bar** - Lists available menus. Select a menu to display a list of commands for that menu.
- **Topology Display Area** - Displays information and color coded status information about all switches and links in the current domain.
- **Status Bar** - Displays current VLAN filter, layout, and zoom factor information, as well as VLANServer color-coded status information.

To display the Topology View, select **Topology** from the **View** menu or click  on the Tool Bar. It takes a few seconds for the view to come up. During that time, “Initializing....” is displayed.

Figure 13-1. Topology View



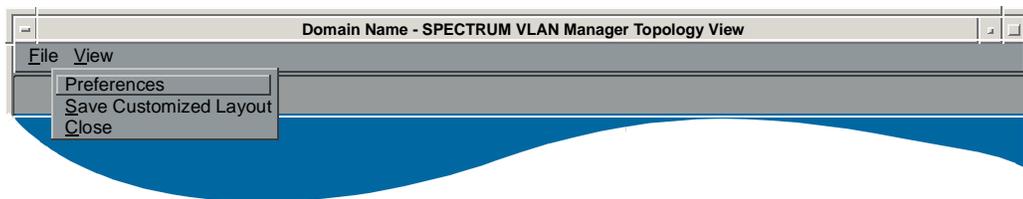
Topology View Menu Bar

The topology view menu bar provides access to two menus: **F**ile and **V**iew.

Topology View File Menu

The **F**ile menu (Figure 13-2) has three selections: **P**references, **S**ave Customized Layout, and **C**lose. Click **C**lose to exit out of the VLAN Manager Topology View and return to the SPECTRUM VLAN Manager Main window. Click on **S**ave Customized Layout to save the current topology layout to the VLANServer database. Click **P**references to display the SPECTRUM VLAN Manager's Preferences window. For information about setting preferences, refer to [Chapter 5, Managing Preferences](#).

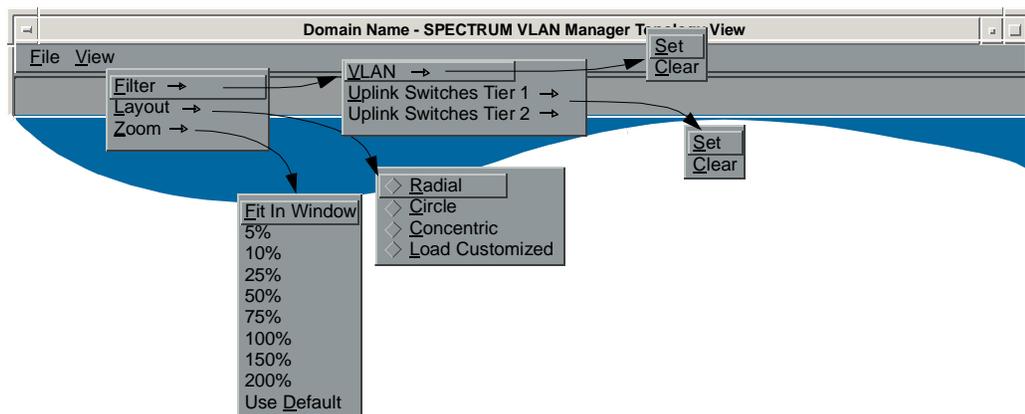
Figure 13-2. File Menu



Topology View View Menu

The **V**iew menu selections (Figure 13-3) are **F**ilter, **L**ayout, and **Z**oom.

Figure 13-3. View Menu



Filter

Filter lets you selectively highlight topology view icons so that the switches that have connections to the members of a selected VLAN or Uplink Chassis are surrounded by a yellow rectangle. Click on **Filter >VLAN**, or one of the **Uplink Switches** options to choose how the view is to be filtered.

VLAN

Set lets you filter the topology view so that the switches that have connections to the members of a selected VLAN are surrounded by a yellow rectangle. The number of users on a switch in the filtered VLAN are displayed in the switch icon (Figure 13-8). **Clear** unhighlights the switches that were highlighted by a topology applied VLAN filter.

To set the topology filter:

1. Choose **Set** from the **Filter >VLAN** menu to display the Select VLAN dialog box (Figure 13-4).

Figure 13-4. Select VLAN Dialog Box



2. Select a VLAN. You can use the **Filter** to find a particular VLAN.

To use this feature:

- a. Click anywhere in the **Filter** text box.
- b. Enter the name of the VLAN you want to find. As you type, VLAN names that do not match the filter criteria will be removed from the VLAN list. Only the domain names that match your filter criteria will remain.
- c. Click on the name of a VLAN and then click **OK** to set the selected VLAN as the filter and to highlight the switches that have connections to the members of that VLAN. Click **Cancel** to terminate the VLAN Filter set.

Uplink Switches Tier 1**Uplink Switches Tier 2**

Set lets you filter the topology view so that the switches configured as Tier 1 or Tier 2 uplink switches are surrounded by a yellow rectangle. **C**lear unhighlights the switches that were highlighted by a topology applied Uplink filter.

To set the topology filter:

1. From the **View>Filter** menu, select either **Uplink Switches Tier 1** (to highlight Tier 1 uplink switches) or **Uplink Switches Tier 2** (to highlight Tier 2 uplink switches).
2. Choose **S**et .

See [Expanding a Domain Using Uplink Switching](#) on page 6-34 for more information on uplink switching.

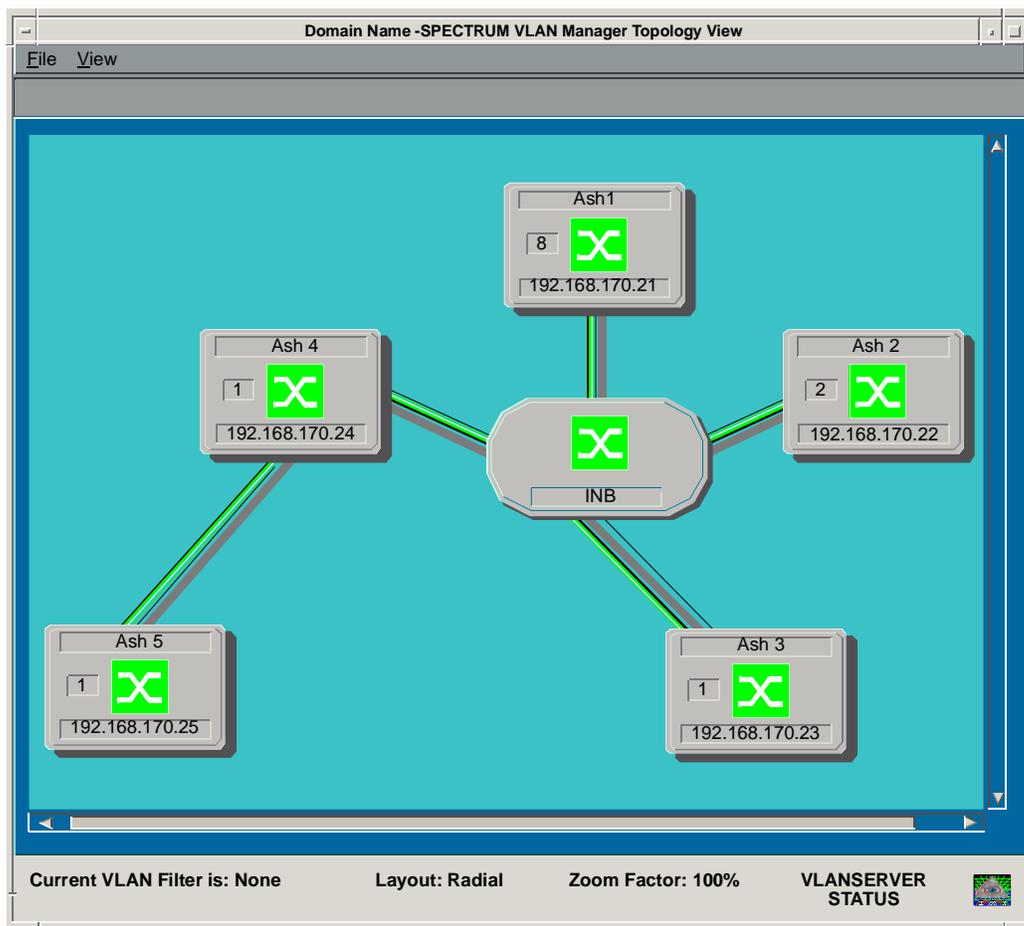
Layout

Click on **L**ayout ?**R**adial, **C**ircle, **C**oncentric, or **L**oad Customized to choose how the icons in the topology view are displayed. The default layout is **L**oad Customized. All icons are cascaded in the upper left-hand corner of the Topology view until a customized layout is saved.

Radial Layout

Radial ([Figure 13-5](#)) places the switch with the greatest number of links in the center of the display with the other switches grouped around it.

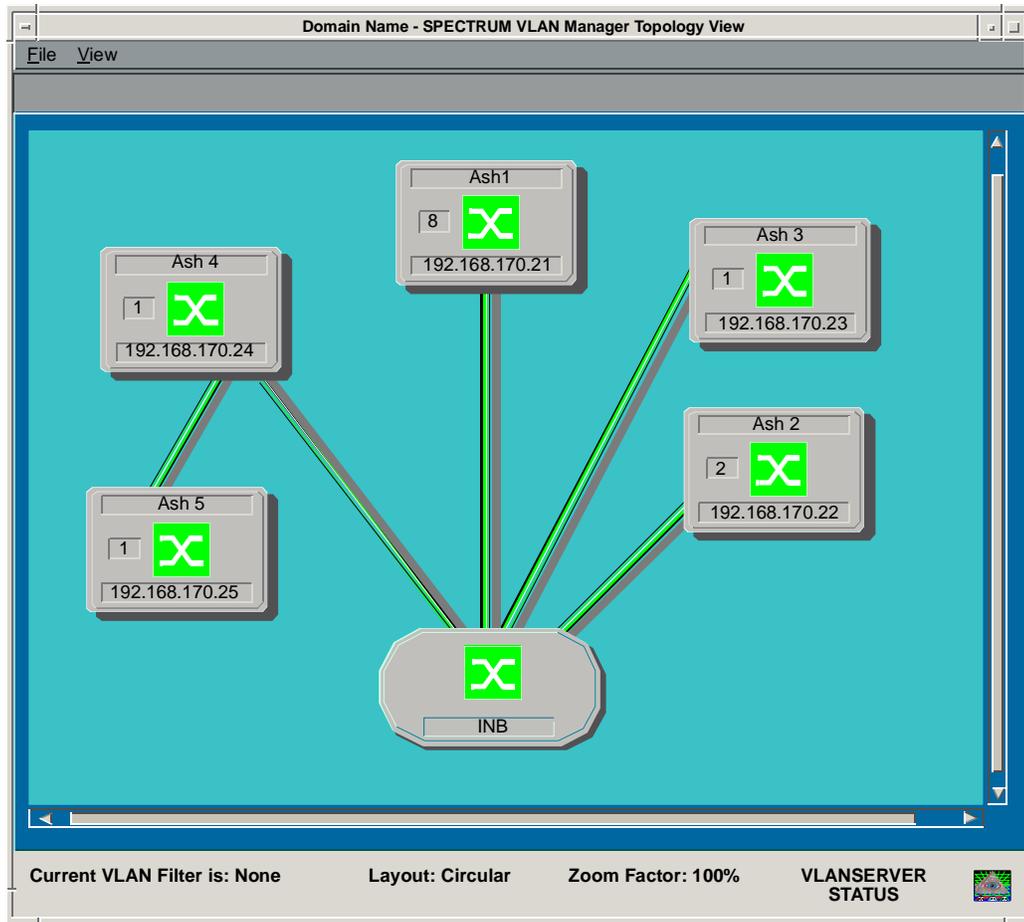
Figure 13-5. Radial Layout



Circle Layout

Circle (Figure 13-6) displays all switches in a circular arrangement.

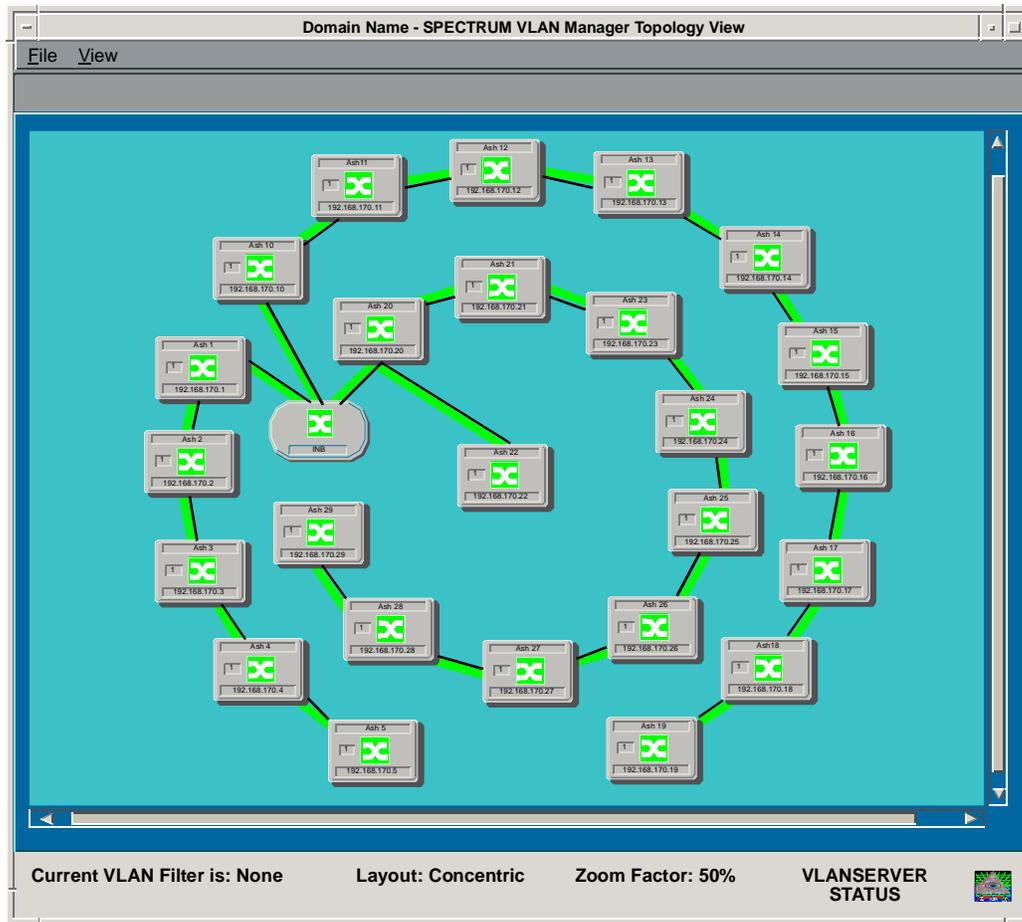
Figure 13-6. Circular Layout



Concentric Layout

Concentric (Figure 13-7) displays all switches in an expanding circular arrangement.

Figure 13-7. Concentric Layout

**Customized Layout**

Customized lets you customize the appearance of the current domain topology by letting you arrange the topology's icons in whatever layout best suits your needs and you can then save the new topology layout to the VLANSERVER database. The latest saved topology layout is displayed when **Customized** is selected from the Layout menu.

All users running against the same VLANSERVER can make changes to the topology layout, using **Customized**.

To create a customized topology layout:

1. Arrange the icons in the topology by clicking and holding an icon (a black outline will appear around the icon), and then dragging the icon to where you would like it placed.



You can move multiple icons around all at once. To do this, select the icons you want to move. Hold and drag the last icon selected. All selected icons move simultaneously.

2. Click **Save Customized Layout** from the **View** menu. Your customized topology layout is saved to the VLANServer database. The following message is displayed when **Save Customized Layout** is selected from the **File** menu: Save changes to customized layout? Note that this will overwrite the existing customized layout for this VLANServer.

Zoom

Click on **Zoom** (Figure 13-3) to display the zoom selection menu. Select one of the choices listed to proportionally increase or decrease the size of the icons in the topology view. **Fit in Window** will zoom the icons to the largest percentage that still allows all icons to be displayed in the view. **Use Default** zooms the icons in the view to the percentage specified by **File > Preferences**. Refer to [Chapter 5, Managing Preferences](#).

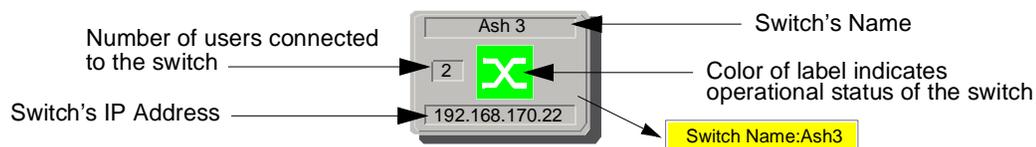
Topology Display Area

The topology display area's icons provide information about the number of users attached to each switch in the domain, the operational status of each switch, and the status of switch links.

Switch Icons

Switch icons (Figure 13-8) provide operational and configuration information as well as access to several support functions. The background of each switch icon label is color-coded to represent the operational condition of that switch: Red for down, Green for up, Blue for initial, and Orange for can ping device but not execute SNMP commands.

Figure 13-8. Switch Icon



A text box above the switch label shows the name of the switch. A text box to the left of the switch label shows the total number of users connected to a switch determined by the VLAN filter selected. A text box directly under the switch label shows the switch IP address.

The switch name is displayed in a pop-up (also called a fly-by) each time the cursor is positioned on the switch icon and not moved for a short time.

The switch pop-up menu provides access to switch related management functions.

Switch Icon Pop-up Menu

The switch icon pop-up menu consists of the following commands: **Properties**, **Switch Details**, **Switch Users**, **Network Connections**, and **Delete Switch**. To select any of these commands, move the cursor over a switch icon, click and hold the right mouse button to display the switch icon pop-up menu, drag the cursor to the command you want to execute, and then release the button.

- **Properties** - Display the Switch Properties tabbed folder. Refer to *Switch Properties*, on page 7-4.
- **Switch Details** - Displays the Switch Details window for the selected switch. Refer to *Displaying Switch Details*, on page 7-11, for information about this window. You can also display this window by double-clicking anywhere on the switch icon with the left mouse button.
- **Switch Users** - Displays the users filtered for the selected switch. It uses the same format as the Directory window. Refer to *Using the Directory*, on page 10-14.
- **Network Connections** - Displays the Network Connections window ([Figure 13-9](#)).

Local Port - Port on which a selected switch hears an adjacent switch.

Neighbor Name - Name of the switch adjacent to the selected switch.

Neighbor IP - Network address of the switch adjacent to the selected switch.

Status - Operational status of the connection between the selected switch and its neighbor. Valid entries are: UP and DOWN. The status of the connection is also indicated by the color of the  icon: Green for UP or Red for DOWN.

Type - Type of connection between the selected switch and its neighbor. For example - Ethernet, FDDI, or INB.

Bandwidth (Mbps) - Total aggregate bandwidth of the connection between the selected switch and its neighbor. For example: Ethernet (10Mbps), FDDI (100Mbps), INB (2500Mbps), ATM (155Mbps).

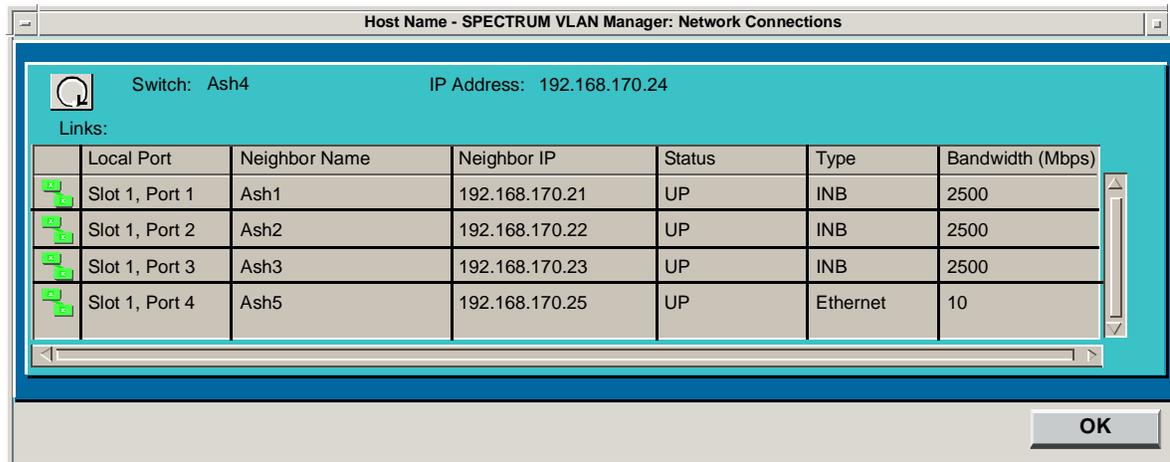
- **Delete Switch** - Delete the selected switch from the VLANServer database.

Managing Switch Links

The Network Connections window provides detailed information about the selected switch's neighbors and the connection to its neighbor. This window consists of header information and a **Links** table. The header information provides the name of the selected switch and the IP address of the selected switch. The **Links** table contains the following fields: **Local Port**, **Neighbor Name**, **Neighbor IP**, **Status**, **Type**, and **Bandwidth (Mbps)**. Use the **OK** button to dismiss the Network Connections window.

The Network Connections pop-up menu lets you delete a failed network connection or display the Link Utilization View. Refer to the *Link Status Pop-up Menu*, on page 13-12.

Figure 13-9. Network Connections



Pipes

A pipe represents one or more links between switches. Pipes provide information about the operational status of all links between switches. If all links between switches are up (Green), the pipe between those switches will be Green. If at least one, but not all links between switches is not down (Red), the pipe between those switches will be Yellow. If all links between switches are down (Red), the pipe between those switches will be Red.

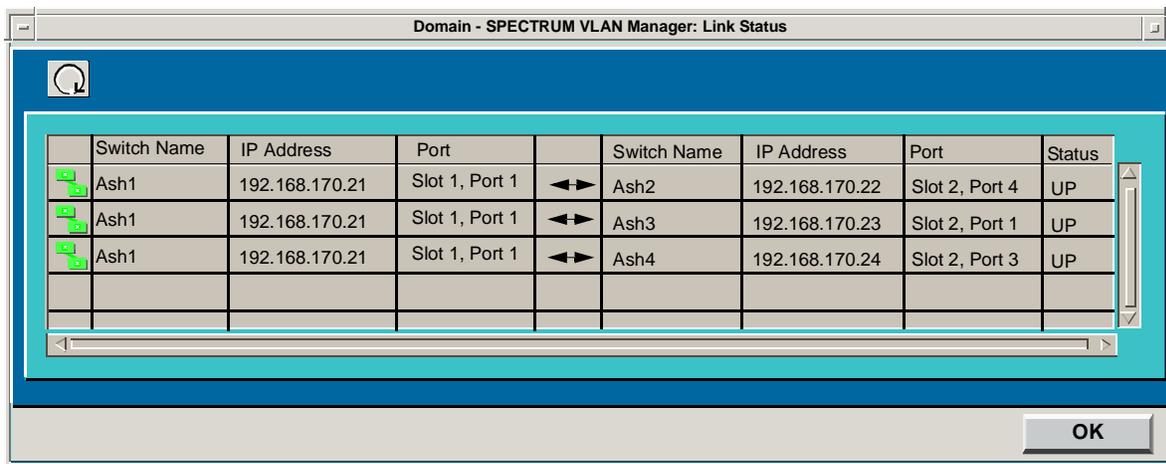
A pipe will be Grey if contact is lost with one of the switches to which it is attached.



Switch links can only be deleted by using **Delete Link** from the Link Status pop-up menu, and, they can only be deleted if the link is down.

Double-click on a point-to-point pipe, double-click on a shared link icon (e.g., INB, FDDI, ATM), or use the pop-up menu to display the SPECTRUM VLAN Manager's Link Status window (Figure 13-10). This window provides detailed information about the links the selected pipe represents. For each link, the name, IP address, and port number of each switch connected to that link are provided along with the type of link, the bandwidth of the link, and the status of the link. The status of a link is shown graphically in the left-most column; Green for up, Red for down, and Grey for unknown. Click **OK** to dismiss the Link Status window. You use the update button to query the link and display the most current information about the link.

Figure 13-10. Link Status



Link Status Pop-up Menu

The Link Status pop-up menu consists of **Delete Link**. To select this command, move the cursor over a link entry, click and hold the right mouse button to display the link status icon pop-up menu, highlight the **Delete Link** command, and then release the button. .

- **Delete Link** - Permanently deletes a switch link from the VLANServer database. A link cannot be deleted if it is up (Green).

Shared Links

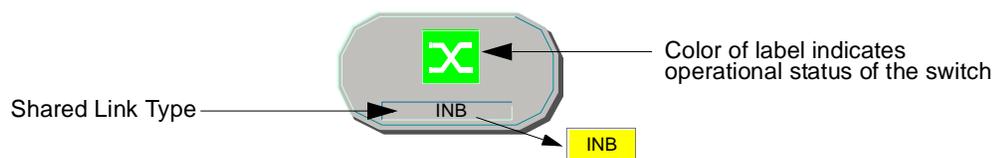
Shared links, such as INB, FDDI, and ATM, represent a connection between switches where each switch can hear more than one neighbor switch. For example, if switches Ash1, Ash2, Ash3, and Ash4 in Figure 13-6 are connected to an INB (Integrated Network Bus) shared link, Ash1 can hear switches Ash2, Ash3, and Ash4; switch Ash2 can hear switches Ash1, Ash3, and Ash4, and switch Ash3 can hear switches Ash1, Ash2, and

Ash4. All switches on the shared link can hear every other switch on the shared link. Switch Ash5 is not on the INB shared link, so it can only be heard by neighboring switch Ash 4.

When displaying the Link Status window for a switch on a shared link, information about the links between that switch and all other switches on the same shared link will be shown. In our example, if we bring up a Link Status window for the link associated with switch Ash1, information about the links from switch Ash1 to switches Ash2, Ash3, and Ash4 is displayed.

In the Topology View, a special icon (Figure 13-11) is used to represent a shared link. In our example, the links between switches Ash1, Ash2, Ash3, and Ash4 all converge on the INB shared link icon.

Figure 13-11.



Managing VLANs Over ATM Networks

This chapter provides an overview of managing VLANs over ATM networks, presents information about current methods of managing VLANs over ATM networks, and describes how to create and manage VLANs over ATM networks using those methods.

Overview

VLAN Manager interoperates with ATM networks to extend the VLAN Manager's ability to manage SecureFast VLAN domains across ATM networks. VLANs and VLAN domains that traverse ATM networks are managed as if the ATM network was transparent.

VLAN Manager offers two methods to provide management over ATM networks: Permanent Virtual Circuits (PVCs) and Switched Virtual Circuits (SVCs).

- **Permanent Virtual Circuits** - Lets you manage VLAN domains across ATM networks by using Permanent Virtual Circuits (PVCs). PVCs provide a permanent connection across an ATM network from one VLAN domain to another, making it possible to collapse multiple domains into a single domain and manage them as a single domain. PVCs must be manually configured.
- **Switched Virtual Circuits** - Lets you manage VLAN domains across ATM networks by using Switched Virtual Circuits (SVCs). SVCs provide switched connections across an ATM network from one VLAN domain to another, making it possible to collapse multiple domains into a single domain and manage them as a single domain. SVCs are automatically configured.

Check the VLAN Manager and switch firmware product SRNs to determine which methods are compatible with your network.

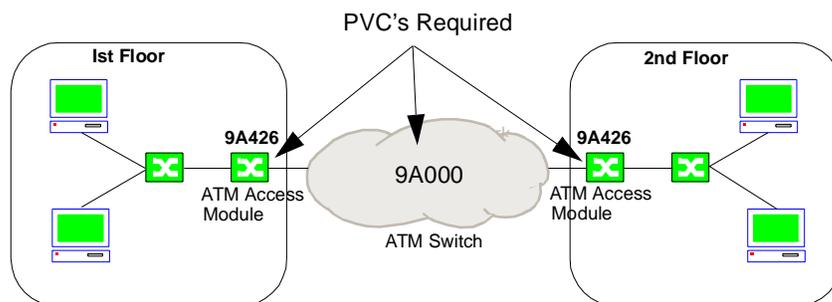
Once you have configured your VLANs and or VLAN domains for ATM interoperation, using VLAN Manager to manage your VLAN network remains essentially the same as managing VLANs over non-ATM networks. Managing VLANs over ATM networks using VLAN Manager allows you to migrate towards an ATM network environment while allowing you to maintain your investment in the SecureFast components of your network.

Managing VLANs Over ATM Networks Using Permanent Virtual Circuits

You can manage VLANs across ATM networks using Permanent Virtual Circuits (PVCs). Suppose for example that you have users in a functional group physically located on two different floors in your building. Each floor is configured with multiple switches, endpoints, etc, and you are using an ATM backbone for inter-floor data communication. Setting up a PVC between the two floors lets you manage the devices on both floors as a single domain.

To manage VLANs over ATM networks using PVCs, you program PVC connections into every switch (ATM switches and Cabletron ATM Access Modules) along the path from one ATM Access Module to another ATM Access Module. For example, if two floors are inter-connected via an ATM network consisting of a single ATM switch, you must create PVCs into both ATM Access Modules and configure a bi-directional VCC (Virtual Channel Connection) into the ATM switch (Figure 14-1).

Figure 14-1. PVCs



When a PVC has been created from end-to-end (one ATM Access Module to other ATM Access Module), the entire topology is discovered. To add additional devices to this configuration, you would create additional PVCs from each ATM Access Module to the ATM switch and configure additional VCCs through the ATM network.

Creating PVC/VCC Connections

The way in which you create a PVC or configure a VCC depends on the type of switch and on how your network is configured.

Switch Type

You create PVCs on ATM Access Modules, those switches connecting a non-ATM switch fabric to an ATM network using Cabletron’s ATM Administrator Management SPMA, or the modules local management tool.

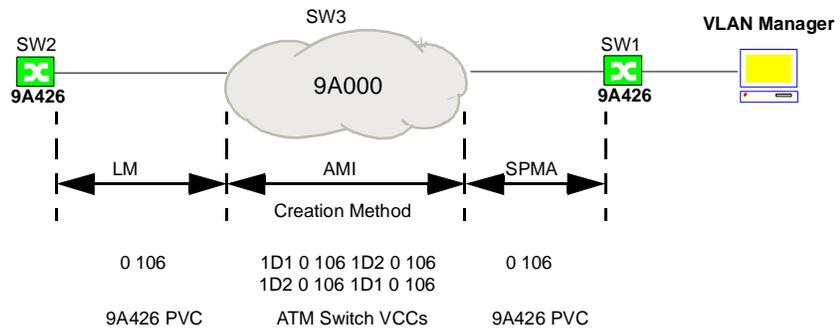
You create VCCs on ATM switches using the manufacturer’s local management tool.

Network Configuration

VLAN Manager cannot manage switches unless a pingable connection exists between the switch to be managed and VLAN Manager. For instance, in Figure 14-2 a pingable connection exists between the workstation running VLAN Manager and SW1; however, no pingable connection exists between VLAN Manager and SW2.

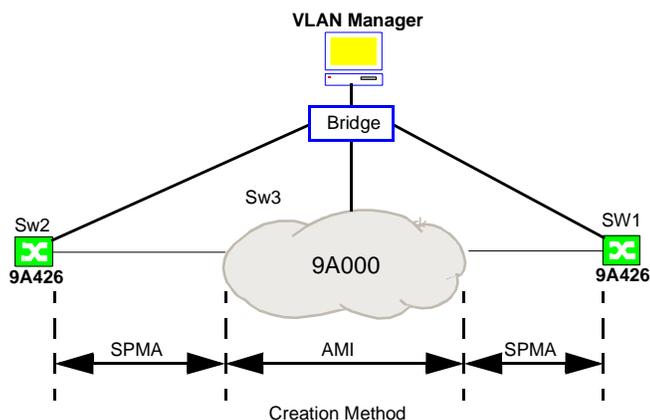
In this scenario, you would connect your console to the serial port on the ATM switch and use the switch’s local management (AMI) to configure a bi-directional VCC on the switch. You would then use Cabletron’s ATM Administrator SPMA to create a PVC from SW1 to the ATM switch. Since the VLAN Manager cannot manage SW2 (no pingable connection exists), you would connect your console to the chassis’s communications port and use the 9A426-02’s local management tool to create a PVC from SW2 to the ATM switch.

Figure 14-2. Create PVC Scenario 1



In the scenario depicted in Figure 14-3, there are pingable connections between the workstation running VLAN Manager and both ATM Access Module switches and the ATM switch. To set up the required PVCs, you would connect your console to the serial port on the ATM switch or telnet to the switch and use the switch’s local management (AMI) to configure a bi-directional VCC into the switch. VLAN Manager discovers SW1, but you have to create SW2 using **Switch ? Create**, and then use the ATM Administrator SPMA to create a PVC from SW1 to the ATM switch and another from SW2 to the ATM switch.

Figure 14-3. Create PVC Scenario 2



Creating an End-to-end PVC

This procedure is based on the network configuration depicted in [Figure 14-2](#). To create a PVC between one ATM Access Module and another ATM Access Module:

1. Configure a bi-directional VCC into SW3. Use the ATM switch manufacturer's local management tool, in this case AMI, to create the VCCs. Refer to *Using AMI to Create VCCs*, on page 14-11, for information about how to create VCCs using the (AMI) ATM Management Interface.
2. Create a PVC connection between SW1 and SW3 using Cabletron's ATM Administrator Management SPMA. Use the same Virtual Path Identifier (VPI)/Virtual Channel Identifier (VCI) pairs you used when you programmed the ATM switch.
 - a. From the VLAN Manager's Main window, select the ATM Access Module into which you want to create a PVC.
 - b. Select **ATM PVC** from the VLAN Manager's **Tools** menu. The ATM Administrator SPMA is launched. Refer to *Using the ATM Administrator Management SPMA to Create PVCs*, on page 14-5, for directions about adding a PVC. At this point, a PVC (network) port is created.
3. Create a PVC connection between SW2 and SW3 using the module's local management tool. Use the same VPI/VCI pairs you used when you created PVCs into the ATM switch. Refer to *Using Local Management to Create PVCs*, on page 14-12, for directions about creating a PVC on a 9A426-02.

The following will occur when all PVC connections have been created from end-to-end.

- The VLAN Manager's Topology view will display the composite topology of all switches in the domain.

- The VLAN Manager's Main window will show the PVCs created on the ATM Access Modules. This usually occurs on the second poll following the creation of the last PVC. Remember, the default poll is set to 300 seconds. You may want to lower the poll time so your changes take effect more quickly.



The default label for a PVC port is Slot #, Port #. You may want to edit the PVC port labels to reflect the switch to which a PVC connects.

Using the ATM Administrator Management SPMA to Create PVCs

To program a PVC into a Cabletron ATM Access Module, you can use Cabletron's ATM Administrator Management SPMA. To do this, you access the ATM Administrator Management SPMA, display the Current Connections screen, and then program the PVC. This section uses the 9A426-02 as an example.

Under certain conditions, you may have to use the ATM Interface's local management tool to create PVCs.

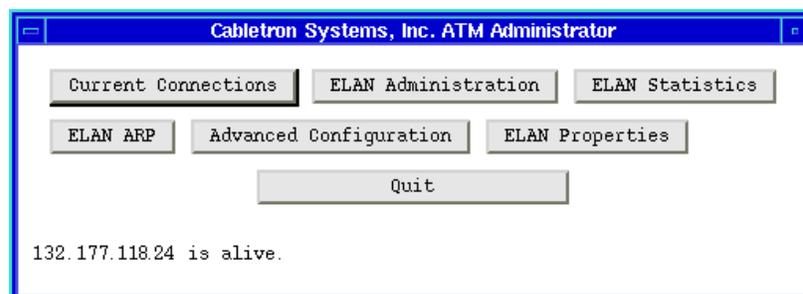


Note that the ATM Administrator Management SPMA has the capability of letting you perform management tasks other than creating PVCs; however, those tasks are beyond the scope of this guide. Refer to the ATM Administrator Management SPMA documentation for a comprehensive description of this product.

Accessing the ATM Administrator Management SPMA

1. You access the ATM Administrator Management SPMA for a particular switch by selecting the switch in the VLAN Manager Main window and then selecting **ATM PVC** from the **Tools** menu. The ATM Administrator screen is displayed (Figure 14-4).

Figure 14-4. ATM Administrator Screen



2. Select **Current Connections**. The Current Connections screen is displayed (Figure 14-5).

Current Connections

The Current Connections screen (Figure 14-5) lets you view and modify the virtual connections established at the device. The Current Connections screen provides a snapshot of both the Permanent Virtual Connections (PVCs) and Switched Virtual Connections (SVCs) configured on the device.

Figure 14-5. Current Connections Screen

The screenshot shows a window titled "Current Connections Screen". It is divided into several sections:

- Device Data:** Contains fields for IP Address (192.168.59.56), Device Name (192.168.59.56), and Device Location (empty).
- Connection Data:** Contains fields for Maximum Connections (1024) and Currently Configured (4).
- ATM Interface:** A dropdown menu showing "7".
- Settings:** A table with columns: Port, VPI, VCI, Encapsulation Type, VC Type, Oper. Status, and Up Time.

Port	VPI	VCI	Encapsulation Type	VC Type	Oper. Status	Up Time
4	0	4	Other	???	Up	0
4	0	4	Other	???	Up	0
4	0	4	VC MUX Bridged Protocol 802.3	???	Up	0
4	2	4	VC MUX Bridged Protocol 802.3	???	Up	0
- Buttons:** Add, Delete, Disable, Modify, Close, and History.

When you first open the screen, the connection entries will be read from the device. The display will be refreshed automatically when any subsequent edits are made to the entry list.

Device Data Fields

The following information appears in the Device Data portion of the Current Connections screen:

- **IP Address** - The Internet Protocol address of the currently contacted device.
- **Device Name** - The SNMP MIB-II SysName of the device (if it has been set at the device via management). The system administrator can use the SysName to identify the device via an ASCII text string (e.g., "Lab 2 9A426-02").

- **Device Location** - The SNMP MIB-II SysLocation of the device (if it has been set at the device via management). The system administrator can use the SysLocation to identify the device's physical location via an ASCII text string (e.g., "Wiring Closet 3").

Connection Data Fields

The following fields appear in the Connection Data portion of the Current Connections screen. Definitions are provided from IETF RFC 1695 Definitions of Managed Objects for ATM Management, Version 8.0.

- **Maximum Connections** - The maximum number of VCCs (PVCs and SVCs) supported at this ATM interface.

This is the number of concurrent Virtual Channel Connections (VCCs) that can be run on the device's LEC interface. A Virtual Channel Connection is a point-to-point data connection over the ATM network and must be established before data transfer can occur between two end stations, but can then be deconstructed as necessary.

If the connection is created "on the fly" when one end station initiates data communication to another, and is then deconstructed when that communication is finished, it is considered a Switched Virtual Circuit. SVCs are set up dynamically by the ATM UNI (User-to-Network Interface) signalling protocol.

If the connection is administratively established and deconstructed — so that two end stations have a sustained data route over the ATM network with an allotted amount of bandwidth — it is a Permanent Virtual Circuit. PVCs require extensive manual configuration, and are intended for use over a long period of time.

- **Currently Configured** - The number of VCCs (PVCs and SVCs) configured for use at the ATM interface.

Settings List

The following information is provided for each PVC and SVC Virtual Channel Connection currently established on the device.

- **Port** - The physical index (ifIndex) of the ATM interface on the device over which the PVC or SVC Virtual Channel Connection has been established. For the 9A126-02 module with default logical port configurations, this will be 7 for the first physical port and 23 for the second physical port.
- **VPI (Virtual Path Identifier)** - The VPI value of the VCL. The maximum VPI value cannot exceed the value allowed by the atmInterfaceMaxVpiBits.
- **VCI (Virtual Channel Identifier)** - The VCI value of the VCL. The maximum VCI value cannot exceed the value allowable by the atmInterfaceMaxVciBits.

A Virtual Channel Connection — the connection between two end stations over a switched ATM network — is composed of a series of one or more links between ATM switch devices, termed Virtual Channel Links (VCL).

A Virtual Path is a group of Virtual Channel Links that have the same end point. Virtual Paths can also be linked; a series of Virtual Path Links from end-point to end-point is termed a Virtual Path Connection.

As an analogy, consider the Virtual Path to be the regional area code in a telephony system, and the Virtual Channel to be the local exchange. This simplifies the routing of ATM cells, since each cell can be forwarded on a “Path” basis (the VPI) until the terminus of the connection, where the cell will be forwarded appropriately according to the specific channel identifier (the VCI).

Each data cell transported on an ATM network is identified by a Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI) combination in the cell header.

The maximum size of the VPI or VCI is determined by the type of ATM interface.

- If the interface is the User-to-Network Interface (or UNI) on a device — like the ATM port on the device — which provides the initial communication interface between the end user and the ATM network, the maximum size of the VPI is eight bits (identifying up to 256 paths — or physical destinations of other ATM devices), and the maximum size of the VCI is 16 bits (identifying up to 65,535 virtual circuits on each path).
- If the interface is the Network-to-Network Interface (or NNI) on an ATM switch device — such as a ForeRunner ATM Switch — acting as an intermediary along the communication path, the size of the VPI is increased to twelve bits (identifying up to 4,096 physical destinations, since it is assumed that the ATM network will be shared by multiple clients).

Encapsulation Type

An instance of this object only exists when the local VCL end-point is also the VCC end-point, and AAL5 is in use.

The type of data encapsulation used over the AAL5 SSCS layer. The definitions refer to RFC 1483 Multiprotocol Encapsulation over ATM AAL5 and to the ATM Forum LAN Emulation specification.”

Possible values are:

- vcMultiplexRoutedProtocol(1) (**VC MUX Routed**)
- vcMultiplexBridgedProtocol8023(2) (**VC MUX 802.3 Bridged**)
- vcMultiplexBridgedProtocol8025(3) (**VC MUX 802.5 Bridged**)
- vcMultiplexBridgedProtocol8026(4) (**VC MUX 802.6 Bridged**)
- vcMultiplexLANemulation8023(5) (**VC MUX 802.3 LANE**).
- vcMultiplexLANemulation8025(6) (**VC MUX 802.5 LANE**)
- llcEncapsulation(7) (**LLC Encapsulation**)
- multiprotocolFrameRelaySscs(8) (**Frame Relay SSCS**)
- other(9) (**Other**)
- unknown(10) (**Unknown**).

Because ATM is designed to link multiple traffic types (Voice, Video, and Data), an ATM device has software or firmware designed to properly sequence and error-check the conversion of each traffic type into and out of ATM cells; this software or firmware is termed the ATM Adaptation Layer (AAL). There are five types of AAL services: AAL1 is used for voice traffic; AAL2 for video; AAL3 and AAL4 for connection-oriented (e.g., TCP) and connectionless traffic, respectively; and AAL5 for Variable Bit Rate (VBR) connection-oriented and connectionless traffic. The ATM Forum LAN Emulation calls for AAL5.

When this Virtual Channel Link is the terminus of connection-oriented data communication (i.e., provides the UNI interface, as opposed to an NNI between switches), a method must be defined so that the data from the source network can be properly encapsulated into 53-byte ATM cells and then restored from ATM cells at the destination network back into the proper MAC-layer format. Each end of the Virtual Channel Connection must share the same encapsulation type (e.g., Ethernet data will be converted to ATM and back to native Ethernet, and so forth).

This field indicates the encapsulation method for each VCC supported by the ATM Access Module.

- **VC Type** - The type of the VCL. Values for this object are Permanent VC, incoming Switched VC, or outgoing Switched VC. This object cannot be modified once created.

pvc(1), -- Permanent VC; svcIncoming(2), -- Switched VC, incoming; svcOutgoing(3), -- Switched VC, outgoing”

This field indicates whether the Virtual Channel Link for each connection was administratively configured (a Permanent VC), initiated at the remote end of the connection for a destination station on a local segment connected to the device (incoming Switched), or initiated at the local end of the connection for a destination address on the remote end of the connection (outgoing Switched).

- **Oper. Status** - This object indicates the current operational status of the VCL. The up and down states indicate that the VCL is currently operational, or not operational, respectively. The unknown state indicates that the status of this VCL cannot be determined.

This field displays whether each Virtual Connection Link is currently up or down, or in some indeterminate state.

- **Up Time** - The value of MIB II's sysUpTime object at the time this VCL entered its current operational state. If the current state was entered prior to the last re-initialization of the agent, then this object contains a zero value.

This field indicates the system uptime set at the ATM Access Module's internal clock at the time that the VCL was initialized.

The uptime is incremented from zero at the start-up (or re-initialization) of the device. If the VCL was a Permanent Virtual Connection that was established prior to the last re-initialization of the device (and therefore stored in the device's NVRAM during shutdown), the UpTime will be returned as a 0.

Editing Current Connections Entries

You use the command buttons at the bottom of the Current Connections screen to add a new Permanent Virtual Circuit (PVC), modify an existing PVC, or delete or disable a PVC. Modifying, Deleting, and Disabling PVCs are beyond the scope of this guide.

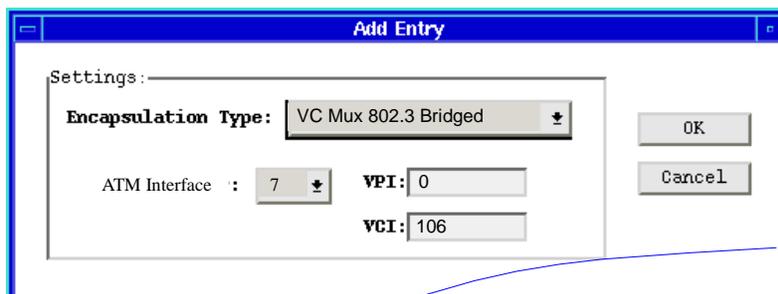
Adding a PVC

You use the Current Connections screen to set up a Permanent Virtual Circuit at the UNI interface of the ATM Access module, as well as to edit a previously configured PVC.

For the PVC to take effect, a corresponding entry must be made at the device at the succeeding link point (whether it is an end station or an interim ATM Switch along the link). For example, if you want to create a PVC between a 9A0000 ATM Switch and 9A426-02 ATM Access Module, you would have to define an equivalent entry at both devices (using the same VPI, VCI, and encapsulation type).

1. Select an ATM Interface from the ATM Interface drop-down list located in the upper right-hand corner of the Current Connections window (Figure 14-5). Select the interface appropriate for the ATM Access Module on which you are creating the PVC. For example, if creating a PVC on a 9A426-02, physical port 1, you would select ATM interface 7.
2. Click **Add** at the bottom of the Current Connections screen. The Add Entry screen is displayed (Figure 14-6).

Figure 14-6. Add Entry Screen



3. In the **VPI** field, type in the Virtual Path Identifier of the PVC (between 0 and 3). Specify the same VPI you specified when you configured the VCCs on your ATM switch.
4. In the **VCI** field, type in the Virtual Channel Identifier of the PVC. Specify the same VCI you specified when you configured the VCCs on your ATM switch.
5. Use the **Encapsulation Type** drop-down list to select **VC MUX 802.3 Bridged**.
6. Use the **ATM Interface** drop-down list button to select the ATM interface at which the PVC will take effect. The ATM Interface you selected on the Current Connections window is automatically displayed.
7. Click **OK** to create the entry.

Using AMI to Create VCCs

The switch software provides switch and connection management, IP connectivity, and SNMP network management. The Switch Control Software (SCS) is the “brains” of the switch. The user interface to the SCS is called the ATM Management Interface (AMI). This section describes how to configure a VCC into Cabletron’s 9A000 ATM switch. For comprehensive information about using AMI, refer to Cabletron’s *ATM Switch Configuration Manual*.

To configure a VCC into Cabletron’s 9A000 ATM switch:

1. Connect your console to the chassis’s communications port or telnet to the module. Log into the module. At the login prompt, type **asx**. Type in the password if one has been assigned. A display similar to the following is displayed and an AMI session is opened.

ATM Management Interface v1.2

Copyright 9c) 1994, 1995 FORE Systems, Inc.

All Rights Reserved

General Commands:

‘?’ to get a list of commands at the current level

‘up’ to go up one menu

‘top’ to go to the root menu

‘exit’ to leave AMI

Opening a session for “127.0.0.1”, please wait. . .

Connected to “127.0.0.1” (9A000)

localhost: :>



If another user already has an AMI session open, you will not be permitted to log in.

2. Create a VCC by typing the following command at the prompt:

```
con vcc new <iport><ivpi><ivci><oport><ovpi><ovci>
```

where:

iport indicates the incoming port number

ivpi indicates the incoming virtual path

ivci indicates the incoming virtual channel

oport indicates the outgoing port number

ovpi indicates the outgoing virtual path

ovci indicates the outgoing virtual channel

For example, **con vcc new 1D1 0 106 1D2 0 106**.

Since all ATM switch PVCs must to be bi-directional, you must configure another VCC in the reverse direction, for example, **con vcc new 1D2 0 106 1D1 0 106**.

3. Display the VCCs you created by typing the following command at the prompt:

```
con vcc sh
```

A display similar to the one shown below will be displayed.

```
Input   Output
Port VPI VCIPortVPIVCIUProtocolName
1D10   1061D201060pvcn/a
1D20   1061D101060pvcn/a
```

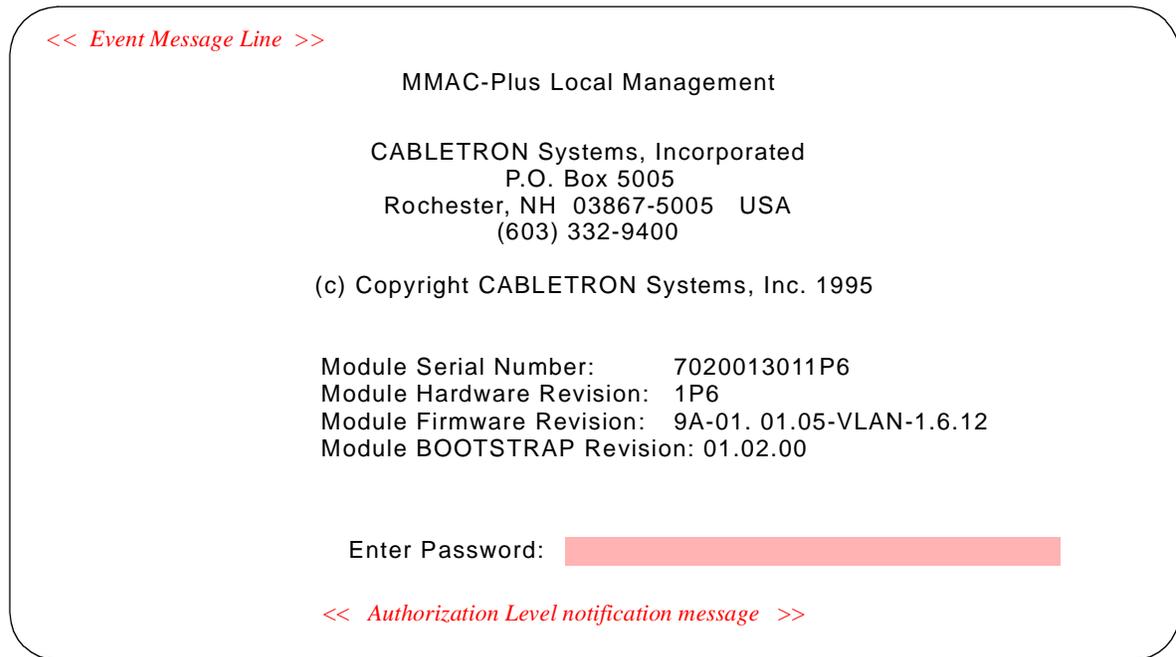
4. Exit AMI by typing **exit** at the prompt.

Using Local Management to Create PVCs

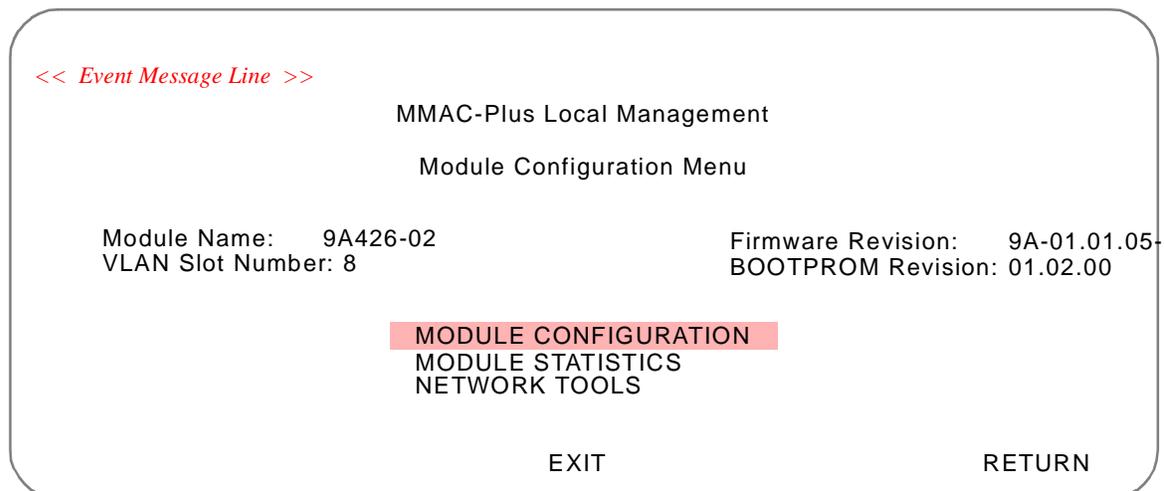
This section describes how to program a PVC into Cabletron's 9A426-02 ATM Access Module. For comprehensive information using local management, refer to the documentation that was provided with the module.

To program a PVC into Cabletron's 9A426-02 ATM Access Module:

1. Connect your console to the chassis's communications port or telnet to the module. A display similar to the following is displayed.



2. Enter the module's password in the **Enter Password** field. A display similar to the following is displayed.



3. Select **MODULE CONFIGURATION**. A display similar to the following is displayed.

```
<< Event Message Line >>

MMAC-Plus Local Management
Module Configuration Menu

Module Name: 9A426-02          Firmware Revision: 9A-01.01.05
VLAN Slot Number: 8          BOOTPROM Revision: 01.02.00

GENERAL CONFIGURATION
SNMP COMMUNITY NAMES
SNMP TRAPS
FDDI CONFIGURATION
MODULE SPECIFIC CONFIGURATION

EXIT                               RETURN
```

4. Select **MODULE SPECIFIC CONFIGURATION**. A display similar to the following is displayed.

```
<< Event Message Line >>

MMAC-Plus Local Management
ATM Screens

Module Name: 9A426-02          Firmware Revision: 9A-01.01.05
VLAN Slot Number: 8          BOOTPROM Revision: 01.02.00

ATM Connection Screens
LAN Emulation Clients
Signalling
ATM Diagnostics
Discovery ELAN Setup

EXIT                               RETURN
```

5. Select **ATM Connection Screens**. A display similar to the following is displayed.

```

<< Event Message Line >>

MMAC-Plus Local Management
    ATM Connection Screens

Module Name: 9A426-02          Firmware Revision: 9A-01.01.05
VLAN Slot Number: 8          BOOTPROM Revision: 01.02.00

    Connection Table
    Connections By Virtual Interface

EXIT [ ] RETURN
    
```

6. Select **Connection Table**. A display similar to the following is displayed.

```

<< Event Message Line >>

MMAC-Plus Local Management
    9A426-02 Connection Table

Module Name: 9A426-02          Firmware Revision: 9A-01.01.05
VLAN Slot Number: 8          BOOTPROM Revision: 01.02.00

ATM Port Current Connections: 2

    IF  Port  VPI  VCI  Encapsulation Type  Status  ATM Address (ESI)
    7   100   0    0005 Other              Enabled
    7   100   0    0006 Other              Enabled

    ADD/DELETE  PORT #: [1]  EXIT  RETURN
    
```

7. Select **ADD/DELETE**. A display similar to the following is displayed.

```
<< Event Message Line >>

MMAC-Plus Local Management
9A426-02 Add/Delete Entry

Module Name: 9A426-02          Firmware Revision: 9A-01.01.05
VLAN Slot Number: 8           BOOTPROM Revision: 01.02.00

ATM Port Current Connections: 2

      VPI   VCI   AAL Type  Encapsulation Type
      0     0005  5         Other

ADD/MODIFY                      EXIT                      RETURN
```

8. Navigate to **VPI** and then enter the VPI of the PVC you want to create. Tab over to **VCI** and then enter the VCI of the PVC you want to create. Press **Return**. Navigate to **ADD/MODIFY**. Press **Return** to create the PVC.
9. Navigate to **EXIT** and then press **Return** to terminate the local management session.

Managing VLANs Over ATM Networks Using Switched Virtual Circuits

You can manage VLANs across ATM networks using Switched Virtual Circuits (SVCs). This feature ensures any-to-any connectivity between endpoints attached to SecureFast switches, connectivity of endpoints behind SecureFast switches, and ATM-attached endpoints.

SecureFast switches in a VLAN domain that manage SVCs are collectively called an SVC mesh. An SVC mesh can contain up to 23 switches. The switches in a mesh are called ATM Access Modules. In addition to performing all SecureFast switching functions, an ATM Access Module can interface with an ATM network through the use of LECs.

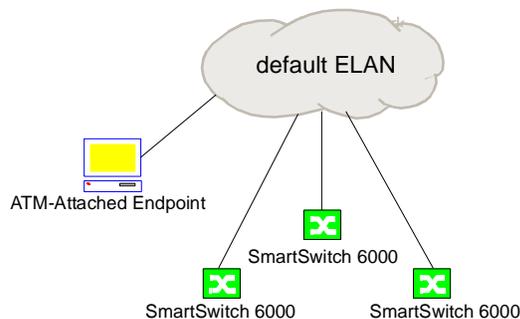
Additional switch meshes can be configured to accommodate future expansion of your network. Refer to *Network Scalability*, on page 14-25 for information about extending your SVC mesh beyond the 23 switch limitation.

Initialization and Configuration

Upon initialization, the LECs in a SecureFast SVC mesh join a ‘discovery’ ELAN automatically by discovering the LAN Emulation Configuration Server (LECS) through the Integrated Layer Management Interface (ILMI) or on the well known address or well known VC. The LECS assigns ELAN membership and other key information to the LEC. For the purposes of this document, the ‘discovery’ ELAN to which LECs are automatically joined is the ‘default’ ELAN, the first ELAN created, however, you can configure any ELAN to be the ‘discovery’ ELAN. Once all LECs have joined the ‘discovery’ ELAN, the SecureFast LECs discover each other. ATM-attached endpoints must also join the ‘discovery’ ELAN. Refer to *ATM-Attached Endpoints*, on page 14-20.

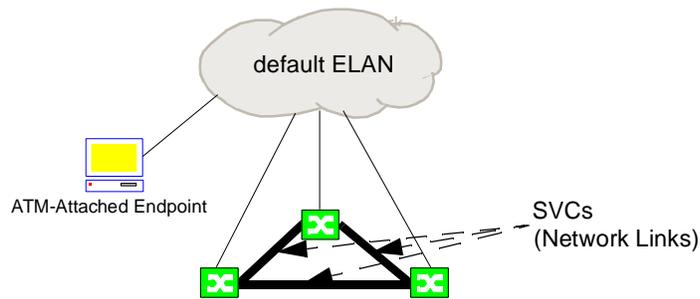
Figure 14-7 shows three SecureFast switches and one ATM-attached endpoint have joined the discovery ELAN.

Figure 14-7. SecureFast LECs and ATM-attached Endpoints Join ‘discovery’ ELAN



When a SecureFast switch receives a discovery packet from another SecureFast switch, it uses UNI signaling to establish a connection known as a Switched Virtual Circuit (SVC) back to the originator. In this way, a full mesh of data direct SVCs is automatically created between all the SecureFast LECs in the network (Figure 14-8).

Figure 14-8. SVCs Between SecureFast LECs



Once established, the SVCs become SecureFast network links.



It is possible to manually create network links between SecureFast switches by administratively configuring Permanent Virtual Circuits (PVCs). It is not necessary to disable LANE nor the discovery mechanism in order to set up PVCs. Refer to *Managing VLANs Over ATM Networks Using Permanent Virtual Circuits*, on page 14-2, or information about setting up PVCs.

The ‘discovery’ ELAN is used to establish the SVC mesh. It does not perform call processing. Call processing is done over the network links.

Topology information and SecureFast protocols are exchanged across the network links. SecureFast switches transmit Switch Hello Packets over the network links to discover adjacent switches and to determine whether each interface is a ‘network’ or ‘access’ port. They use the SecureFast Resolve protocol to resolve MAC addresses to switches and to support user mobility. They also use the VLAN flood protocol to encapsulate broadcast/unknown traffic and forward it over the network links and throughout the SecureFast domain.

ATM network links are treated in the same manner as SecureFast links would be in a LAN environment. As such, traffic from multiple VLANs can be trunked across the ATM SVC mesh. Load sharing over links of equal bandwidth is allowed between SecureFast ATM devices, as is the configuration of parallel LAN connections. Additionally, SPECTRUM VLAN Manager can provide full network visibility and control over all of the VLANs in the domain.

SecureFast LECs use the discovery protocol to continually listen on the ‘discovery’ ELAN for new SecureFast LECs. When a new LEC is discovered, it is automatically added to the SVC mesh.

Once the mesh of SVCs is created, the links no longer use the ‘discovery’ ELAN unless there is a change in the domain’s switch fabric.

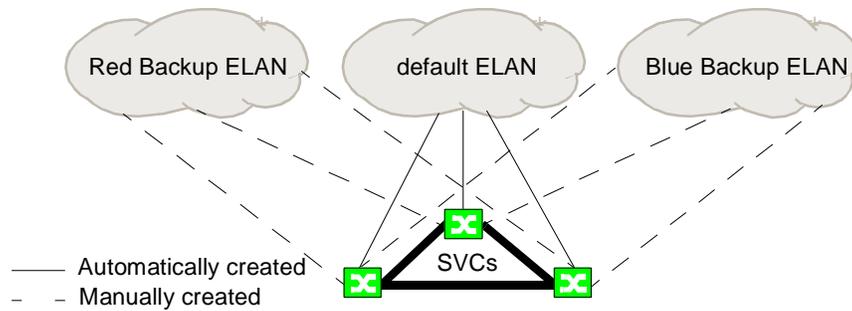
Backup ELANs

To provide fault tolerance to your SVC mesh, you can create multiple ELANs and activate multiple LECs on each of the switches in an SVC mesh. With the discovery protocol enabled, each LEC on every switch can be configured to join one of the backup ELANs (Figure 14-9).



A LEC on each switch in an SVC mesh must join the backup ELAN and be enabled, using the switch’s local management tool. For information about creating backup ELANs, refer to *Configure ELANs/LECs*, on page 14-22.

Figure 14-9. Backup ELANs

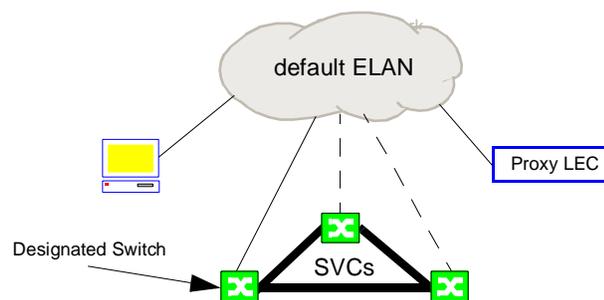


This ensures that new SecureFast LECs will be discovered. It also ensures fault tolerance for the SVC mesh if the ‘discovery’ ELAN fails. Should a failure occur, an SVC mesh will result via a backup LEC.

ATM-Attached Endpoints

ATM-attached endpoints must also join the ‘discovery’ ELAN in order for connections between those endpoints and connections to endpoints within the SecureFast domain to be set up. Once ATM-attached endpoints have joined the ‘discovery’ ELAN and SecureFast switch LECs have been configured to operate in ‘topology.ra’ mode, an election protocol establishes a designated switch for ATM-attached endpoint connectivity. This feature is known as ‘redundant access’. The designated switch is responsible for transmission of endpoint data to all non-SecureFast ATM attached devices, while the redundant switches stand by to ensure endpoint connectivity (Figure 14-10).

Figure 14-10. ATM Attached Endpoints



Each ATM attached device on the ‘discovery’ ELAN can be assigned independently either to an existing VLAN or a new VLAN. This means that multiple VLANs can use the same ELAN. In other words, an ATM-attached endpoint on the ‘discovery’ ELAN could be assigned to an open MAC-based VLAN that includes LAN endpoints connected to one or more switches. At the same time, a generic proxy LEC could also be a member of the ‘discovery’ ELAN but could be assigned to its own secure port-based VLAN. The election protocol provides fault tolerance for connectivity to ATM attached devices in much the same way as the Spanning Tree protocol does for traditional LANs. If the designated switch or its ATM uplink fails, the remaining switches automatically elect a new designated switch. Endpoint traffic is rerouted through the ATM link of the new designated switch.

Using SVCs to Manage VLANs Over ATM Networks

Before you can use SVCs to manage your VLANs over an ATM network, you must:

- Install and configure your hardware (e.g., install hardware, install firmware, install cabling, and configure hardware). Note that each SVC mesh can contain up to 23 switches. Additional meshes can be configured to achieve network scalability or to enhance scalability, uplinks can be applied to the SVC mesh core.
- Install and configure LANE services.

- Create an ELAN(s). You must create at least one ELAN, the ‘discovery’ ELAN. You can create additional ELANs to support fault tolerance and/or network scalability. Refer to *Configure ELANs/LECs*, on page 14-22 for more information about creating additional ELANs.
- Run Discovery. Refer to *Run Discovery*, on page 14-23.

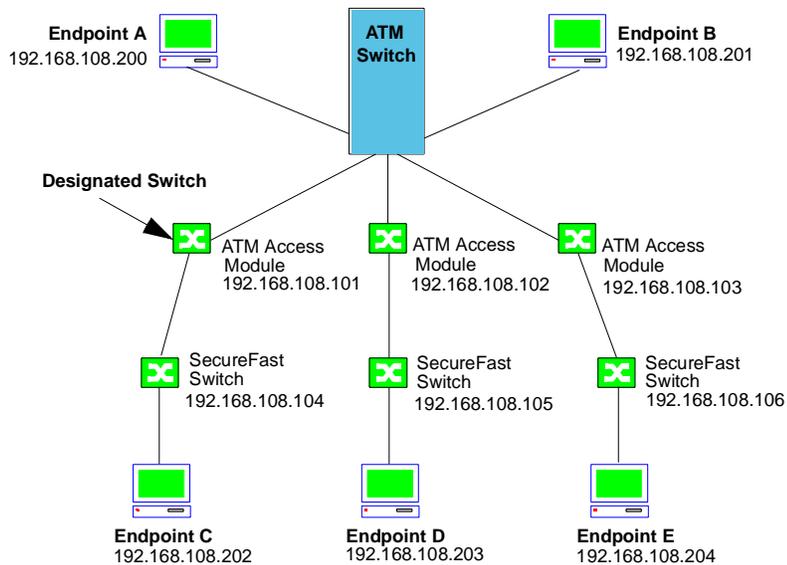


This section presumes that you have installed and configured your hardware, installed firmware, and installed LANE services.

Sample SVC Network

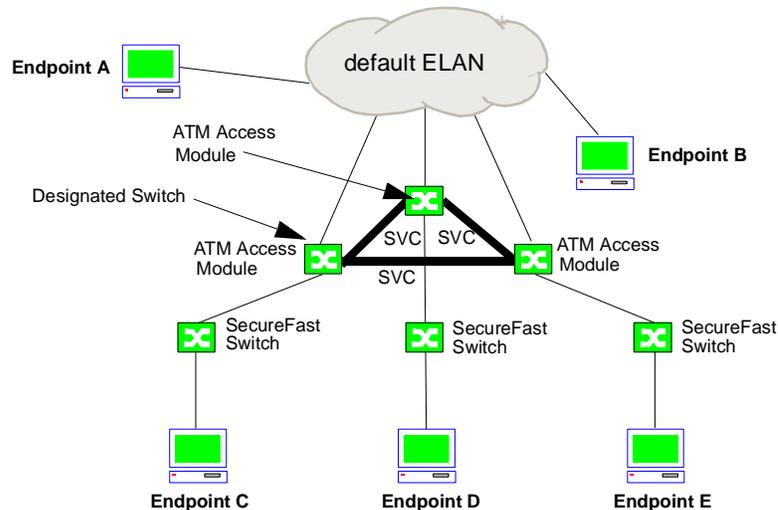
The sample network in Figure 14-11 consists of an ATM switch running LANE services. Two endpoints are directly attached to the ATM switch. Three ATM access modules (each in a separate chassis) are also connected to the ATM switch. A single SecureFast switch is connected to each ATM interface. A single endpoint is connected to each SecureFast switch.

Figure 14-11. SVC Sample Network



The logical view of this sample network would appear as shown in Figure 14-12:

Figure 14-12. Sample SVC Network Logical View



Configure ELANs/LECs

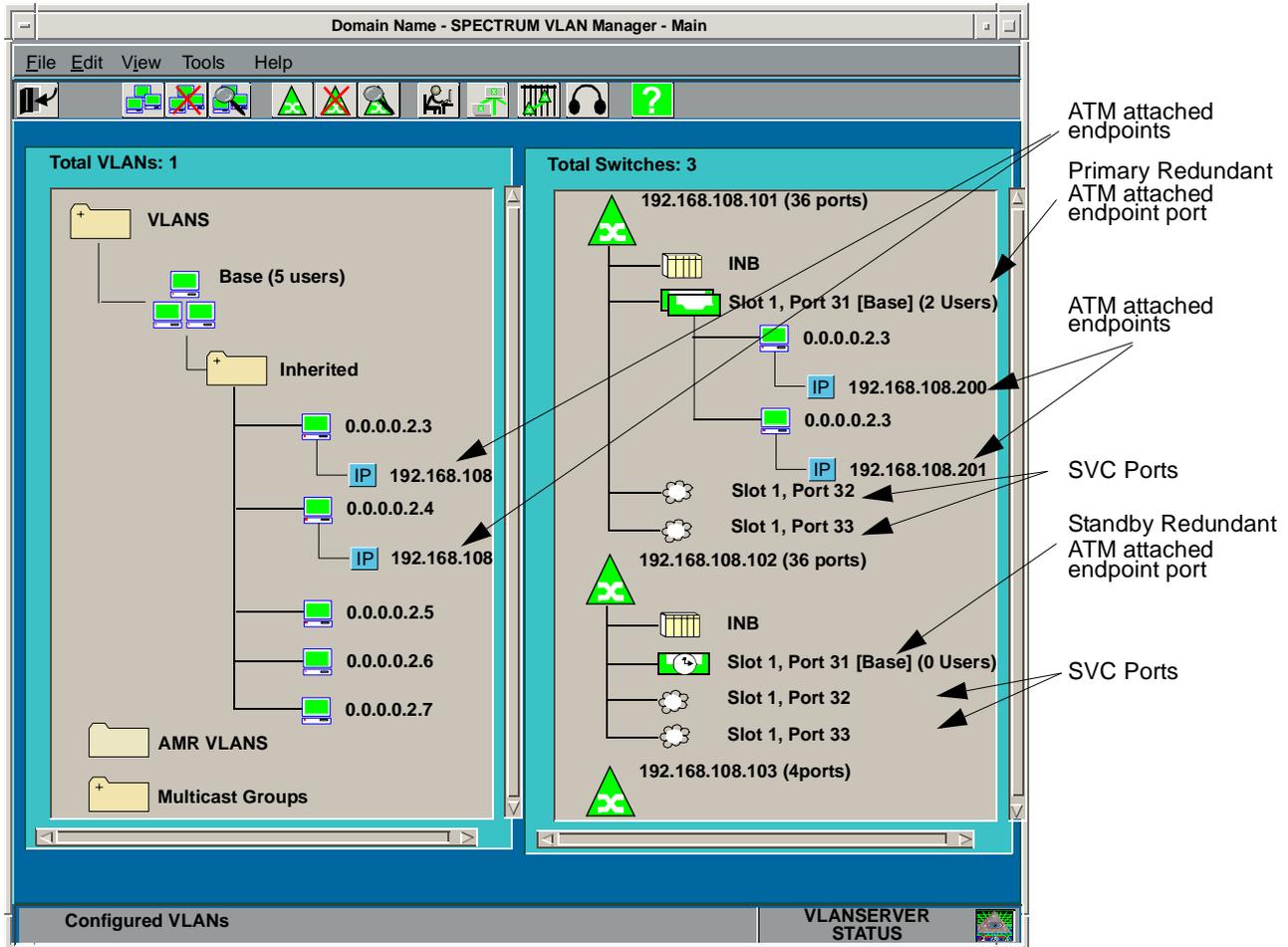
1. Create the 'default' ELAN. This is the 'discovery' ELAN and is used to discover other SecureFast switches in a domain, set up the SVC mesh, and manage ATM-attached endpoints. Use the LANE Services tool that was provided with your ATM switch (Refer to Chapter 3 in the ATM Switch Configuration Manual for the 9A000 ATM switch module).
2. Configure a LEC on each SecureFast ATM Access Module to join the 'discovery' ELAN. Use the switch's local management to create the LEC, then use the switch's local management or the Discovery ELAN Configuration tool to join the LEC to the 'discovery' ELAN.
3. Configure each ATM-attached endpoint to join the 'discovery' ELAN.
4. Configure SecureFast LEC to operate using the 'topology.ra' agent. Use the switch's local management or the Topology Port Manager. For example, to configure a LEC to operate use the 'topology.ra' agent using the switch's local management:
 - a. Start the switch's local management.
 - b. Select 'Network Tools'.
 - c. Type 'tpmgr list' to show the Topology Port Table for the switch.

- d. Use the Topology Port Table displayed in Step c to determine which logical port (LEC) you want to set to use the 'topology.ra' agent.
- e. Type 'tpmgr add <x> topology.ra' where x is the Logical Port (LEC) you want to set.

Run Discovery

If discovery were run on the sample network, the Main VLAN Manager window will look something like the window shown in Figure 14-13. For clarity, switch 192.168.108.106 and some ports are not shown.

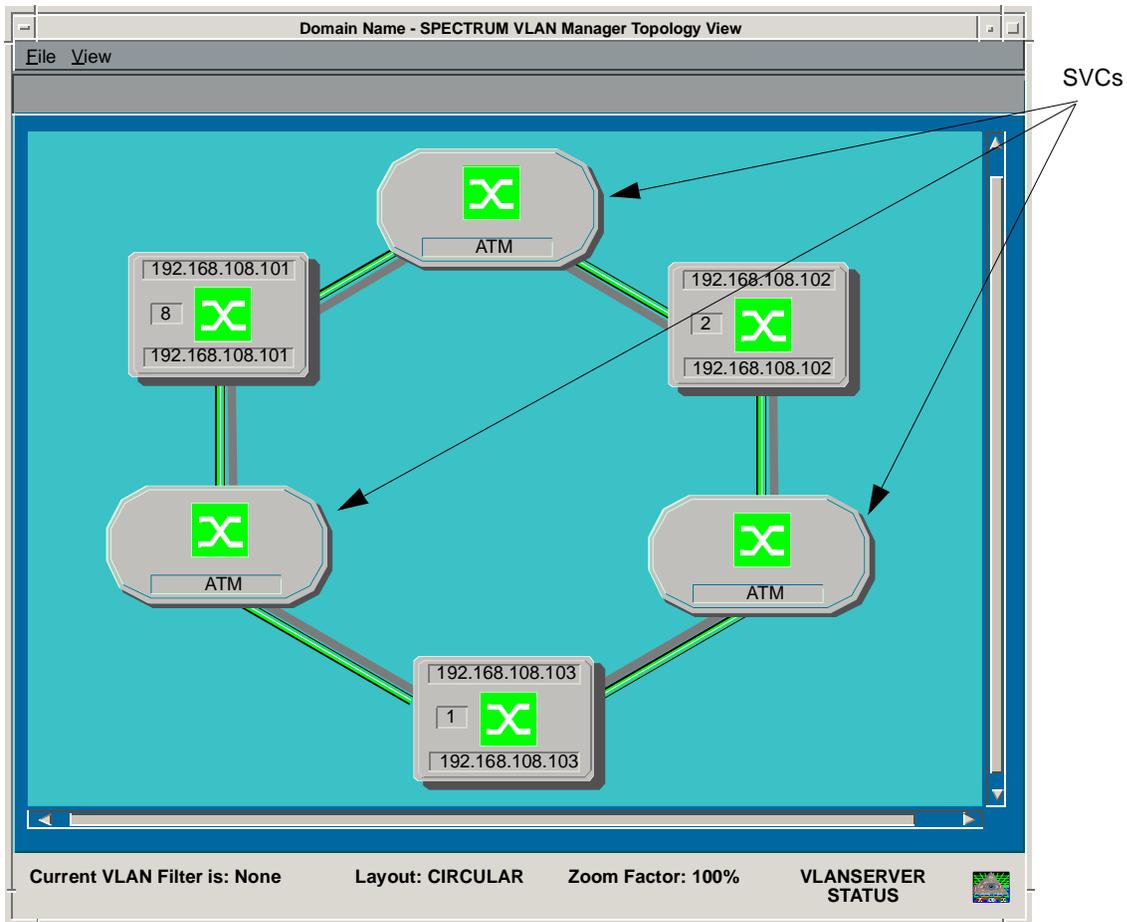
Figure 14-13. Sample Network VLAN Manager Main Window



Switch 192.168.108.101 has been designated as the primary switch. As such, it is responsible for all communication to ATM attached endpoints. If the switch or the link to the switch fails, one of the standby switches will become the primary switch. When the failure associated with the original primary switch is resolved, the original switch will resume as the primary switch. This example shows the default VLAN. Additional VLANs can be created and managed in the same way as non-ATM VLANs.

The Topology view for our sample network is shown in [Figure 14-14](#).

Figure 14-14. Sample Network Topology View



Network Scalability

To aid in network scalability, several configuration options are available. Two options demonstrate how to extend the SecureFast domain by conserving LECs and inter-switch network links. A third option shows how to interconnect multiple SecureFast domains with an ATM attached router and a fourth option shows how to extend the SecureFast domain using uplink switching.

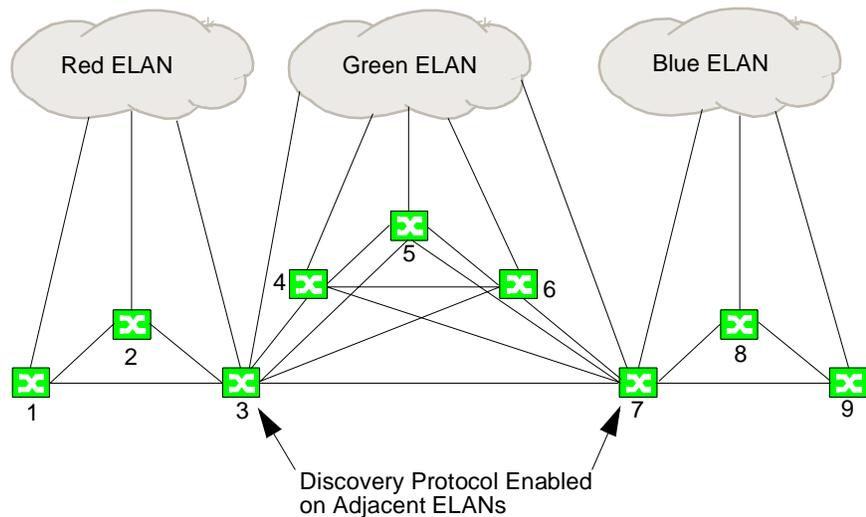
Refer to the firmware SRN applicable to the SecureFast switches in your network for information about limitations.

Option 1

Scalability of a SecureFast ATM network can best be achieved by reducing the number of inter-switch links. One way to do this is to create multiple ELANs on which discovery will occur. Then manually assign a single SecureFast LEC on each of the SecureFast switches to one of the available ELANs. For best results, each ELAN should support about the same number of switches.

On the logical borders of each ELAN, select one or two switches as border switches. These border switches host multiple SecureFast LECs, and each of these LECs is assigned to one of the adjacent ELANs (Figure 14-15).

Figure 14-15. Scalability Option 1



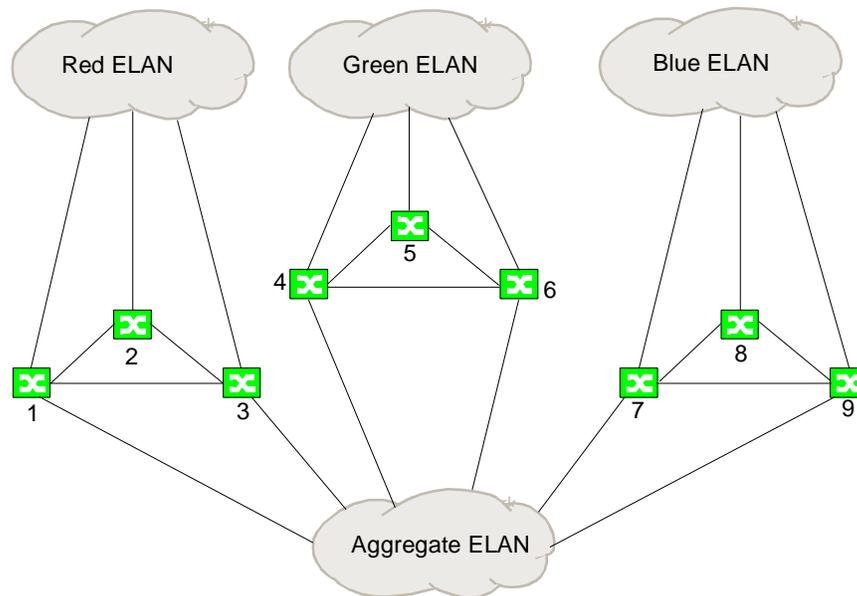
In Figure 14-15 SecureFast switches 3 and 7 are border switches. Both have membership in, and have enabled discovery on two ELANs. Now, instead of one large mesh consisting of 36 SVCs, three interconnected meshes consisting of a total of 16 SVCs are established.

With this scalability method implemented, the SecureFast network functions as before. The only difference is that in large networks like this traffic on the network links may take an additional switch hop or two. It is legal to configure multiple border switches for fault tolerance, but this lessens the reduction of inter-switch links. Another way to improve fault tolerance while limiting the number of inter-switch links is to manually create a backup PVC between SecureFast switches that are members of separate ELANs but are not configured as border switches. For example, one PVC could be created between switches 2 and 4 and another between switches 6 and 8. This would ensure connectivity within the domain even if one or more of the border switches failed.

Option 2

An alternative scalability option is to interconnect ELANs with an aggregate ELAN (Figure 14-16).

Figure 14-16. Scalability Option 2



With this option, multiple ELANs are created and then a single SecureFast LEC on each SecureFast switch is manually assigned to one of the available ELANs. On the logical borders of each ELAN, one or two SecureFast switches are selected as border switches.

These border switches host multiple SecureFast LECs and one of the remaining LECs is assigned to another ELAN, which is referred to as the aggregate ELAN.

The aggregate ELAN is used to establish a full mesh of SVCs only between the SecureFast LECs that have joined it.

Figure 14-16 shows that two SecureFast switches from each ELAN are border switches and as such have joined the aggregate ELAN. Configuring redundant border switches in this way provides greater fault tolerance but also lessens the opportunity for the reduction of inter-switch links.

In this scenario, the three meshes of three SVCs each, which were created by the three ELANs, are interconnected by another mesh of 15 SVCs that were created by the aggregate ELAN. A total of 24 inter-switch network links are used instead of the 36 that would have been used with a single SVC mesh created by a single ELAN. If redundant border switches had not been configured, then only 15 network links would have been used. PVCs between non-border switches on the different ELANs could also be used to provide fault tolerance while further reducing the number of network links.

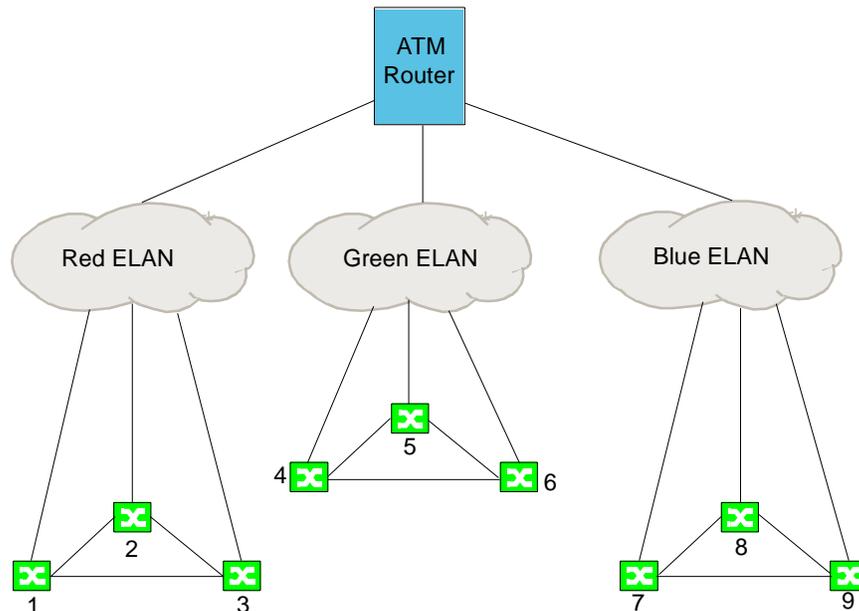
This method also functions just like a typical SecureFast network. The only difference is that traffic on the network links may take an additional switch hop.

Option 3

This option (Figure 14-17) involves segmenting the SecureFast network into multiple domains. This is accomplished by creating subnets. All of the endpoints that are to be part of the same SecureFast domain are assigned to the same layer 3 subnet address. Likewise, endpoints in different domains are assigned to different subnets.

Within the domain, all SecureFast capabilities are available and most everything functions as described in Options 1 and 2, in fact the two previous methods can be implemented within this option. Communication across the domains is accomplished through a router with proxy arp enabled.

Figure 14-17. Scalability Option 3



One design constraint prevents generic non-SecureFast proxy LECs and directly attached ATM endpoints from being members of the same ELAN as an ATM attached router. Those devices can be contained within a SecureFast domain which also includes a router, but they must be assigned to one or more ELANs that exclude the router as a member. The router's ELAN will be assigned as a SecureFast router port.

Option 4

This option consists of a set of SFS-ATM access devices forming an SVC mesh. Each device has a number of uplink chassis connected to it.

Creating Additional ELANs

As discussed earlier in this chapter, there are two reasons why you may create ELANs other than the 'discovery' ELAN, for fault tolerance (*Backup ELANs*, on page 14-19) and for network scalability (*Network Scalability*, on page 14-25).

In any case, creating an ELAN is a two step process.

- You create the ELAN using the LANE services tool that came with your ATM switch or the ATM PVC tool available from the VLAN Manager's **Tools** menu.

- You create and configure a LEC from each switch in the domain to join the newly created ELAN using the switch's local management tool.

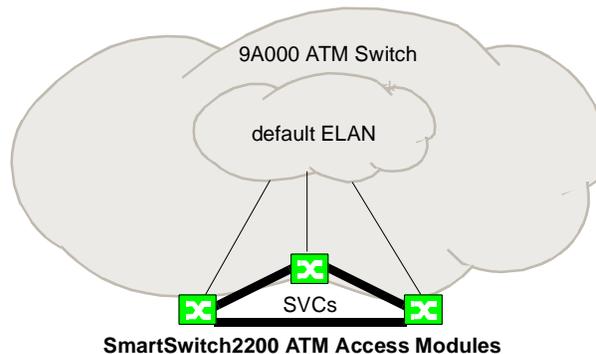
The following section shows by example how you would create an additional ELAN for use in providing fault tolerance for your SVCs. The procedure used to create an ELAN for the purposes of expanding your SVC mesh beyond the 23 switch limit would be the same.

Example

You decide to add fault tolerance to your SVC mesh by adding a backup ELAN. Our sample network for this example is comprised of an ATM network. In this case, a single 9A000 ATM switch on which the 'default' ELAN has been created using LANE Services and three switches (SmartSwitch2200 ATM access modules).

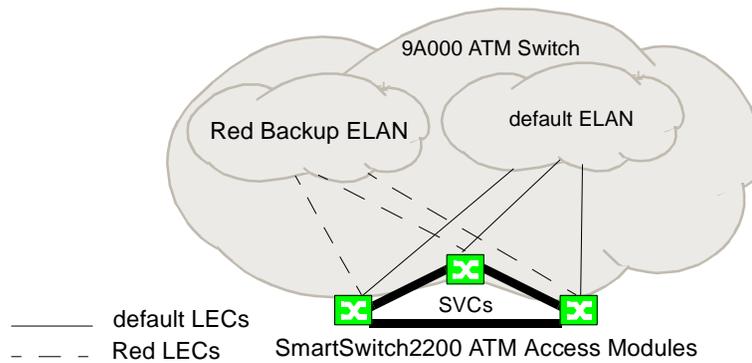
The original configuration of this network might look something like the one shown in [Figure 14-18](#). In this configuration, the switches in the mesh have each joined a LEC, the 'default' ELAN. The SVCs that are created are managed by the "default" ELAN. If the "default" ELAN fails, connections across the ATM network will not be broken; however, without the 'default' ELAN, however new LECs could no longer join the mesh and existing LECs could not move between the ATM switches in the network.

Figure 14-18. Original Configuration



After you created and configured the backup ELAN, the configuration would look something like the one shown in [Figure 14-19](#). The SVCs are still managed by the 'default' ELAN; however, if the 'default' ELAN fails, the 'Red' ELAN takes over SVC management. In this case, connections across the ATM network will not be broken, new LECs could join the mesh, and existing LECs could move between the ATM switches in the network.

Figure 14-19. Backup Configuration



To get to this configuration, you would first create the 'Red' ELAN on the 9A000 ATM switch and then join and enable a LEC from each of the three SmartSwitch2200 ATM access modules to the 'Red' ELAN. Both steps can be performed using the respective switch's local management tool.

Figure 14-20 shows a sample of the Discovery ELAN Setup screen for the SmartSwitch2200. In this sample, notice that the first LEC (Index 1) is enabled but an Elan Name is not specified. This is because the first instance of a LEC does an automatic unspecified join. The LEC doesn't look for an ELAN with a particular name but rather joins the first ELAN it finds. In most cases this is the 'default' ELAN. You can fill in the name of the ELAN by moving the cursor to the Elan Name field for that LEC and typing the name of the ELAN that the LEC joined.

The second LEC has joined the Red ELAN and is enabled. This was done by moving the cursor to the Elan Name field for the second LEC (Index 2), and typing in the name of the ELAN (Red), and then moving to the Status field for that LEC and toggling the status to Enabled.

In this example, the Mode for all LECs is Master. Also, note that you have to select SAVE before your configuration changes are saved.

Figure 14-20. Discovery ELAN Setup Screen

2E42-27 Local Management

Interface 27 Discovery Elan Setup

Device Type: 2E42-27 Firmware Revision: 04.00.03
 BOOTPROM Revision: 01.00.03

Index	Elan Name	Mode	Status
1		[Master]	[Enabled]
2	Red	[Master]	[Enabled]
3		[Master]	[Disabled]
4		[Master]	[Disabled]
5		[Master]	[Disabled]
6		[Master]	[Disabled]
7		[Master]	[Disabled]
8		[Master]	[Disabled]

SAVE NEXT EXIT RETURN

Discovery ELAN Configuration

Overview

Normally, SecureFast LECs join the 'default' ELAN, the first ELAN created, as the 'discovery' ELAN. You can change the 'discovery' ELAN to be any ELAN configured, by editing Discovery ELAN Configuration using the ATM Access Module's local management tool or by using the Discovery ELAN Configuration tool. In addition to changing the 'discovery' ELAN, you can change the Master/Slave status of an ELAN and change the Enabled/Disabled status of an ELAN.

This section describes using the Discovery ELAN Configuration tool to edit the Discovery ELAN Configuration. To edit the Discovery ELAN Configuration using an access module's local management tool, refer to the User's Guide for the HSIM (High Speed Interface Module) installed in your access module.

Using the VLAN Manager to Edit the Discovery ELAN

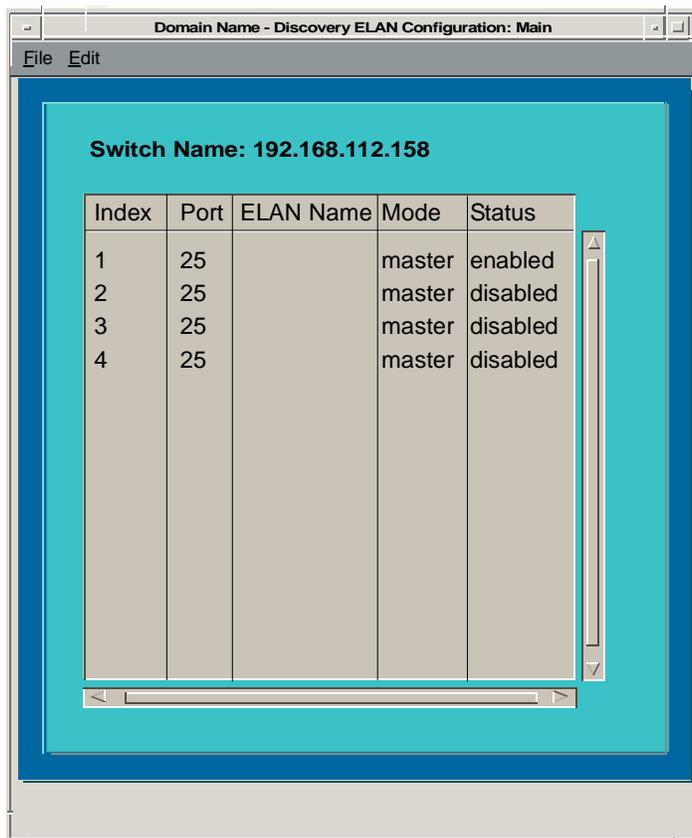
You can change the name and the status of the ‘discovery’ ELAN using the VLAN Manager’s Discovery ELAN Configuration tool. To display the Discovery ELAN Configuration Main window (Figure 14-21), choose **Discovery ELAN Configuration** from VLAN Manager’s **Tools** menu. The window consists of the **File** and **Edit** menus and the Switch Name, Index, Port, ELAN name, Mode and Status fields. Each menu and field is described in the following sections.



If the ‘default’ ELAN is being used as the ‘discovery’ ELAN, the Discovery ELAN Configuration window’s ELAN Name field will be blank, however, SecureFast LECs will still automatically join the ELAN. You can force the ELAN Name to be displayed by performing the following steps in order:

1. Use the ATM PVC tool’s ELAN Administration window to change the name of the ELAN to match the ‘default’ ELAN’s name.
2. Change the Discovery ELAN name to match the ‘default’ ELAN’s name using the switch’s Local Management or the ELAN Discovery Configuration tool.

Figure 14-21. Discovery ELAN Configuration



Discovery ELAN Configuration Menus

File Menu

The **F**ile menu consists of the following commands: **P**references and **E**xit.

- **P**references - Lets you define Global, Main, Topology view, Path Trace, and Connection Table settings for VLAN Manager. Refer to [Chapter 5, Managing Preferences](#), for information about how to set preferences.
- **E**xit - Displays the Exit Discovery ELAN Configuration confirmation box. Click **OK** to exit Discovery ELAN Configuration or **Cancel** to return to the Discovery ELAN Configuration main window.

Edit Menu

The **E**dit menu consists of the following commands: **E**dit ELAN Name, **T**oggle **M**aster/Slave, and **T**oggle **E**nable/Disable.

- **E**dit ELAN Name - Lets you change the name assigned to an ELAN.
- **T**oggle **M**aster/Slave - Lets you toggle between Master and Slave modes.
- **T**oggle **E**nable/Disable - Lets you toggle between Enable and Disable status.

Discovery ELAN Configuration Fields

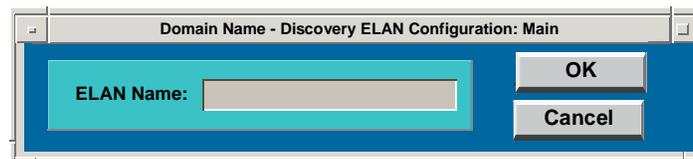
- **Switch Name** - Switch for which discovery ELAN configuration information is being displayed.
- **Index** - (Read-only) Displays the number assigned to this ELAN. The number of discovery ELANs that can be assigned to an HSIM varies. Refer to the documentation that came with your HSIM.
- **Port** - Physical interface to which the HSIM is connected to the ATM network.
- **ELAN Name** - (Modifiable) Name of the discovery ELAN that the HSIM will join when the Discovery ELAN becomes enabled.
- **Mode** - (Toggle) Changes the operational mode of an HSIM. When in 'Master' mode, the HSIM will accept connections from all other HSIMs in the Discovery ELAN to which it belongs. When in 'Slave' mode, the HSIM will only accept connections from other HSIMs configured to be in 'Master' mode.
- **Status** - (Toggle) Changes the operational status of an HSIM. When 'Enabled', the HSIM will join the specified discovery ELAN. When 'Disabled', the HSIM will disconnect from the specified discovery ELAN.

Editing a Discovery ELAN Name

To edit the name of a discovery ELAN:

1. Select an ATM access module (switch) from the physical pane of VLAN Manager's Main window.
2. Select **Discovery ELAN Configuration** from the **Tools** menu to display the Discovery ELAN Configuration window.
3. Click anywhere in the entry that contains the ELAN name you want to edit and then select **Edit ELAN Name** from the **Edit** menu to display the Discovery ELAN Configuration: Edit ELAN Name dialog box.

Figure 14-22. Editing An ELAN Name



4. Enter the new name of the selected ELAN into the ELAN Name text box and then click **OK** to change the name or **Cancel** to dismiss the Edit ELAN Name dialog box without changing the name.

Changing the Operational Mode of an HSIM

To change the operational mode of an HSIM:

1. Select an ATM access module (switch) from the physical pane of VLAN Manager's Main window.
2. Select **Discovery ELAN Configuration** from the **Tools** menu to display the Discovery ELAN Configuration window.
3. Click anywhere in the entry that contains the ELAN for which you want to change the operational mode then select **Toggle Master/Slave** from the **Edit** menu. The mode for the selected ELAN toggles between 'Master' and 'Slave' each time you choose **Toggle Master/Slave**.

Changing the Operational Status of an HSI

To change the operational status of an HSI:

1. Select an ATM access module (switch) from the physical pane of VLAN Manager's Main window.
2. Select **Discovery ELAN Configuration** from the **Tools** menu to display the Discovery ELAN Configuration window.
3. Click anywhere in the entry that contains the ELAN for which you want to change the operational mode and then select **Toggle Enabled/Disabled** from the **Edit** menu. The mode for the selected ELAN toggles between 'Enabled' and 'Disabled' each time you choose **Toggle Enabled/Disabled**.

Advanced VLAN Policy

This chapter provides an overview of SPECTRUM VLAN Manager's Advanced VLAN Policy application and information required to launch and use the application.

Overview

Advanced VLAN Policy lets you control VLAN policy in ways not possible using basic VLAN Manager policy.

Basic VLAN Manager policy limits the number of VLANs a shared resource such as a DHCP server or general file server can be a member of to eight. If a shared resource needs to be a member of more than eight VLANs, a second router interface may solve this problem depending on the router. Advanced VLAN Policy provides a solution to this eight VLAN limit limitation without having to use additional router interfaces. Refer to the example on page 15-16.

Basic VLAN policy establishes a VLAN's relationship to all other VLANs in a domain. If a VLAN is configured as 'Secure', members of that VLAN can only communicate with other members of that same VLAN. Communication between secure VLANs is not possible without the use of a router if a secure policy exists. Advanced VLAN Policy allows you to control connect and flood policy on a VLAN pair basis.

Basic VLAN policy requires that you map additional VLAN memberships to any group that you want to connect to another secure group. For instance, there may be a group of users to which you would like to restrict access, but allow perhaps one or two other groups to connect to that secure group. Using Advanced VLAN Policy, all groups retain their VLAN memberships, but you can change the policy of the exceptions to allow connections to another secure VLAN.

In addition, Advanced VLAN Policy provides the following benefits:

- Increased speed at which policy checks are done.
- Additional router interfaces are not needed in situations where a shared resource in a secure VLAN needs to connect to endpoints in more than eight VLANs, reducing overall network cost.
- External routers are not needed to connect VLANs, which reduces latency.
- Administrative configuration of a router Access Control List is not required, saving time and operational expense.

Launching Advanced VLAN Policy

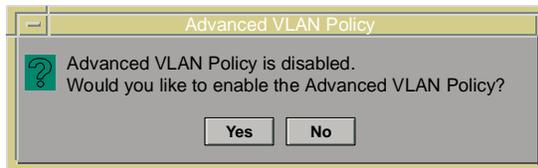


If Advanced VLAN Policy has already been enabled in a domain, and you then delete the domain (or reinitialize the VLANServer database) and rediscover the domain, Advanced VLAN Policy is disabled. You can re-enable it using the **Tools>Advanced VLAN Policy** menu option described in the next section.

To launch Advanced VLAN Policy for the current domain, click **Advanced VLAN Policy** from the **Tools** menu. A message is displayed informing you that Advanced VLAN Policy is loading. A progress bar shows how much of the application has been loaded. Once loaded, one of two things will occur.

- If this is the first time Advanced VLAN Policy has been loaded or if Advanced VLAN Policy was disabled before it was last closed, a message is displayed informing you that Advanced VLAN Policy is disabled (Figure 15-1). Click **OK** to enable Advanced VLAN Policy. A confirmation message is displayed informing you that Advanced VLAN Policy is enabled. Click **OK** to continue.
- The Advanced VLAN Policy main window is displayed (Figure 15-2).

Figure 15-1. Advanced VLAN Policy Disabled Message



1. Advanced VLAN Policy cannot be enabled if there are more than 128 non-AMR VLANs in the domain. If the domain contains more than 128 VLANs, a message informing you of that condition will be displayed.
2. If all switches in the domain you are running Advanced VLAN Policy against do not have the correct version of SecureFast firmware installed, the following error message is displayed. Refer to the VLAN Manager Release Notes for firmware requirements.





If a switch with incorrect firmware is discovered after the Advanced VLAN Policy is enabled, the results will be unpredictable. Running Advanced VLAN Policy against switches running incorrect firmware is not supported.

Advanced VLAN Policy Dependencies

Basic policy settings influence advanced policies in the following ways:

- When you create a VLAN, you set several properties for the VLAN: Policy Open or Secure, Flooding On or Off, and Status Enabled or Disabled. These properties interact with the Advanced VLAN Policy as follows:
 - **Open/Secure** - Used by Advanced VLAN Policy to initially populate the Connect policy for the VLAN. Refer to *Initial Settings on Page 15-8*.
 - **Flooding On/Flooding Off** - If flooding is On, the VLAN will flood according to the policy set in Advanced VLAN Policy. If flooding is Off, the VLAN will not flood at all, not even to itself.
 - **Enabled/Disabled** - No effect on Advanced VLAN Policy.



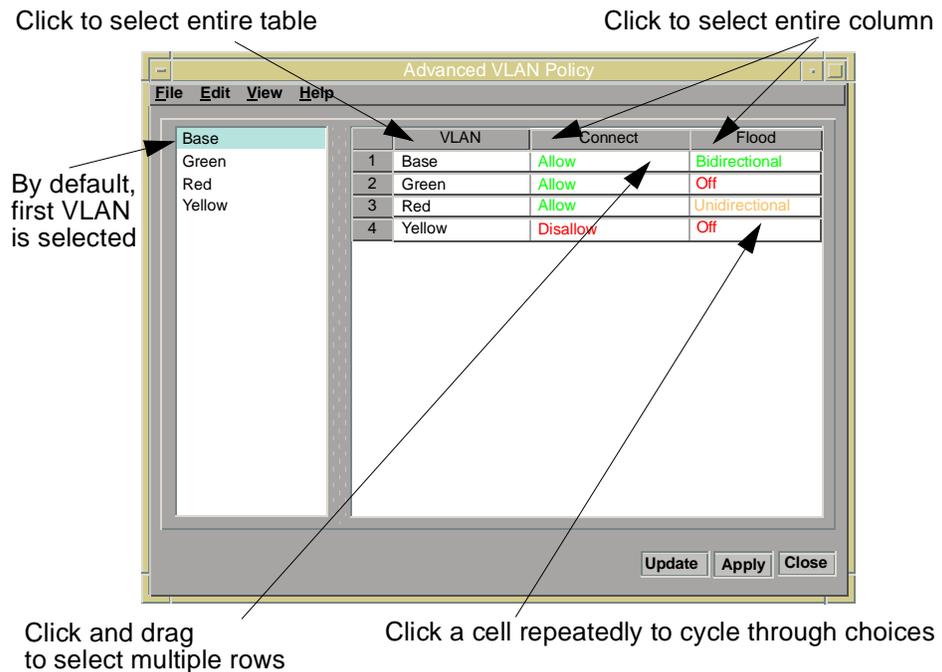
Even though a VLAN is disabled, you are still able to modify its Advanced Policy settings. The settings will not have any effect, however, until the VLAN is enabled.

- If a VLAN is toggled from Open to Secure (or vice versa) and its advanced policies have not been modified, the advanced policies will automatically be modified to be consistent with the initial settings. For instance, if a VLAN is toggled from Open to Secure, that VLAN's 'Connect' policy will be set to 'Disallow' with respect to all other VLANs (provided the policies have not been modified previously).

Using Advanced VLAN Policy

The Advanced VLAN Policy main window ([Figure 15-2](#)) contains the **File**, **Edit**, **View**, and **Help** menus, the Policy Table, which is composed of a left pane and a right pane, and the **Update**, **Apply**, and **Close** buttons. The left pane contains a list of all the non-AMR VLANs in a domain. The right pane contains three columns, **VLAN**, **Connect**, and **Flood**. The **VLAN** column contains a list of all the VLANs in a domain. The **Connect** column shows the connect policy that has been assigned to its corresponding VLAN. The **Flood** column shows the flood policy that has been assigned to its corresponding VLAN. Refer to *Advanced VLAN Policy Main Window Policy Table on Page 15-7* for detailed information about the Policy Table.

Figure 15-2. Advanced VLAN Policy Main Window

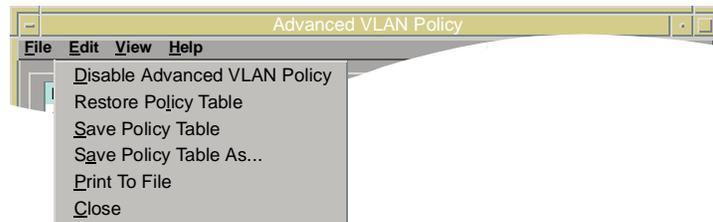


Advanced VLAN Policy Main Window Menus

File Menu

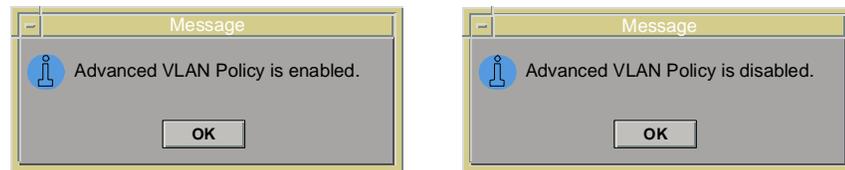
The **File** menu (Figure 15-3) consists of the following items: **D**isable/**E**nable Advanced VLAN Policy (Toggle), **R**estore Policy Table, **S**ave Policy Table, **S**ave Policy Table As, **P**rint To File, and **C**lose.

Figure 15-3. Advanced VLAN Policy File Menu



Enable Advanced VLAN Policy/Disable Advanced VLAN Policy - Lets you enable or disable Advanced VLAN Policy. When you click **Enable Advanced VLAN Policy**, Advanced VLAN Policy is enabled. When you click **Disable Advanced VLAN Policy**, Advanced VLAN Policy is disabled. A notification box (Figure 15-4) is displayed giving you the results of the operation. Policy control reverts back to basic policy if you disable Advanced VLAN Policy. Changes to the Advanced VLAN Policy table cannot be applied if Advanced VLAN Policy is disabled.

Figure 15-4. Enable/Disable Confirmation Box



Restore Policy Table - Restores Advanced VLAN Policy table information from the specified file. Policies must be applied using the **Apply** button before they will take effect.

Save Policy Table - Saves current Advanced VLAN Policy table information for the current domain. If a file has not been created for the information, you will be asked to specify a file.



The Advanced VLAN Policy table information is written to the VLANServer database when you click the **Apply** button. The **Save Policy Table** option writes this information to a file, not the database.

Save Policy Table As - Saves current Advanced VLAN Policy table information for the current domain in the specified file.

Print To File - Displays the **Print To File** submenu. This menu consists of the following items: **Text** and **Comma Delimited**.

Text - Prints current Advanced VLAN Policy table information to the specified file in plain text format.

Comma Delimited - Prints current Advanced VLAN Policy table information to the specified file in comma delimited text format.



Information saved using **Print To File** cannot be used to restore Advanced VLAN Policy table information. Use **Save Policy Table** or **Save Policy Table As** and then **Restore Policy Table** to restore policy table information.

Close - Terminate the Advanced VLAN Policy application.

Edit Menu

The **Edit** menu consists of the following items: **Select All**, **Select Column**, **Select Row**, **Properties**, and **Flood Policies**.

Select All - Highlights the entire policy table. An alternative is to click the upper left cell of the table header.

Select Column - Highlights the selected column in the policy table. An alternative way to select a column is to click the column heading.

Select Row - Highlights the selected row in the policy table. An alternative way to select a row is to click the VLAN name for the row.

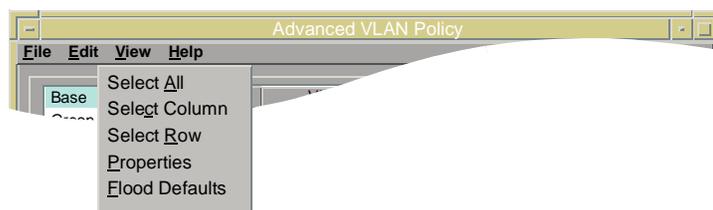
Properties - Displays the Properties dialog box. The dialog box displayed depends on the current selections made in the policy table. Refer to [Figure 15-10](#).

Flood Defaults - Displays a dialog box which lets you change the default advanced flood policies for a VLAN with respect to newly created VLANs in a domain. Flooding at the Advanced VLAN Policy level controls flooding of broadcast packets between endpoints in the same VLAN and in different VLANs provided flooding is enabled at the basic policy level.



This does not change the basic VLAN policy defaults.

Figure 15-5. Advanced VLAN Policy Edit Menu



View Menu

The **View** menu consists of the following items: **S**ort and **R**everse Policy.

Sort - Displays the Sort dialog box. This dialog lets you sort the right hand panel.

Reverse Policy - Displays the Reverse Policy dialog box. This dialog box shows the current selection in the reverse direction.

Figure 15-6. Advanced VLAN Policy View Menu



Help Menu

The **File** menu consists of the following item: **A**bout Advanced VLAN Policy.

About Advanced VLAN Policy - Provides release and copyright information about the version of Advanced VLAN Policy installed.

Figure 15-7. Advanced VLAN Policy Help Menu



Advanced VLAN Policy Main Window Policy Table

The Advanced VLAN Policy main window policy table (Figure 15-2) lets you set and apply the connect and flood policy for the selected VLAN in relationship to all other VLANs in a domain. The policy for a VLAN selected from the left window pane is shown in relationship to all other VLANs in a domain in the right window pane.

The connect policy determines if the selected VLAN can connect to other VLANs in a domain. Connectivity policy is symmetrical, that is, if the Connect policy for the 'Red' VLAN in relationship to the 'Blue' VLAN is set to 'Allow', the reverse will be true, the Connect policy for the 'Blue' VLAN in relationship to the 'Red' VLAN will also be 'Allow'.

Flood policy determines if the selected VLAN can flood unresolvable broadcast packets to other VLANs in a domain. Flood policy is not always symmetrical. Flood policy can be set to 'Bidirectional', 'Unidirectional', or 'Off', and will only be symmetrical if set to 'Bidirectional' or 'Off'. If the Flood policy for the 'Red' VLAN in relationship to the 'Blue' VLAN is set to 'Bidirectional', the reverse will be true, the Flood policy for the 'Blue' VLAN in relationship to the 'Red' VLAN will also be 'Bidirectional'. The same is true for a Flood policy set to 'Off'. However, if the Flood policy for the 'Red' VLAN in relationship to the 'Blue' VLAN is set to 'Unidirectional', the reverse policy will not be the same. The Flood policy for the 'Blue' VLAN in relationship to the 'Red' VLAN will be set to 'Off'.

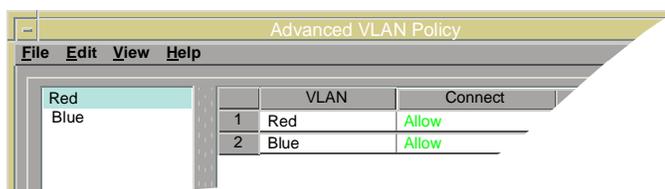
Initial Settings

Connect Policy

Initially, the contents of the Connect column are populated based on the basic VLAN Manager policy settings for each VLAN in the domain. The initial setting is 'Allow' between Open VLANs. The initial setting between Secure VLANs or between a Secure and an Open VLAN is 'Disallow'. The initial setting between a VLAN and itself is 'Allow'.

For instance, if two 'Open' VLANs ('Red' and 'Blue') exist in a domain, when the VLAN Policy table is populated, the Connect policy for each VLAN with respect to the other VLAN will be 'Allow' since both VLANs are in 'Open' mode. Connections are permitted with all other 'Open' mode VLANs in the domain. The Connect policy for the 'Red' VLAN in relationship to all VLANs in the domain is shown in [Figure 15-8](#).

Figure 15-8. Initial Connect Policy Example 1



	VLAN	Connect
1	Red	Allow
2	Blue	Allow

If a third VLAN ('Green') is created in Secure mode, the Connect policy for the Green VLAN with respect to the other two VLANs will be 'Disallow'. The Connect policy for the 'Green' VLAN in relationship to all VLANs in the domain for that situation is shown in [Figure 15-9](#).

Figure 15-9. Initial Connect Policy Example 2

	VLAN	Connect
1	Green	Allow
2	Blue	Disallow
2	Red	Disallow

Flood Policy

Initially, the contents of the Flood column are populated using the Flood Default table settings for each VLAN in the domain (Figure 15-16). The initial Flood Default for all VLANs in a domain is 'Off' except to itself. You can change the behavior of the initial flood settings by changing the flood defaults. For instance, let's say you want any newly created VLANs to be able to flood to the 'Blue' VLAN. You would set the default flood policy for the 'Blue' VLAN to 'On' and then apply the changes. From that time on, any new VLANs created would have a 'Unidirectional' flood policy in relationship to the 'Blue' VLAN.



If the basic Flood setting for a VLAN is set to 'Off', the Advanced VLAN Flood Policy for that VLAN is completely disabled, including to itself.

Selecting Parts of the Policy Table

Before you can set policy, part or all of the policy table must be selected. You can use the mouse, or **Edit** menu choices to make your selections. If you select a single row, multiple rows, or the entire table, you can change Connect and/or Flood policy. If you select the Connect column, you can change Connect policy. If you select the Flood column, you can change Flood policy.

- To select the entire policy table, click the VLAN column heading or choose **Select All** from the **Edit** menu.
- To select the entire Connect or Flood column, click the Connect or Flood column heading or you can click anywhere in a column and then choose **Select Column** from the **Edit** menu.
- To select an entire row, click on the number corresponding to the row you want to select or click anywhere in a row and then choose **Select Row** from the **Edit** menu.
- To select multiple cells, click on a cell and drag the mouse into other cells you want to select.
- To select an individual cell, click on the cell. Clicking a cell repeatedly lets you cycle through the choices for that cell. For instance, clicking in a Connect column cell repeatedly changes the contents of the cell from 'Allow' to 'Disallow', Clicking a

Flood column cell repeatedly changes the contents of the cell from 'Off' to 'Bidirectional' to 'Unidirectional'. When you have made all changes to the table, click **Apply** to enforce the changes.

Text in the policy table's Connect and Flood columns is color coded. Color definitions are described as follows:

Table 15-1. Connect and Flood Column Color Coding Definitions

Color	Connect Column	Flood Column
Green	Allow	Bidirectional
Red	Disallow	Off
Orange	N/A	Unidirectional

Advanced VLAN Policy Main Window Buttons

Update - Click to update the contents of the policy table.

Apply - Click to save the changes you have made to VLAN policies during the current Advanced VLAN Policy session and leave the application open.

Close - Click to exit the Advanced VLAN Policy application. If you click **Close** before saving (applying) the changes you made to VLAN policies during the current Advanced VLAN Policy session, a dialog box is displayed, asking you to confirm your decision. If you proceed without saving, none of the changes you made will be saved and the application will be terminated.

Setting Advanced VLAN Policy



If the VLANServer database changes (e.g., a new VLAN is created) in such a way as to change the Advanced VLAN Policy table or Flood Defaults table, a message informing you of that situation is displayed.

If the VLAN Policy table is affected, the following message is displayed.



Changes will not be displayed until the affected table is updated.

You use the functionality available from the Advanced VLAN Policy main window to set policies for VLANs that already exist in a domain and to perform support tasks such as sorting the contents of a column, viewing reverse flood policy, and setting flood defaults.

To fine tune the policy for an existing VLAN:

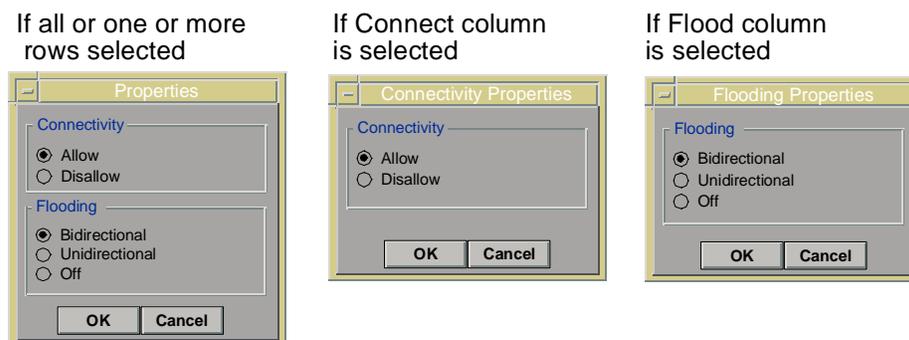
1. Select the VLAN for which you want to change policy from the left pane (Figure 15-2) of the Advanced VLAN main window.
2. Select the part(s) of the Advanced VLAN Policy main window's right pane for which you want to edit policy (in relationship to the VLAN you selected in Step 1) (Figure 15-2).



The policy for single cells can be set by clicking on the cell repeatedly until the choice you want is displayed. To save the change, click **Apply**.

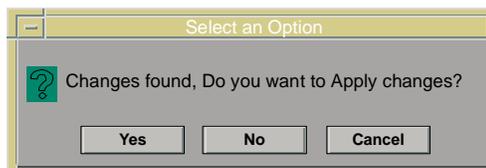
3. From the **Edit** menu (Figure 15-5), Select **Properties**. The Properties dialog box is displayed. The contents of the dialog box (Figure 15-10) depends on what parts of the right pane you selected in Step 2. If you did not make any selections, the **Properties** window will not be displayed.

Figure 15-10. Advanced VLAN Policy Properties Dialog Boxes



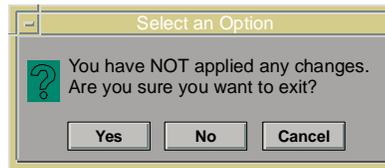
4. Make changes in the Properties dialog box by clicking **Allow** or **Disallow** in the Connectivity dialog box and then clicking **Bidirectional**, **Unidirectional**, or **Off** in the Flooding dialog box.
5. Click **Apply** to save your changes, or **Close** to close the Advanced VLAN Policy window.
 - If you make changes and then click **Update** without first clicking **Apply**, the message shown in [Figure 15-11](#) is displayed.

Figure 15-11. Update Message



Yes applies changes, and then updates, **No** does not apply changes but will update, and **Cancel** terminates the operation.

- If you make changes and then click **Close** without first clicking **Apply**, the message shown in [Figure 15-12](#) is displayed.

Figure 15-12. Close Message

Yes exits the application, **No** and **Cancel** terminates the operation.

- If you make changes and then click **Apply**, the message shown in [Figure 15-13](#) is displayed.

Figure 15-13. Apply Message

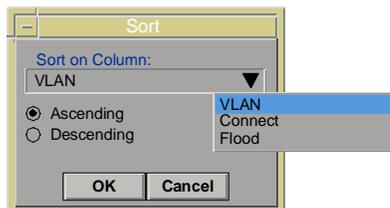
Advanced VLAN Policy settings are not persistent. If you reinitialize your database, Advanced VLAN Policy settings will be lost. To avoid this situation, File ? Use Save Policy Table to save Advanced VLAN Policy settings. The file created using this function can be used to restore the settings if you reinitialize your database.

Sorting the Advanced VLAN Policy Main Window

You use **Sort** to rearrange the contents of any column in the right pane according to criteria you select from the Sort dialog box.

To sort a column:

1. Select **Sort** from the Advanced VLAN Policy View menu. The Sort dialog box is displayed ([Figure 15-14](#)).

Figure 15-14. Sorting the Advanced VLAN Policy Main Window

2. Select a column to sort on from the Sort on Column drop-down list. Your choices are: **VLAN**, **Connect**, or **Flood**.
3. Click the type of arrangement you want the sorting process to use. Your choices are: **Ascending** or **Descending**.
4. Click **OK** to sort the column and then dismiss the Sort dialog box or **Cancel** to dismiss the Sort dialog box without sorting the column.

Viewing Reverse Policy

The Reverse Flooding viewing feature displays the policy of a selected VLAN in reverse. This is useful when the flood policy for a VLAN is set to '**Unidirectional**'. You can see the reverse policy of the VLAN at a glance without having to change the policy table view. This dialog box is non-modal. Any time a cell or row is picked from the right pane, the dialog will be updated to reflect the reverse policy.

1. Click a VLAN in the left pane. The right pane displays the relationship between the VLAN selected from the left pane in relationship to all VLANs in the domain (including itself).
2. Click anywhere in the row containing the policy information of the VLAN for which you want to display the reverse policy.
3. Select **Reverse Policy** from the Advanced VLAN Policy View menu. The Reverse Policy dialog box is displayed (Figure 15-15).

Figure 15-15. Viewing Reverse Policy



With the Reverse Policy table open, click on any row in the Policy Table to show the reverse policy for the VLAN in that row.

- Click **OK** to dismiss the Reverse Policy dialog box.

Setting Flood Defaults

The contents of the Flood Defaults table are used when a new VLAN is created to populate the **Flood** column of the Policy table. For instance, let's say you want any newly created VLANs to be able to flood to the 'Blue' VLAN. You would set the default flood policy for the 'Blue' VLAN to 'On' and then apply the changes. From that time on, any new VLANs created would have a 'Unidirectional' flood policy in relationship to the 'Blue' VLAN. The default value is 'Off'.

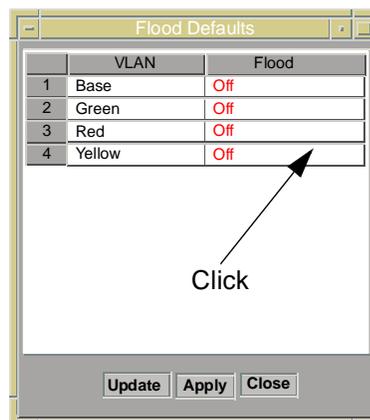


If the basic Flood setting for a VLAN is set to 'Off', the Advanced VLAN Flood Policy for that VLAN will be ignored with respect to connection establishment. The VLAN will not flood at all.

To edit the Flood Defaults table:

- Select **Flood Defaults** from the Advanced VLAN Policy **Edit** menu. The Flood Defaults table is displayed (Figure 15-16).

Figure 15-16. Setting Flood Defaults



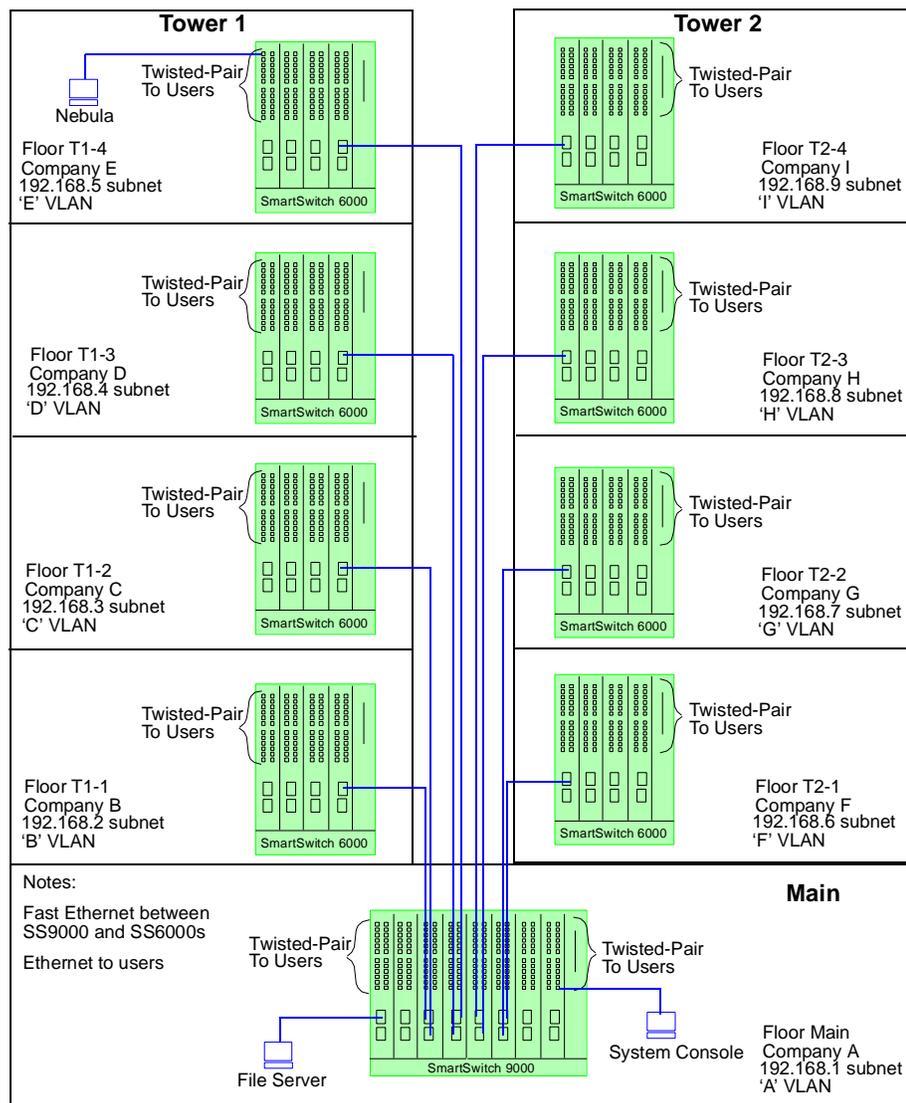
2. Click anywhere in the Flood cell you want to change, repeating this action until the choice you want (**Off** or **On**) is displayed.
3. Click **Update** to update the Flood Defaults table, **Apply** to save your changes, or **Close** to close the Flood Defaults table.

Advanced VLAN Policy Network Example

Setup

You are the system administrator of the Sunshine office complex. The complex consists of twin towers with a shared main floor. The complex's network is configured as shown in [Figure 15-17](#).

Figure 15-17. Sunshine Office Complex Network Configuration



Each office has been wired for Ethernet connections to a SS6000 in the wiring closet. Each SS6000 has been wired for Fast Ethernet connections to the SS9000 in the main floor wiring closet. In addition, the main floor wiring closet contains a File Server and the System Console.

The complex is designated with a network address of 192.168.x.x. You designate each of the tower floors and the main floor as a separate subnet. The main floor has a subnet address of 192.168.1, floor T1-1 192.168.2, etc. The network is fully operational.

You are using VLAN Manager to manage the network. You designated the entire network as belonging to the ‘Sunshine’ domain. Each floor (subnet) has its own VLAN as do the File Server and the System Console.

Each floor is to be occupied by a different company. Company A will occupy the main floor, Company B T1-1, and so forth and so on.

Requirement

The network requirement is to prohibit communication between endpoints in different companies but allow communication between endpoints in the same VLAN and also allow all endpoints on the network to access the File Server.

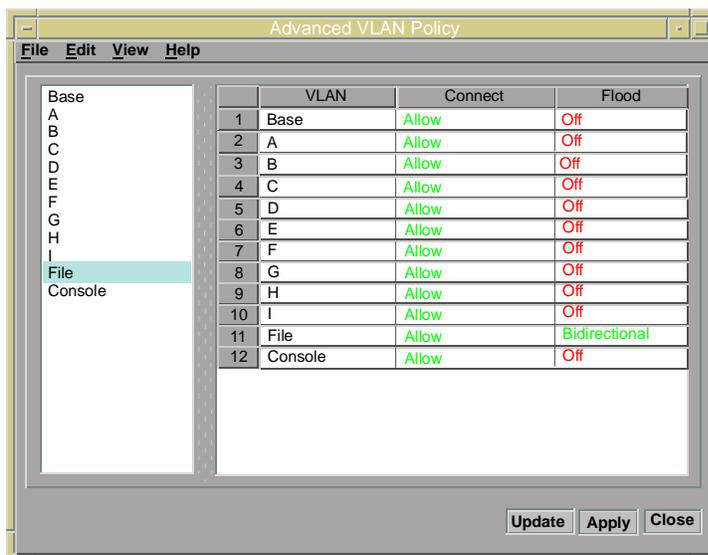
Solution

To meet the network requirement using Advanced VLAN Policy, you would:

1. Create nine ‘Secure’ VLANs (‘A’ - ‘I’), one for each company. This prohibits communication between endpoints in different VLANs but allows communication between endpoints in the same VLAN.
2. Create a ‘Secure’ VLAN for the File Server (File).
3. Assign the endpoints in each company membership in that company’s VLAN, and assign the File Server membership in the ‘File’ VLAN. This can be done using static or inherited membership.
4. Launch Advanced VLAN Policy from the VLAN Manager **Tools** menu and enable the application.
5. Use Advanced VLAN Policy to configure the ‘File’ VLAN with the Connect policy set to ‘Allow’ to all other VLANs (Figure 15-18). This policy lets the ‘File’ VLAN connect to all other VLANs and since the Connect policy is symmetrical, all VLANs can connect to the ‘File’ VLAN. This policy allows all users to gain access to the File Server but prohibits communications between company VLANs.

Say endpoint ‘Nebula’ who is a member of the ‘E’ VLAN wants to connect to the File Server. Nebula’s source switch, using local directory checking and inter-switch resolves finds the File Server (assuming all endpoints connected to the switches have been previously learned). Policy is checked. Since the ‘E’ VLAN (Nebula’s VLAN) is allowed to connect to the ‘File’ VLAN, the connection would be set up.

Figure 15-18. Sunshine Office Complex Advanced Connect VLAN Policy



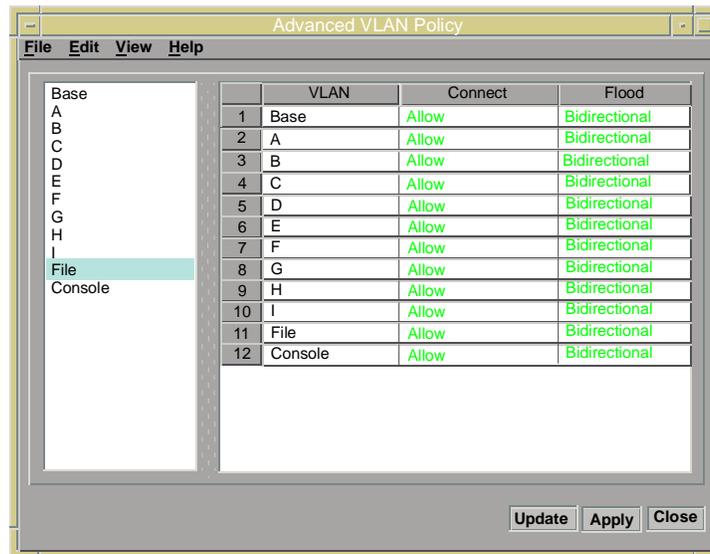
This solution works under these circumstances because no flooding is required. If the switch to which the File Server is connected had *not* previously learned about the File Server, the File Server would not be resolved using local directory checking and inter-switch resolves and flooding would be required. Since flooding is not allowed between the 'E' VLAN and the 'File' VLAN, the File Server would never be resolved and a connection would never be set up.

To resolve the File Server, the Flood policy would have to be set to **'Bidirectional'** between the 'File' VLAN and the 'E' VLAN (Figure 15-19).

The 'E' VLAN would then be allowed to flood to the 'File' VLAN and the 'File' VLAN would be able to flood to the 'E' VLAN since 'Bidirectional' flooding is symmetrical.

The source switch would flood out all 'E' and 'File' VLAN ports. The flood would propagate throughout the domain and the File Server would be found. Since the Connect policy is still in force which allows all VLANs to connect to the 'File' VLAN, the connection would be set up.

Figure 15-19. Sunshine Office Complex Advanced Connect VLAN Policy



This solution lets not only allows endpoints in the 'E' VLAN to connect to the File Server, it allows all endpoints in the domain connect to the File Server while maintaining security between VLANs.

Managing the Advanced VLAN Policy Table

An Advanced VLAN Policy table contains all advanced VLAN policy information for a domain. Several versions of the table can be saved and then restored as needed. This can be useful when testing new policies. For instance, you can save the current table, create a new table, test it, and be able to restore the original table if need be.

If the database is reinitialized, you can bring up the Advanced VLAN Policy application and then restore the Advanced VLAN Policy table.



If the entire VLAN install area is to be deleted, copy saved versions of the Advanced VLAN Policy table to a safe location before deleting the area.

This section describes how to save an Advanced VLAN Policy table, Restore an Advanced VLAN Policy table, and print an Advanced VLAN Policy to a text file.

Saving an Advanced VLAN Policy Table

You can save an Advanced VLAN Policy table by using **Save Policy Table** or **Save Policy Table As** items from the **File** menu. **Save Policy Table** is used to initially save a policy table or to save changes to a policy table using the same file name and file location. **Save Policy Table As** is used to save a policy table using a different file name or file location.

Saving a Policy Table Using Save Policy Table

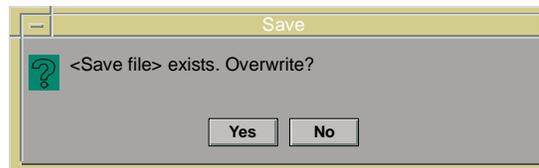
To save an Advanced VLAN Policy table by using **Save Policy Table**:

1. Select **Save Policy Table** from the **File** menu. A message (Figure 15-20) informing you that the save file already exists is displayed. You must confirm that the file can be overwritten.



If the Advanced VLAN Policy table you want to save has never been saved before, the **Save Policy Table As** window is displayed. Refer to *Saving a Policy Table Using Save Policy Table As* on Page 15-21.

Figure 15-20. Save Policy Table Overwrite Message



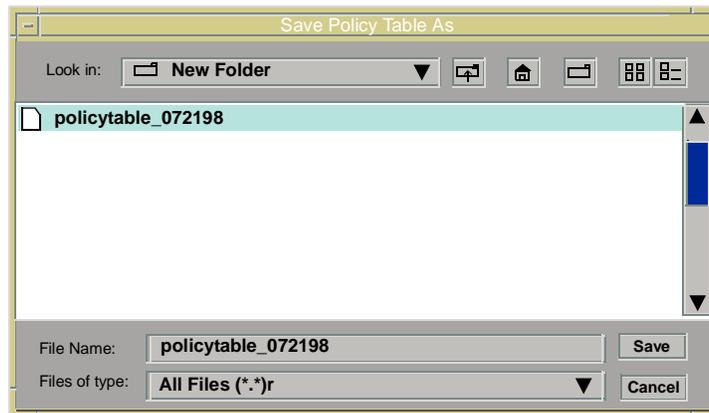
2. Click **Yes** to save the table to the existing file or **No** to terminate the operation.

Saving a Policy Table Using Save Policy Table As

To save an Advanced VLAN Policy table by using **Save Policy Table As**:

1. Select **Save Policy Table As** from the **File** menu. The **Save Policy Table As** window is displayed (Figure 15-21). This window operates much like the Windows NT Open dialog box with one notable exception; the name of the folder created using the **New Folder** button cannot be changed in the **Save Policy Table As** window. You change the name using your UNIX or NT graphical user interface or command line interface.

Figure 15-21. Save Policy Table As Window



2. Navigate to the folder in which you want to save the policy table.
3. Enter the name of the save file in the **File Name** text box.
4. Click **Save** to save the policy table or **Cancel** to terminate the save operation.

Restoring an Advanced VLAN Policy Table

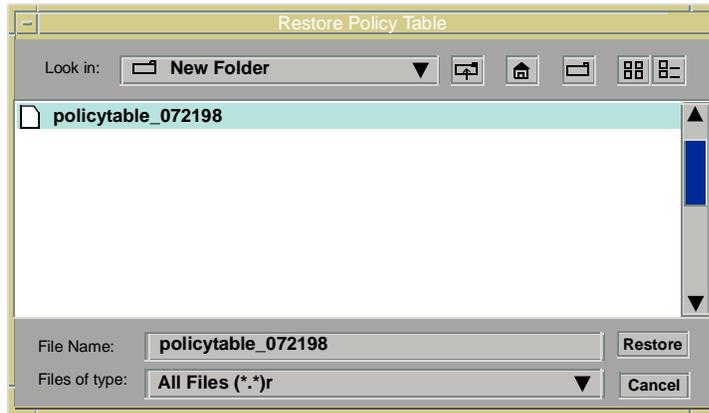
To restore an Advanced VLAN Policy table by using **Restore Policy Table**:



If you restore a VLAN Policy table and VLANs have been created or deleted since the file was created/saved, you will be notified of the discrepancies between the VLANs in the current table and those in the saved file. The discrepancies can be ignored or can be resolved by adding or deleting VLAN, as required and then restoring the table from the saved file again. You must apply the restored policies before they will take effect.

1. Select **Restore Policy Table As** from the **File** menu. The Restore Policy Table window is displayed (Figure 15-21).

Figure 15-22. Save Policy Table As Window



2. Navigate to the folder where the saved policy table that you want to restore resides.
3. Click on the name of the file you want to restore. The file name is automatically entered in the **File Name** text box.
4. Click **Restore** to restore the selected policy table or **Cancel** to terminate the restore operation.

Printing an Advanced VLAN Policy Table to a Text File

You can print a policy table to a file by using **Print To File**. A file can be printed in one of two formats: text or comma delimited.



A policy table printed to a file using Print To File cannot be restored. Only policy tables saved using Save Policy Table or Save Policy Table As can be restored.

The sample formatted outputs below show only a portion of the actual outputs. The actual outputs would contain data about each VLAN in relationship to all non-AMR VLANs in the domain.

Text Format

```
Source VLANDestination VLANConnectFlood
```

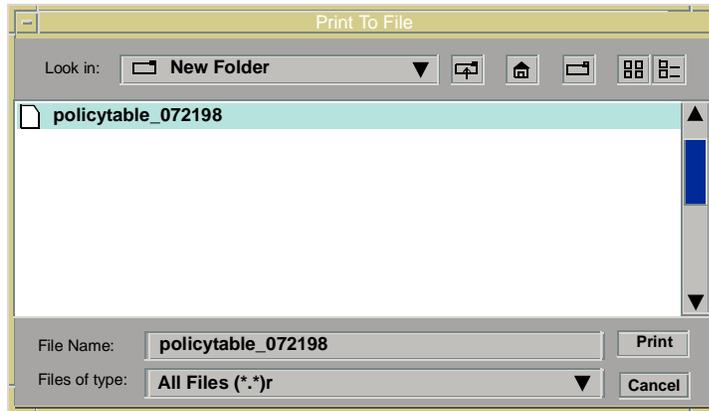
```
BaseBaseAllowBidirectional
```

```
BaseA AllowBidirectional
```


To print a policy table to a file:

1. Select **Text** or **Comma Delimited** from the **File >Print To File** menu. The Print To File window (Figure 15-23) window is displayed.

Figure 15-23. Print To File Window



2. Navigate to the folder in which you want to print the policy table.
3. Enter the name of the print file in the **File Name** text box.
4. Click **Print** to print the selected policy table to the print file or **Cancel** to terminate the print to file operation.

Managing Your Database

This chapter provides step-by-step instructions for managing your VLANServer database, using SPECTRUM VLAN Manager's graphical user interface.

VLAN Manager Database Backup

Creating regular backup copies of your database is the foundation of database maintenance. A reliable backup copy of your database can help you restore the integrity of your database following power failures or other system interruptions. This section describes how to do a backup automatically, using VLAN Manager's On-Line Backup utility. Other database maintenance tasks include manually backing up (saving) the database and restoring database backup files. You perform these tasks from the VLAN Manager Control Panel. Refer to *The SPECTRUM VLAN Manager Control Panel*, on page 2-9.

On-Line Backup

VLAN Manager's On-Line Backup feature can relieve you of manually creating backups of your database. On-Line Backup can be configured to automatically save your database at regular intervals, while the VLANServer is running. It can also be used to save your database on demand without bringing the VLANServer down. The interval between automatic saves is determined by a schedule that you can adjust to your particular network environment.

On-Line Backup saves the entire database (models and catalog). Where disk space is limited, On-Line Backup can be configured to automatically compress backup files using the standard shell utility, **compress**.

On-Line Backup performs a save in two major steps: a copy is made to preserve a "snapshot" of your database files, and this copy is then saved (and compressed if required).

Polling, trap handling, and network management activities are suspended during the first step (copying database files). While this is a relatively short process, you should still consider these interruptions to determine how often and when to schedule automatic save operations. The time required to perform the copy depends on your workstation hardware and the size of the database.

Backup File Maintenance

When automatic backups are enabled, backup files can accumulate in your backup directory and deplete available disk space. To avoid backup failures, files must be moved to a more permanent storage media or removed entirely.

Configuring On-Line Backup

To configure online backup:

1. Select **Online Backup** from the **File** menu to display the On-Line Database Backup Configuration window (Figure 16-1).

Figure 16-1. On-line Database Backup Configuration View

The screenshot shows a configuration window titled "SPECTRUM VLAN Manager - VLANServer DB Backup". The window has a blue background and contains several settings:

- Backup Now:** A button labeled "No".
- Backup Compression:** A button labeled "Enabled".
- Backup File Prefix:** An empty text input field.
- Backup Directory:** An empty text input field.
- Automatic Backup:** A button labeled "Disable".
- Backup Interval:** A label "(hours)" followed by a text input field containing "24", and a label "(minutes)" followed by a text input field containing "0".
- Next Backup Time:** A text input field containing "None".
- Status:** An empty text input field.

At the bottom of the window, there are four buttons: "OK", "Reset", "Apply", and "Cancel".

2. Set each option according to the following field descriptions:

Backup Now (No/Yes)

Select **Yes** to initiate a database backup as soon as the **OK** button is clicked. Select **No** (default) to initiate a backup based on the automatic backup selections. Upon completion of the backup process, the button is restored to its default setting. Files created by backups are saved according to the configuration parameters specified.

Backup Compression (Enabled/Disabled)

Select **Enabled** to compress backup files using the compress utility before files are written to disk. Compressed files are saved with a **.Z** suffix appended to the file name. Select **Disabled** (default) to save files in uncompressed format.

Prefix for Backup File Name

This parameter is the user-defined portion of the backup file name. VLAN Manager assigns a default “db” prefix. When added to the suffix, you can change this to any character string that creates a legal filename for the system where you are running VLANServer (no entry means that no prefix appears in the filename).

The filename suffix indicates the date and time when the backup was executed, in the following format: *yyyymmdd_hhmm* [Z]

where:	yyyy	4-digit year
	mm	month 1 - 12
	dd	day of the month 1 through 31
	hh	hour of the day - 1 through 24
	mm	minute - 00 through 59
	.Z	indicates a compressed backup (compressed files only)

Backup Directory

This parameter defines the location where backup files are stored. It is recommended that you back up to a local directory. The default backup path is `/usr/Spectrum/VLAN-DB-Backup`.

Automatic Backups (Disabled/Enabled)

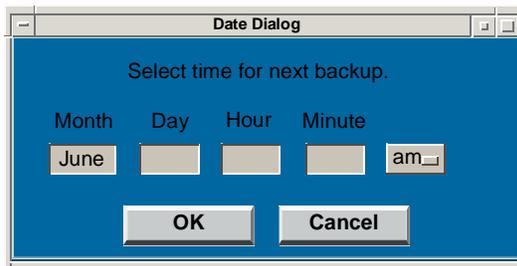
This button controls automatic initiation of On-Line Backups. Possible entries: **Disabled** - no automatic backups initiated, and **Enabled** - automatic backups initiated. If this button is set to **Disabled**, the **Next Backup Time** button is grayed out and set to None.

Backup Interval

When automatic backups are enabled, these entries determine, in hours & minutes, the interval between automatic backups. The default interval is 24 hours and 0 (zero) minutes. The recommended backup interval is one week or less. Any value can be entered for hours and minutes. For example, a one week interval would be $24 \times 7 = 168$ hours, and 0 minutes or, you could enter the same interval as any combination of hours and minutes (0 hours, and 10,080 minutes.)

Next Backup Time

Click this button to display the Date Dialog window (Figure 16-2).

Figure 16-2. Date Dialog Window

This window shows the date and time for the next scheduled backup, when automatic backups are enabled. You can enter a date and time for the first backup, but subsequent backups will be performed at the interval set by the Backup Interval parameters. To have automatic backups occur at the same time each day, set the interval to 24 hours and 00 (zero) minutes.

If a date and time in the past are entered, the backup interval parameter entries are added to the date and time to adjust it to a date and time in the future, which then becomes the Next Backup Time.

Backup Status

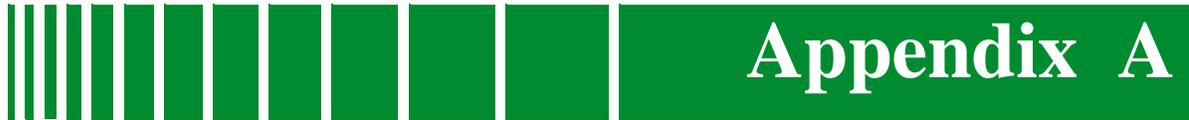
This read-only parameter indicates the database backup status as: “Ready”, “Checking setup”, “Copying database. VLANServer paused.”, “Last backup successful”, “Saving copied database. VLANServer resuming normal activity.”, “SSdbsave failed!”, or “Backup failed!”.

If an online backup attempt fails, check file permissions and available disk space.



If you Restore a database from an automatic backup, you may have to uncompress it and/or copy it into the <VLAN Install area>VLAN/server directory.

To restore a database, see *Restoring the VLANServer Database*, on page 2-18.



Glossary

This glossary is divided into two parts, each associated with or related to Virtual LANs or VLAN Manager. The first part consists of a list of commonly used acronyms and their meanings. The second part consists of a list of commonly used terms and their definitions.

Acronyms

- AAL** - ATM Adaptation Layer
- AMI** - ATM Management Interface
- AMR** - Automatic Membership Registration
- ARP** - ArpNet Protocol
- ATM** - Asynchronous Transfer Mode
- BPDU** - Bridge Protocol Data Units
- BUS** - Broadcast Unknown Server
- CLI** - Command Line Interface
- DCM** - Device Communication Manager
- DNS** - Domain Name Server
- ELAN** - Emulated LAN
- FDDI** - Fiber Distributed Data Interface
- FNB** - Flexible Network Bus
- FPS** - Fast Packet Switch
- GUI** - Graphical User Interface
- IGMP** - Internet Group Management Protocol
- INB** - Internal Network Bus

IP - Internet Protocol

IPX - Internet Packet Exchange

ISO - International Standards Organization

LAN - Local Area Network

LANE - Local Area Network Emulation

LEC - LAN Emulation Client

LECS - LAN Emulation Configuration Server

LES - LAN Emulation Server

MAC - Media Access Control

MCSP - Multicast Cabletron Switch Protocol

MIB - Management Information Base

NIS - Name Information Server

NNI - Network-to-Network Interface

NVRAM - Non-Volatile RAM

OSI - Open Systems Interconnection

OSPF - Open Shortest Path First

PVC - Permanent Virtual Circuit

PVID - Port VLAN ID

RAM - Random Access Memory

RIP - Router Interface Protocol

SAP - Service Advertisement Protocol

SA/DA - Source Address/Destination Address

SCS - Software Control Software

SFPS - SecureFast Packet Switch

SNMP - Simple Network Management Protocol

SPMA - SPECTRUM Portable Management Application

SRN - Software Release Notice

STP - Shielded Twisted-Pair

SVC - Switched Virtual Circuit

TFTP - Trivial File Transfer Protocol

TOS - Type Of Service

TTL - Time To Live

UNI - User-to-Network Interface

VCC - Virtual Channel Connection

VCI - Virtual Channel Identifier

VPI - Virtual Path Identifier

VLAN - Virtual Local Area Network

VLSP - Virtual Link State Protocol

VRRP - Virtual Router Redundancy Protocol

Terms

1d trunk - A connection from a switch that passes only untagged traffic.

access port - A port on a VLAN switch that has been designated for user (end-system) connections.

alias - A way of identifying a user by something other than its MAC address, for example, by IP or IPX address.

Automatic Membership Registration (AMR) - A SecureFast VLAN Manager feature that dynamically creates VLANs, joins endpoints to those VLANs, and floods packets to those VLANs according to the set of criteria rules.

Base VLAN - VLAN that all endpoints in a domain have membership in until administratively moved to another VLAN.

bindery - A database that contains a complete collection of related information.

broadcast - Data sent from one endpoint to all other network endpoints (point-to-multipoint communications).

community name - Defines security communities to which an SNMP agent is permitted access to a device and establishes Read/ReadWrite privileges.

default gateway - The switch port configured to service connection requests to subnets not serviced by the switches in a domain.

default VLAN - The VLAN assigned to be the default VLAN for a port. All endpoints connecting to a port will assume membership in the default VLAN for that port.

directory - A set of data about all users in a domain. Typically, the directory contains such entries as the user's physical address, the switch and port to which the user is connected, and the network type, and the user's name.

discover - Process used to find switches and users contained in a VLAN domain.

daemon - A software program that generally performs a single task and is executed only when it is needed.

domain - A Group of VLAN switches bounded by a router or ATM device.

Domain Name Server (DNS) - A protocol used to provide mappings between host names and IP addresses.

endpoint - A device attached directly to a switch's network user port (e.g., workstation, PC, or router).

flooding - A method used by SecureFast switches so that, if the switch fails to resolve the destination address for a packet to a host or a VLAN, the packet is transmitted out all the switch's ports except the port the packet was received on.

folder - A virtual container used to group users. There are two levels of folders. The first level groups different VLAN types (e.g., VLAN, AMR). The second level groups users of the same type (e.g., inherited, static).

Graphical User Interface (GUI) - An interface that allows a user to select a menu item by using a mouse to point to a graphic icon or piece of text. This is an alternative to the more traditional command line interface, where an alphanumeric string is used to convey instructions. GUIs make computer applications easier to use for humans (i.e., user friendly).

hub - The center of a star topology network or cabling system in which a multi-node network topology has a central multiplexor with many nodes feeding into and through the multiplexor or hub. The other nodes do not usually directly interconnect.

Internet Protocol (IP) - One of a collection of communication protocols which has become the *de facto* solution for open networking.

IP address - A 32-bit address divided into two fields: a network-identifier and a host-identifier. The network-identifier refers to a particular physical network in an Internet, and the host-identifier refers to a particular device attached to that physical network.

IP Multicast - A SecureFast VLAN Manager feature that automatically creates IP Multicast groups for each IP Multicast address heard by the switches in a SFS domain. This feature lets you perform many IP Multicast administrative tasks including adding or removing receivers from an IP Multicast group and setting security for switches and ports associated with IP Multicast groups.

Internet Packet Exchange (IPX) - A communications protocol developed by the Novell Corporation.

LEC failover - A mechanism that lets you create multiple instances of an ELAN. Backup ELANs or “failovers” protect against communication loss if a primary ELAN fails. LEC failover is a proprietary feature of FORE Systems. Failover ELANs are created and configured using your FORE LANE Services tool.

legacy network - Traditional router and bridge LANs, using Ethernet, Token Ring, or FDDI.

MAC - Media access connection of the data link layer.

multicast - Data sent from one endpoint to a group of other network endpoints (point-to-multipoint communications).

OSI model - A seven layer model that defines the rules for transferring information from one endpoint to another. The seven layers are defined below.

(1) Physical Layer - Responsible for the transmission of bit streams across a particular physical transmission medium. It involves a connection between two endpoints allowing electrical signals to be exchanged between them.

(2) Data Link Layer - Responsible for moving information across a particular link. Across that link, it ensures good transmission and correct delivery by checking errors, retransmitting as necessary, and attaching appropriate addresses to the data sent. The contention access methods (e.g., CSMA/CD, and Token Passing) are regarded as Layer 2 activities.

(3) Network Layer - Concerned with routing data from one network to another. It is responsible for establishing, maintaining, and terminating the network connection

between two users and for transferring data along that connection. Although there can be only one network connection between two given users, there can be many possible routes from which to choose when the particular connection is established.

(4) Transport Layer - Responsible for providing data transfer between two users at an agreed level of quality. When a connection is established, this layer is responsible for selecting a particular class of service to be used, for monitoring transmissions to ensure the appropriate service quality is maintained, and for notifying the users if it is not.

(5) Session Layer - Focuses on providing services used to organize and synchronize the dialog that takes place between users and to manage the data exchange. A primary concern of the session layer is controlling when users can send and receive concurrently or alternately.

(6) Presentation Layer - Responsible for the presentation of information in a way that is meaningful to the network users. This may include character code transmission, data conversion, or data compression and expansion.

(7) Application Layer - Provides a means for application processes to access the system interconnection facilities in order to exchange information. This includes services used to establish and terminate the connections between users and to monitor and manage the systems being interconnected, as well as the various resources they employ.

Local Area Network (LAN) - A data communications network that can cover a limited area of up to about six miles in radius with moderate to high data speeds. The devices linked by a LAN may all be in the same building or in a group of buildings in relatively close proximity. It is user-owned and does not run over leased lines, although it might have gateways to public and/or private networks.

MAC address - Physical address for a given device.

multicast - Data sent from one endpoint to multiple network endpoints (point-to-multipoint communications).

Network Port - A port on a VLAN switch that has been designated for network connections.

packet - A unit of data consisting of several fields. Packets may be of fixed lengths or varying lengths.

poll - Periodic collection of specific information from a network device which is being managed by VLAN Manager.

port restriction - Restriction placed on a port which allows only specified MAC addresses to be connected to the port.

port violation - Heard when a MAC address not specified for a restricted port is discovered on that port.

Port VLAN ID (PVID) - An identification that encompasses a particular switch port's identification and that port's VLAN membership.

preference - A client/UI setting about what data to display and how to display to. For example, display ToolTips or display the Topology view at 50% zoom.

processd - A process launching and tracking daemon that provides the VLANServer with the ability to control various processes that are run on various servers and clients in a distributed VLANServer environment.

property - An attribute of an object which is being managed. For example, setting a multicast port's query interval.

provision - To configure a connection manually.

redundant access port - Let you configure endpoints within a VLAN domain to be connected to more than one switch access port (one active, the others in standby).

repeater - In a LAN, this is a device that repeats a signal from one cable to the next, thereby, increasing the reach of a LAN signal. In FDDI, a repeater is an opto-electrical module that receives an optical signal and converts it into an electrical equivalent of the optical signal.

router - Unlike bridges, routers operate at the Network level (Layer 3) of the OSI model. Also unlike bridges, routers are protocol specific, acting on routing information carried by the communications protocol in the Network layer. Bridges pass Layer 2 (Data Link) packets directly on to the next segment of a LAN, whereas routers can use the information they have about the network topology to choose the best route for a packet. Because routers are Layer 3 devices, they are independent of the Physical (Layer 1) level.

seed switch - The switch identified to VLAN Manager as the starting point for the domain discovery process.

shared link - Connections between switches where each switch can hear more than one neighbor switch.

Simple Network Management Protocol (SNMP) - A application protocol providing network management within the Internet suite of Protocols.

switch - A network entity that provides switching functionality. The two types of switches considered in this document are SFPSs and ATM switches.

tag header - A 12-bit field within a frame that identifies the VLAN that the data frame belongs to.

tapped connection - A connection that is being monitored.

unicast - Data sent from one endpoint to a another network endpoint (point-to-point communications).

untagged frame - A data frame that does not have a Tag Header inserted into it.

uplink switching - A switch configuration used to extend the size of a domain beyond the 128 switch limit.

user/alias restriction - Restriction placed on a user or user alias which allows the user only to be connected to a specified port.

user/alias violation - Heard when a user MAC address or alias is discovered on a port other than the port to which it is restricted.

violator node - A user that has been discovered on a restricted port, and the port is not restricted to that endpoint, or a restricted user that has been moved to a port other than the user's restricted port.

VLAN - A local area network of users having full connectivity (sharing broadcast, multicast, and unicast packets) independent of any particular physical or geographical location. In other words, users that share a virtual LAN appear to be on a single LAN segment regardless of their actual location.

VLANServer - Provides VLAN Manager's intelligence. It contains models of the actual network devices and their interactions.

Wizard - A VLAN Manager feature that helps users quickly and effortlessly configure VLAN Manager resources.

SecureFast DHCP Relay Agent

This appendix provides information about the configuration and operation of the SecureFast DHCP Relay Agent.

Overview

DHCP (Dynamic Host Configuration Protocol) allows an endpoint to automatically obtain an IP address for a fixed length of time (lease period) from a remote server (DHCP server). Leases can be renewed. When the lease period expires, the IP address is returned to the pool of IP addresses administered by the DHCP server and can be assigned to another endpoint on the network.

The VLAN Manager uses DHCP client tagging to identify DHCP endpoints. DHCP endpoints are shown in the VLAN Manager's Main window using the DHCP Client icon.



DHCP Client Tagging is disabled by default. When DHCP client tagging is disabled, a DHCP client will still be able to request and acquire an IP address but the icon representing the endpoint will not appear in the VLAN Manager's Main window. Use **Services** from the **Tools >SecureFast Tools >Element Management** menu to enable DHCP Client Tagging. Refer to the *SecureFast Tools Guide* for information about how to use **Services**.

Acquiring an IP address from a DHCP server consists of two phases. The first phase consists of the endpoint broadcasting a request for an IP address to the DHCP servers and collecting IP address offers from the servers. The second phase consists of choosing an IP address offer from a DHCP server.

If an endpoint has access to a DHCP server, the request for an IP address can be made directly to the server; however, if an endpoint does not have access to a server, a DHCP relay agent can be used. A DHCP relay agent relays packets between servers and endpoints. This makes it possible to service subnets that do not have a DHCP server available and eliminates the need to set up a DHCP server for each subnet. When an endpoint requests an IP address, the relay agent intercepts the request and unicasts the IP address request to the DHCP, substituting its own IP address as the requesting address. The DHCP server uses the relay agent's IP address to determine the range of IP addresses

for the requesting endpoints subnet and sends the relay agent an IP address offer. The relay agent receives an IP address from the DHCP server and forwards it to the requesting endpoint.

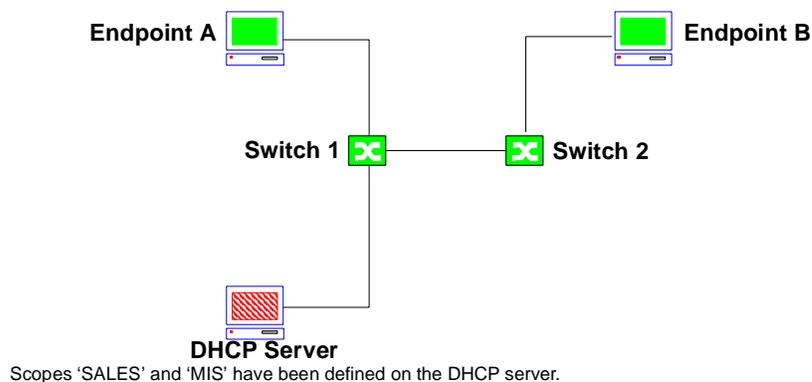
DHCP Relay Agent functionality is usually performed in Layer 3 routers to allow DHCP servers to recognize the address range (scope) used in response to a specific endpoint's DHCP request. SecureFast uses a similar functional model but does so within a single switched domain.

The SecureFast DHCP Relay Agent allows IP addresses of different scopes to be dynamically assigned to members of VLANs in a SecureFast domain from a single DHCP server by relaying DHCP packets between requesting endpoints and the DHCP server. Each VLAN is configured with a unique DHCP Relay Agent address. This address is used to scope the IP address offered to a requesting endpoint to the address range assigned to a particular VLAN.

DHCP Configuration

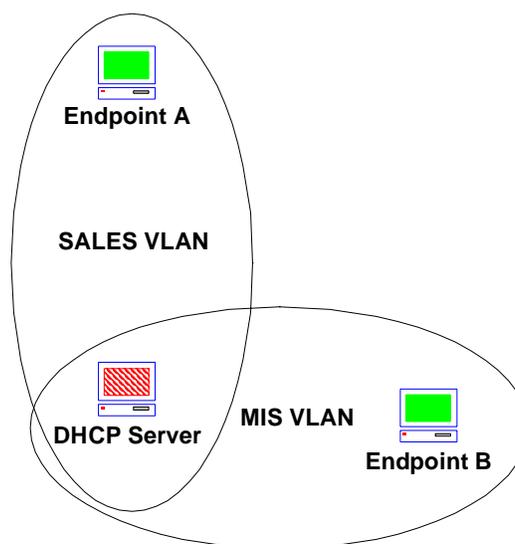
The sample network shown in [Figure B-1](#) consists of a DHCP server with two scopes defined, a set of SecureFast switches, and two DHCP endpoints (clients).

Figure B-1. DHCP Relay Agent Sample Network (Physical View)



As shown in [Figure B-2](#), the endpoints in this configuration are placed in two VLANs called SALES and MIS. Endpoint A is a member of the SALES VLAN and Endpoint B is a member of the MIS VLAN. The DHCP server must be a member of both the SALES and the MIS VLAN.

Figure B-2. DHCP Relay Agent Sample Network (Logical View)



The goal of this model is to allow the DHCP server to service the SALES and MIS VLANs as separate scopes by using DHCP Relay Agent functionality. Scopes have to be defined at the DHCP server for the two VLANs (SALES and MIS) and the scopes have to be defined to VLAN mappings.

Defining Scopes

Scopes are defined at the DHCP server. Scopes consist of a range of IP addresses to be allocated for a particular VLAN as well as network mask, exclusion, and other parameters associated with the VLAN. The scopes for VLAN SALES and VLAN MIS are shown below.

SALES	
Starting IP Address:	172.16.1.9
Ending IP Address:	172.16.1.254
Network Mask:	255.255.255.255
Exclusions:	172.16.1.9
Other Parameters:	SwitchedNetworkFlag=1

MIS	
Starting IP Address:	172.16.2.9
Ending IP Address:	172.16.2.254
Network Mask:	255.255.255.255
Exclusions:	172.16.2.9
Other Parameters:	SwitchedNetworkFlag=1

The way in which you define a scope depends on your DHCP server. Refer to your DHCP server documentation.

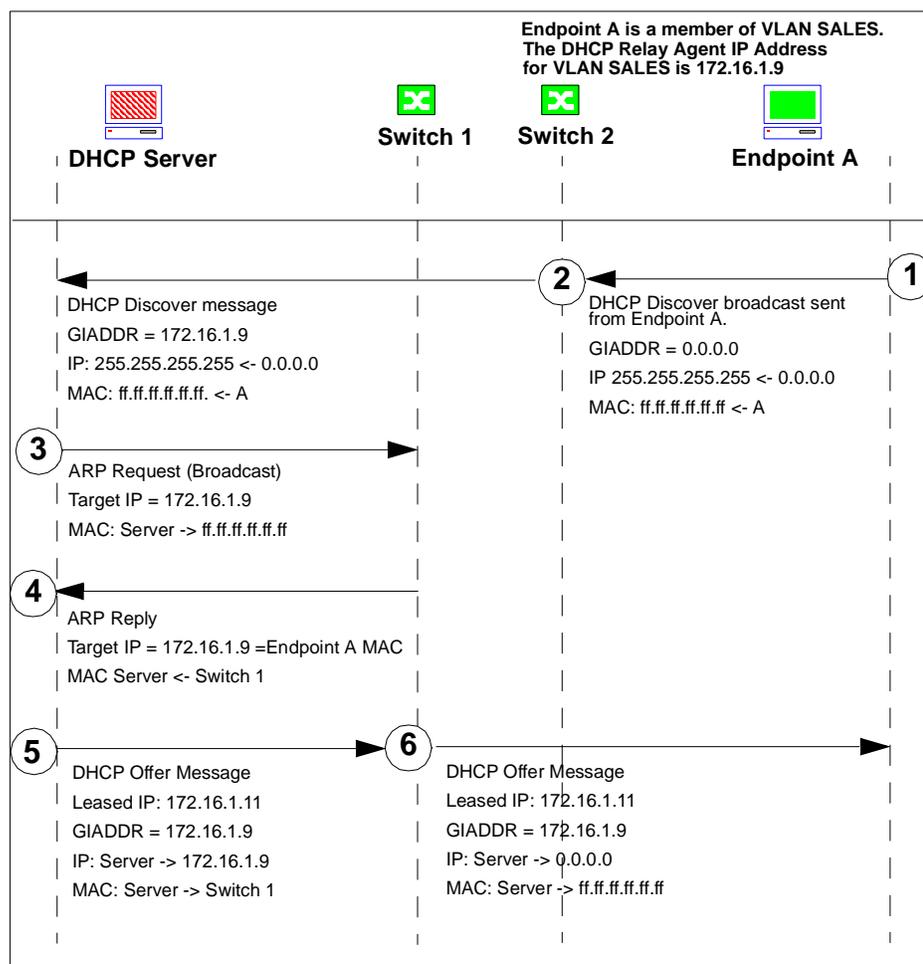
Mapping Scopes to VLANs

Scopes are mapped to VLANs using the SPECTRUM VLAN Manager user interface. More specifically, by entering a scope's DHCP Relay Agent IP address in the General VLAN Properties DHCP Relay Agent IP Address field. The DHCP Relay Agent IP address for a scope is the address entered into the Exclusions field. The SALES scope is mapped to the SALES VLAN by entering 172.16.1.9 into the SALES VLAN General Properties DHCP Relay Agent IP Address field. The MIS scope is mapped to the MIS VLAN by entering 172.16.2.9 into the MIS VLAN General Properties DHCP Relay Agent IP Address field.

DHCP Operation

Figure B-3 shows the packet flow of the DHCP IP address request between Endpoint A and the DHCP server with the assistance of the SecureFast DHCP Relay Agent. A description of each step follows the figure.

Figure B-3. DHCP Packet Flow

**Step 1**

A DHCP Discover broadcast sent from Endpoint A

Step 2

Switch 2 intercepts the DHCP discover broadcast. Since this is a DHCP message, the switch determines Endpoint A's VLAN mapping by checking the VLAN mapped to Endpoint A's port. Since Endpoint A is a member of VLAN SALES, the switch inserts the GIADDR (Gateway Internet Address) of 172.16.1.9. This address is the DHCP Relay Agent IP address. The switch then floods the Discover message Endpoint A's VLAN (SALES).

Step 3

Once the DHCP Discover message is seen by the DHCP server, remember, the server has to be in the same VLAN as Endpoint A, the server allocates an IP address from scope SALES because the GIADDR of 172.16.1.9 identifies the request as belonging to that scope. Since this is considered a remote scope, the server is required to send its DHCP Offer message directly to the DHCP Relay Agent indicated by the GIADDR field. If required, the server will ARP for the GIADDR first to resolve the MAC to IP mappings needed.

Step 4

The local switch to the DHCP server will intercept the ARP broadcast frame from the server. The switch is the relay agent so it will generate an ARP response sending its own MAC address.

Step5

The DHCP server will then send its DHCP offer to the GIADDR of 172.16.1.9. Since the packet is destined to the MAC address of the local switch, that switch will receive this packet and process it as a DHCP message.

Step 6

The local switch to the server (Switch 1) will modify the MAC and IP destinations to be broadcasts. Once the packet is converted back to broadcast form, the packet will be flooded to Endpoint A's VLAN SALES to complete the initial process.

The DHCP Request and Acknowledge messages will repeat the same process to finalize the DHCP parameter allocation. This mechanism allows for endpoints in VLAN SALES to draw addresses from the scope defined for their subnet while endpoints in other VLANs can draw addresses from other scopes mapped to their respective VLANs. This effectively allows a mapping between scopes and VLANs using a shared DHCP server.

DHCP When More Than Eight Scopes are Serviced by a Single DHCP Server

In a network environment where a single DHCP server is used to service more than eight address scopes, Advanced VLAN Policy must be configured through SPECTRUM VLAN Manager. Advanced VLAN Policy allows a network administrator to overcome the limitation from previous SecureFast releases that a user may be a member of up to (8) VLANs. This new policy feature allows complete control over flooding and connections between any pair of VLANs, thus allowing DHCP broadcast messages from users of many different VLANs to be flooded to the DHCP Server VLAN. Refer to [Chapter 15, *Advanced VLAN Policy*](#).

To accommodate this network environment, the network administrator must:

1. Define address scopes on the DHCP server
2. Logically map address scopes to appropriate VLANs

3. Configure Advanced VLAN Policy to allow DHCP broadcast messages to be delivered to the DHCP server.

The following sections provide details for these activities.

Define Address Scopes

Define address scopes on the DHCP server. You define one address scope per VLAN. Below is an example of a DHCP server configuration which includes a total of nine address scopes, including one defined for the “BASE” VLAN.

BASE	
Starting IP Address:	172.16.1.9
Ending IP Address:	172.16.1.254
Network Mask:	255.255.255.0
Exclusions:	172.16.1.9
Other Parameters:	SwitchedNetworkFlag=1

SALES	
Starting IP Address:	172.16.2.9
Ending IP Address:	172.16.2.254
Network Mask:	255.255.255.0
Exclusions:	172.16.2.9
Other Parameters:	SwitchedNetworkFlag=1

ENGINEERING	
Starting IP Address:	172.16.3.9
Ending IP Address:	172.16.3.254
Network Mask:	255.255.255.0
Exclusions:	172.16.3.9
Other Parameters:	SwitchedNetworkFlag=1

PAYROLL	
Starting IP Address:	172.16.4.9
Ending IP Address:	172.16.4.254
Network Mask:	255.255.255.0
Exclusions:	172.16.4.9
Other Parameters:	SwitchedNetworkFlag=1

MARKETING	
Starting IP Address:	172.16.5.9
Ending IP Address:	172.16.5.254
Network Mask:	255.255.255.0
Exclusions:	172.16.5.9
Other Parameters:	SwitchedNetworkFlag=1

MANUFACTURING	
Starting IP Address:	172.16.6.9
Ending IP Address:	172.16.6.254
Network Mask:	255.255.255.0
Exclusions:	172.16.6.9
Other Parameters:	SwitchedNetworkFlag=1

PERSONNEL	
Starting IP Address:	172.16.7.9
Ending IP Address:	172.16.7.254
Network Mask:	255.255.255.0

PERSONNEL	
Exclusions:	172.16.7.9
Other Parameters:	SwitchedNetworkFlag=1

SUPPORT	
Starting IP Address:	172.16.8.9
Ending IP Address:	172.16.8.254
Network Mask:	255.255.255.0
Exclusions:	172.16.8.9
Other Parameters:	SwitchedNetworkFlag=1

ADMINISTRATION	
Starting IP Address:	172.16.9.9
Ending IP Address:	172.16.9.254
Network Mask:	255.255.255.0
Exclusions:	172.16.9.9
Other Parameters:	SwitchedNetworkFlag=1

Map Scopes to VLANs

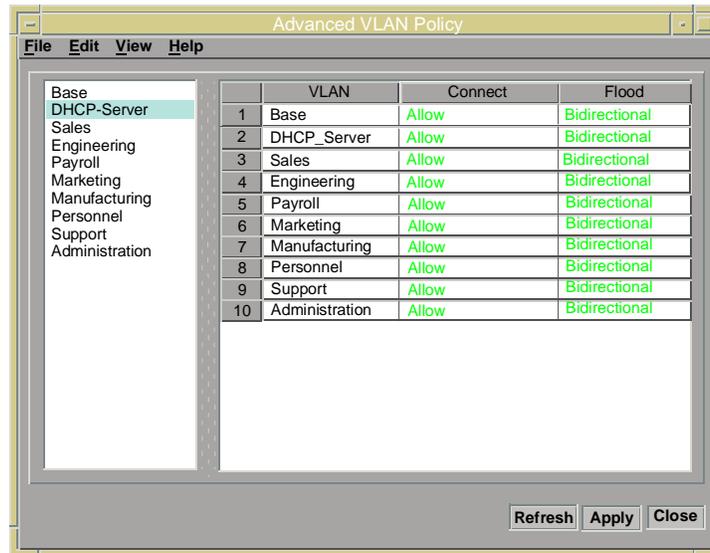
Logically map DHCP address scopes to VLANs. In this example, the network administrator associates the 172.16.1.x network to the BASE VLAN, the 172.16.2.x network to the SALES VLAN, etc. You do this by reserving a DHCP relay address within each network and assigning it to the appropriate VLAN. Each relay address must be unique and should be excluded from the applicable DHCP scope (see the above DHCP configuration example). As discussed earlier in this document, the DHCP relay addresses are to be used by the switches when modifying the GIADDR parameter of any DHCP Discover or Request received on a given VLAN.

Configure Advanced VLAN Policy

Configure Advanced VLAN Policy to allow flooding to be enabled between all DHCP client VLANs and the DHCP server VLAN. In an Advanced VLAN Policy configuration consisting of a single DHCP Server allocating addresses for nine VLANs, including the

“BASE” VLAN, the DHCP server is placed in its own VLAN which for the purposes of this example is named the DHCP_Server VLAN. Through the Advanced VLAN Policy configuration screen, the “**Flood**” and “**Connect**” attributes should be enabled with the “**Flood**” attribute set for “**Bi-directional**” between the DHCP_Server VLAN and each VLAN representing an address scope.

Figure B-4. Advanced VLAN Policy Configuration



You are now ready to map VLANs to ports, allowing port level control over DHCP address assignment in an enterprise switch network, using a single DHCP server.

A

- AAL [A-1](#)
- access port icon, the
 - tasks [3-23](#)
- Access Ports [1-8](#)
- acronyms [A-1](#)
- add alias [3-10](#), [10-10](#)
- add tap
 - connection table [11-11](#)
- add users
 - how to in VLANs [3-27](#)
- address interception
 - as a switch function [1-8](#)
- admin status
 - Connection table call list [11-8](#)
- Administrative Type [7-13](#), [8-5](#)
- advanced graphical user interface [1-4](#)
- Advanced Tab [8-4](#)
- Advanced VLAN Policy [9-3](#), [15-1](#)
 - fine tuning [15-11](#)
 - launching [15-2](#)
 - main window [15-3](#)
 - menus [15-4](#)
 - sorting [15-13](#), [15-14](#), [15-15](#)
- advanced VLAN policy
 - launching [15-2](#)
 - overview [15-1](#)
 - using [15-3](#)
- aging configuration [3-10](#)
- aging description [11-14](#)
- AMI [A-1](#)
- AMR [A-1](#)
 - AppleTalk [9-24](#)
 - behavior [9-21](#)
 - BPDU [9-25](#)
 - creating using the wizard [6-6](#)
 - DECNet [9-25](#)
 - displaying AMR VLANs [9-28](#), [12-2](#)
 - enabling [9-26](#)
 - using Domain Properties [9-27](#)
 - using the wizard [9-26](#)
 - IP-Subnet [9-21](#)
 - IPX RIP/SAP [9-22](#)

- NetBios [9-21](#)
- overview [1-6](#), [9-19](#)
- types [9-20](#)
- VINES [9-25](#)
- AppleTalk [7-10](#)
 - enabling and disabling domain wide [6-41](#)
- AppleTalk AMR Islands [7-10](#)
- ARP [A-1](#)
- assign default VLAN [3-9](#), [9-18](#)
- assignment of VLANs [1-8](#)
- ATM [A-1](#)
- automated
 - changes [1-4](#)
 - moves [1-4](#)
 - See also* user
 - adds
 - automated [1-4](#)
 - user adds [1-4](#)

B

- bandwidth (MBPS)
 - Switch icon pop-up menu [13-10](#)
- block resolve
 - launching [6-32](#)
- Blockable Status [10-8](#)
- boradcasts
 - direction all through one port [9-2](#)
- BPDU [A-1](#)
- broadcast [A-4](#)
- broadcast traffic
 - control [1-4](#)
- broadcasts
 - troubleshooting [9-2](#)
- BUS [A-1](#)

C

- call processing
 - administrative VLAN switch [1-8](#)
- call tap
 - adding [11-10](#)
 - adding/releasing [11-9](#)

-
- enabling and disabling domain widw [6-41](#)
 - modifying [11-12](#)
 - refreshing the data in the table [11-10](#)
 - releasing [11-11](#)
 - CAUTION
 - delete switch [7-3](#)
 - flooding "off" [9-3, 9-7](#)
 - Choosing Commands [3-14](#)
 - circle mode
 - domain topology [13-7](#)
 - CLI [A-1](#)
 - closing
 - Topology view->File [13-3](#)
 - closing windows
 - VLAN Manager [3-17](#)
 - collapse all
 - from View->VLAN menu [3-12](#)
 - collapsing elements [3-26](#)
 - communications
 - VLANServer [2-22](#)
 - compatible with VLAN SF features
 - routers [1-5](#)
 - switches [1-5](#)
 - compatible. 1-4
 - See also* VLAN Manager compatibility [1-4](#)
 - configuration menu
 - Connection table [11-16](#)
 - configure VLAN domain
 - how to [6-19, 6-21, 6-39](#)
 - configure VLANServer
 - functions [2-12](#)
 - how to [2-22](#)
 - configure VLANServer performance
 - how to [2-21](#)
 - Connection Configuration
 - Age Pass Count [11-17](#)
 - Age Pass Delta [11-17](#)
 - Age Pass in Progress [11-17](#)
 - editable attributes [11-17](#)
 - High Mark
 - aging connection [11-17](#)
 - how to edit attributes [11-18](#)
 - Last Pass Time [11-17](#)
 - Number To Age [11-17](#)
 - Present Capacity [11-17](#)
 - Time Since Last Pass [11-17](#)
 - Connection Configuration Button
 - Close [11-18](#)
 - Force Age Full [11-18](#)
 - Force Age Partial [11-17](#)
 - OK [11-17](#)
 - connection configuration buttons [11-17](#)
 - connection configuration fields [11-17](#)
 - Connection Table
 - Directory pop-up menu [10-18](#)
 - Directory window->View [3-12, 10-15](#)
 - connection table
 - complete query [11-2](#)
 - functions [11-7](#)
 - information fields [11-7](#)
 - menus [11-5](#)
 - partial query [11-3](#)
 - Preference type [5-1](#)
 - Connection table preferences
 - functions [5-6](#)
 - connection table preferences
 - from SecureFast VLAN main window [5-6](#)
 - from the connection table window [5-6](#)
 - functions [5-6](#)
 - set up [5-7](#)
 - connection-oriented [1-8](#)
 - control menu
 - functions [2-11](#)
 - Control Panel [2-9, 2-23](#)
 - control panel
 - configure menu functions [2-12](#)
 - exit button functions [2-14](#)
 - file menu functions [2-10](#)
 - pull-down menu functions [2-10](#)
 - control status
 - Connection table call list [11-8](#)
 - Create
 - Wild Card VLAN [9-2](#)
 - create
 - a new VLAN [3-15](#)
 - from Edit menu [3-9, 3-10](#)
 - from File->Domain menu [3-8](#)
 - Create User
 - from Directory window->Edit [10-15](#)
 - creating new switches
 - how to [10-1](#)
 - creating users [10-25](#)
 - CsProcdDb.k [2-24](#)
- ## D
- daemon [2-23, A-7](#)
 - database dialog box
 - directory list [2-16](#)

- files window functions 2-16
- filter field functions 2-16
- DCM A-1
- Default VLAN 8-5
- default VLAN
 - Ports list 7-14
- default zoom
 - topology preferences 5-4, 5-5
- delete
 - defined 9-4
 - VLAN domains, how to 6-17
- Delete Users
 - Directory pop-up menu 10-18
 - Directory window->Edit 10-15
- destination address 1-8
- destination alias (network address)
 - Connection table call list 11-7
- details
 - from View menu->Switch menu 3-12
 - from View->VLAN menu 3-12
- DHCP 3-21, 7-10
 - client tagging
 - enabling and disabling domain wide 6-41
- dhcp
 - description 3-21
- DHCP Server Islands 7-10
- DHCP Server Single Flood 6-24
- DHCP server VLAN 6-23
- DHCP Server VLAN Islands 6-23
- dialog box 3-16
 - working with 3-16
- dialog windows *See* dialog box 3-4
- Directory
 - Adding/Removing a User Alias 10-18
 - Creating a User 10-16
 - Deleting a User 10-17
 - Editing User Properties 10-17
 - Menus 10-15
 - Pop-up Menu 10-18
 - Removing Users from a Switch 10-17
 - Users List 10-16
 - Using 10-14
- directory
 - domain information 3-13
- Directory pop-up menu 10-17
 - functions 10-18
- Directory window
 - functions 10-14
- Disabled 10-47

- Discover
 - how to use 6-12
- discover
 - from File->Domain menu 3-7
- discovery ELAN configuration 14-31
- displaying switch details, how to 7-11
- DNS A-1
- documentation
 - User's Guide 3-14
- Domain 6-41
- domain
 - domain maintenance 3-7
 - opens maintenance menu 3-7
 - overview 1-4
 - purpose 6-1
- Domain Details window 6-30
- Domain Properties 6-18
 - AMR 6-21
 - General 6-19
 - IP Address Learning 6-24
 - Services 6-22
 - User Persistence 6-26
- Domain Wide Services 6-41
- download
 - SecureFast firmware 7-15
- dragging and dropping elements 3-27
- duplicate addresses 10-19
- duplicate MAC addresses
 - enabling and disabling 10-8
- duplicate user MAC addresses 10-2
- duration
 - Connection table call list 11-8

E

- edit
 - Directory menu 10-15
 - menu commands 10-15
- edit menu 3-8, 3-13
- editing window panes
 - collapsing elements 3-26
 - expanding elements 3-26
- ELAN A-1
- embedded layer 3 virtual routing 1-8
- ending a VLAN manager client session 2-8
- endpoint 1-8, A-4
 - communication between 1-4
 - directly attached 1-4
 - information, discovery of 1-9

- membership criteria [1-5](#)
 - via access ports [1-8](#)
- error/cursor location information [3-28](#)
- Ethernet
 - independent operation [1-5](#)
- exit
 - file menu
 - connection table [11-6](#)
 - VLAN control panel menu [2-11](#)
- exiting
 - options [3-7](#)
- Exiting VLAN Manager [2-8](#)
- expand all
 - from View->VLAN menu [3-12](#)
- expanding. *See* editing window panes
 - expanding elements [3-26](#)
- explode
 - Connection table [11-6](#)

F

- fast buttons
 - control panel functions [2-12](#)
- FDDI [A-1](#)
- File
 - close Directoy [10-15](#)
 - Directory menu [10-15](#)
- File menu
 - connection table [11-5](#)
- file menu
 - domain topology [13-3](#)
- filter
 - functions [6-43](#), [7-15](#)
 - text box [6-18](#), [13-4](#)
- flood suppression
 - enabling and disabling domain wide [6-41](#)
- flooding [A-4](#)
- FNB [A-1](#)
- FPS [A-1](#)
- from Edit menu [3-9](#), [3-10](#)
- functional group
 - members on LAN segment [1-2](#)

G

- General Tab [8-3](#)
- global
 - Preference type [5-1](#)

- global preferences
 - enable dialogs [5-2](#)
 - enable tool tips [5-1](#)
 - enable toolbar [5-1](#)
 - enable warning beeps [5-2](#)
 - how to set up [5-2](#), [5-4](#)
 - VLAN windows [5-1](#), [5-3](#)
- graphical command tool icons
 - VLAN Manager [3-15](#)
- Graphical User Interface [A-5](#)
- graphical user interface
 - VLAN Manager [1-9](#)
- group users
 - how to [9-1](#)
 - VLAN management [9-1](#)
- GUI [A-1](#)

H

- host
 - user endpoint name VLAN details [10-16](#)
 - User list
 - endpoint name [9-10](#)

I

- icon
 - access port [3-23](#)
 - INB port [3-23](#)
 - network address [3-21](#), [3-24](#)
 - network port [3-23](#)
 - user [3-24](#)
- ID
 - Ports list [7-13](#)
- IGMP [A-1](#)
- import [10-23](#)
 - using [10-24](#)
- in port
 - Connection table call list [11-8](#)
- INB [A-1](#)
- INB port icon
 - switch window pane element [3-23](#)
- independent operation
 - SF VLAN features [1-5](#)
- initialize to legacy database
 - VLAN control panel menu [2-11](#)
- initializing VLANServer database [2-20](#)
- install
 - VLAN Manager [xv](#)

Internet Packet Exchange [A-5](#)
Internet Protocol [A-5](#)
inter-VLAN communication [1-4](#)
 requirements [9-3, 9-7](#)
IP [A-2](#)
IP address [A-5](#)
IP addresses [1-2](#)
IP multicast
 enabling [6-7, 6-22](#)
 overview [1-6, 3-19, 12-1](#)
 properties [12-4](#)
IPX [A-2](#)
ISO [A-2](#)

K

key icon
 logical window pane element [3-21](#)

L

LAN [A-2](#)
LANE [A-2](#)
launch [6-1](#)
 VLANserver [1-9](#)
layer 3
 routing [1-4](#)
 switching [1-4](#)
layout
 Topology view->View [13-3](#)
LEC [A-2](#)
LECS [A-2](#)
Legacy Network [A-5](#)
LES [A-2](#)
limiting broadcasts [1-3](#)
Link State Protocol [6-31, 7-13](#)
Links table
 Bandwidth (Mbps) [13-11](#)
 Local Port [13-11](#)
 Neighbor IP [13-11](#)
 Neighbor Name [13-11](#)
 Status [13-11](#)
 Switch icon pop-up menu [13-11](#)
 Type [13-11](#)
live links [xvii](#)
load balancing
 redundant paths [1-4](#)
Local Area Network [A-6](#)

local directory
 endpoint MAC addresses [1-8](#)
local port
 Switch icon popup menu [13-10](#)
lock
 physical window pane element [3-23](#)
Lock Users to Default VLAN [8-5](#)
logical window pane [3-18](#)

M

MAC [A-2, A-5](#)
MAC Address [7-13](#)
MAC address [A-6](#)
MAC addresses
 duplicate
 enabling and disabling [10-8](#)
makeinstdb [2-24](#)
manual workstation configuration [1-2](#)
MCSP [A-2](#)
Media Type [8-4](#)
membership administration [1-4](#)
membership criteria
 VLAN [1-5](#)
menu
 commands [3-14](#)
 pull-down [3-6](#)
 submenus [3-6](#)
MIB [A-2](#)
mode
 Ports list [7-14](#)
models
 actual network devices [1-10, A-8](#)
modes of operation
 VLAN firewalls [1-3](#)
monitor
 network [1-4](#)
moves [1-2](#)
 member [1-2](#)
Multicast
 Allow [6-22](#)
 Allow all multicast senders [6-23](#)
 Enable [6-7](#)
 Enable optimization [6-8, 6-23](#)
 Enable scoping [6-7, 6-23](#)
multicast [A-5](#)
 enabling and disabling domain wide [6-41](#)
Multicast Tab [8-6](#)

multiple user interfaces
 attached to single VLANserver 1-9
Multicast
 setting optimization threshold 6-8, 6-23

N

neighbor IP
 Switch icon pop-up menu 13-10
neighbor name
 Switch icon pop-up menu 13-10
NetBEUI Service
 enabling and disabling domain wide 6-41
NetBIOS over IP Service
 enabling and disabling domain wide 6-41
NetBIOS over IPX Service
 enabling and disabling domain wide 6-41
network
 device models 1-10, A-8
 problems 1-2
network address
 User list 9-10, 10-16
network address icon
 physical window pane element 3-21, 3-24
network connections
 Switch icon pop-up menu 13-10
Network Port A-6
network port icon
 switch window pane element 3-23
network protocols
 operation independent of 1-5
network type
 User list 9-10, 10-16
NIS A-2
NNI A-2
No VLANServer to talk to 2-5
note
 domain creation w/wizard 6-2
 domain name server 6-3
 dragging a switch to target VLAN 9-14
 dragging VLANs 9-16
 multiple network addresses 9-11
 network without domain name server 6-13
 polling interval
 Configure 6-20
 Create 6-17
 Discover 6-14
 View->Directory info 9-10
Notice iii

Novell Service
 enabling and disabling domain wide 6-41
NVRAM A-2

O

off
 unresolved destination 9-3, 9-7
on
 unresolved destination 9-3, 9-7
On-Line Backup
 typical save times 16-2
online backup 3-7
open
 from File->Domain menu 3-7
open host communication 1-4
open mode
 configuring user 1-3
Open Shortest Path First
 enabling on router port 8-45
Operational Type 7-13, 8-5
OSI A-2
OSI model A-5
OSPF A-2
 enabling and disabling on router ports 8-11
OSPF Multicast
 enabling on router as opposed to OSPF
 Broadcast Control 8-46
OSPF multicast
 disabling on router port 8-46
 enabling on router port 8-45
out port
 Connection table call list 11-8

P

packet A-6
path trace 11-12
path trace preferences
 functions 5-5
 set up 5-6
performance tuning
 VLANServer 2-21
permanent virtual circuits
 description 14-1
 managing VLANs 14-2
 creating an end-to-end PVC 14-4
 creating PVC/VCC connections 14-2

physical address
 User list 9-10, 10-16
 physical window pane 3-21
 plug and play ease of use
 SF VLAN features 1-4
 poll switch 3-10, 7-16
 port
 adding a router to 8-11
 call tap 11-11
 deleting router configurations from 8-11
 directing all broadcasts through 9-2
 dragging 3-27
 locking/unlocking 8-24
 maintenance 3-10
 making it a member of all VLANs 9-2
 modify routers on 8-11
 properties 8-3
 selected switch 7-11
 setting to be redundant 8-25
 User list 9-10, 10-16
 port name
 Ports list 7-13
 port properties 8-3
 Advanced tab 8-4
 General tab 8-3
 Multicast tab 8-6
 Redundant tab 8-7
 Restrictions tab 8-8
 Ports List
 functions 7-13
 Preferences
 customizing VLAN windows 5-1
 Topology view->File 13-3
 preferences
 connection table 5-6
 define settings 3-7
 description 5-1
 global 5-1
 main 5-3
 amr user alias filter 5-3
 multicast user alias filter 5-3
 switch sort 5-3
 path trace 5-5
 topology view 5-4
 preferences...
 connection table->File 11-5
 process control
 buttons 2-11
 processd 2-23
 properties
 alias 10-12
 general 10-13
 restrictions 10-13
 domain 6-18
 amr 6-21
 general 6-19
 services 6-22
 user persistence 6-26
 port 8-3
 advanced 8-4
 general 8-3
 multicast 8-6
 redundant 8-7, 8-37
 restrictions 8-8
 User Count 8-4
 VLAN 9-8
 smart 3-8
 switch 7-4
 general 7-5
 multicast 7-7
 user 10-6
 restrictions 10-9
 VLAN membership 10-9
 VLAN 9-6
 Provision
 functions 11-18
 provision 3-10
 provisioned redundant access 8-32
 PVC A-2
 permanent Virtual Circuit 11-18
 PVID A-2

R
 radial layout 13-5
 RAM A-2
 rebooting
 all switches in a domain 6-33
 an individual switch 7-17
 rebooting an individual switch 7-17
 reconfigure switch 7-16
 red buttons
 VLANServer 2-12
 redirect port 8-39
 redundant access
 enabling and disabling domain wide 6-41
 redundant access ports 3-11, 8-25
 redundant paths 1-4
 redundant server
 enabling Self ARP Packet Learning 8-5

- Redundant Tab [8-7](#)
- refresh switch [3-10](#)
- Reinitializing processd [2-23](#)
- releasing a call
 - how to [11-14](#)
- remove Users from Switch
 - Directory pop-up menu [10-18](#)
 - Directory window->Edit [10-15](#)
- repeater [A-7](#)
- replace switch [7-18](#)
- replacing a switch [7-18](#)
- rerouting
 - automatic [1-4](#)
- resolution
 - VLAN switch [1-8](#)
- resolve [1-8](#)
- restore database
 - VLAN control panel menu [2-11](#)
- restore VLANServer database
 - how to [2-18](#)
- restoring VLANServer database [2-18](#)
 - from previously saved database [2-18, 2-20](#)
 - initializing to legacy [2-20](#)
- Restricted Rights Notice [iv](#)
- restrictions [8-42](#)
- Restrictions Tab [8-8](#)
- RIP [A-2](#)
- router [A-7](#)
 - inter-VLAN communication [1-4](#)
- router connections
 - Connection table [11-6](#)
 - Connection Table Preferences [5-7](#)
- router port configuration [8-9](#)
- Router Wizard
 - [8-10](#)
 - domain information [8-11](#)
 - enabling and disabling OSPF and VRRP [8-11](#)
 - internal subnets [8-11](#)
 - launching [8-10](#)
 - port information [8-11](#)
 - router list and router settings [8-11](#)
- space delimited [10-20](#)
 - using [10-21](#)
- save database
 - VLAN control panel menu [2-11](#)
- saving the VLANServer database
 - how to [2-15](#)
- scroll bars
 - description of [3-24](#)
- SCS [A-2](#)
- search
 - functions [6-43, 7-15](#)
- search/filter
 - features [7-11](#)
 - for a port [6-43, 7-15](#)
 - how to use [9-12, 10-19](#)
 - User Directory [10-19](#)
 - user management [10-14](#)
- search/filter button
 - functions [9-12, 10-19](#)
- secure mode [1-3](#)
 - configuring user [1-4](#)
 - defined [9-3, 9-7](#)
- SecureFast VLAN manager
 - link status window
 - functions [13-12](#)
- security
 - adding a user [4-2, 4-3](#)
 - configuration [4-2](#)
 - configuring [4-1](#)
 - deleting a host [4-3](#)
 - deleting a user [4-3](#)
 - user permissions [4-1](#)
 - user privileges [3-7](#)
 - VLAN [1-3](#)
- seed switch [A-7](#)
 - function [6-1](#)
- select file to save database dialog box
 - functions [2-16](#)
- select switch and port...
 - display dialog box [11-11](#)
- select VLAN dialog box, the [13-4](#)
- selecting elements
 - drag and drop [3-27](#)
- Self ARP Packet Learning [7-14](#)
 - enabling and disabling [8-5](#)
- set/unset router port [3-11](#)
- SFPS [A-2](#)
- SFS Version [6-31, 7-12](#)
- shared links [13-12](#)
- Simple Network Management Protocol [A-7](#)

- smart hub [A-5](#)
- SNMP [A-2](#)
 - with VLAN Manager [1-9](#)
- software intervention [1-8](#)
- sort
 - Connection table, functions [11-6](#)
 - view menu
 - connection table [11-6](#)
- sort feature
 - how to use [11-9](#)
- source address [1-8](#)
- source alias (network address)
 - Connection table call list [11-7](#)
- source blocker
 - description [6-32](#)
 - enabling and disabling domain wide [6-41](#)
 - launching [6-32](#)
- source blocking [10-8](#)
- Source Configuration Table [10-8](#)
- Spanning Tree [6-32, 7-13](#)
- SPMA [A-2](#)
- SRN [A-2](#)
- stand-alone application
 - VLAN Manager [xv](#)
- start VLAN Manager
 - functions [2-11](#)
- start VLANServer
 - functions [2-11](#)
- starting
 - Control Panel [2-1](#)
 - VLAN Manager Client [2-4](#)
 - VLAN Manager Client Using the Autostart Feature [2-6](#)
 - VLANServer Using the Autostart Feature [2-3](#)
- Statistics [11-17](#)
- status
 - Ports list [7-13](#)
 - Switch icon pop-up menu [13-10](#)
- status field
 - functions [2-14](#)
- stopping
 - VLANServer [2-9](#)
- stopping VLANServer
 - from command line [2-9](#)
 - from the control panel [2-9](#)
- STP [A-2](#)
- subnet membership [1-2](#)
- subnets
 - on router ports [8-11](#)
- SVC [A-2](#)
- Switch [A-7](#)
- switch
 - address resolution [1-8](#)
 - broadcast interception [1-8](#)
 - call processing [1-8](#)
 - call tap [11-11](#)
 - configuring protocols [7-20](#)
 - created [1-4](#)
 - delete from VLAN domain [7-3](#)
 - MAC-layer [1-8](#)
 - maintenance [3-10](#)
 - polling [7-16](#)
 - submenu [3-12](#)
 - synchronization [7-16](#)
 - User list [9-10, 10-16](#)
- switch details
 - Switch icon pop-up menu [13-10](#)
- Switch Details window
 - community name [7-12](#)
 - description [6-30, 7-12](#)
 - general information [7-11](#)
 - IP address [6-31, 7-12](#)
 - MAC address [6-31, 7-13](#)
 - switch [6-30, 7-12](#)
 - switch status [6-31, 7-13](#)
 - uptime [6-31, 7-13](#)
- switch icon [3-22](#)
 - functions [13-9](#)
 - tasks [3-22, 3-23](#)
- switch icon pop-up menu
 - functions [13-10](#)
- switch management
 - tasks [7-1](#)
- switch ports [1-3](#)
- switch users [3-12](#)
 - Switch icon pop-up menu [13-10](#)
- switched virtual circuits
 - description [14-1](#)
 - managing VLANs [14-17](#)
 - attached ATM endpoints [14-20](#)
 - backup ELANs [14-19](#)
 - creating additional ELANs [14-28](#)
 - how to [14-20](#)
 - initialization and configuration [14-17](#)
 - network scalability [14-25](#)
 - overview [14-17](#)

T

- tabbed folder [3-5](#)
- tabbed folders *See* dialog box [3-5](#)
- tap
 - destination [11-10](#)
 - point [11-11](#)
 - source [11-10](#)
- tapped connections [3-13](#)
- tasks [3-20](#)
- TFTP [A-2](#)
- TFTP download
 - functions [2-12](#)
- Threshold, multicast optimization [6-8, 6-23](#)
- throughput
 - SF VLAN features [1-4](#)
- toggle
 - enable/disable [3-9](#)
 - lock/unlock [3-10](#)
 - open/secure [3-9](#)
- tool tips
 - VLAN Manager [3-15](#)
- tools menu
 - ATM PVC [3-13](#)
 - discovery ELAN configuration [3-14](#)
 - duplicate addresses [3-12](#)
 - redirect port [3-13](#)
 - TFTP download [3-13](#)
- topology
 - from View menu [3-13](#)
- topology display area
 - functions [13-9](#)
- topology filter
 - how to set [13-4, 13-5](#)
- Topology View
 - filtering for uplink switches [13-5](#)
- topology view
 - accessing [13-1](#)
 - display area [13-1](#)
 - displays [13-5](#)
 - functions [13-1](#)
 - Preference type [5-1](#)
 - status bar [13-1](#)
- topology view menu bar
 - functions [13-2](#)
- topology view preferences
 - functions [5-4](#)
 - how to set up [5-5, 5-6](#)
 - set up [5-4, 5-5](#)

- total switches
 - displayed [3-21](#)
- Trademarks [iii](#)
- transfer
 - group member [1-3](#)
- troubleshooting
 - broadcasts [9-2](#)
- type
 - Connection table call list [11-8](#)
 - Switch icon pop-up menu [13-10](#)

U

- UNI [A-3](#)
- unicast [A-7](#)
- UNIX
 - starting the control panel [2-1](#)
- update
 - Connection table [11-6](#)
- upgrade
 - SecureFast firmware [7-15](#)
- uplink operational checks [6-37](#)
- Uplink State [6-31, 7-13](#)
- Uplink Switches
 - filtering for in topology view [13-5](#)
- uplink switching
 - configuring [6-35](#)
 - overview [6-34](#)
- user
 - endpoint name [10-16](#)
 - ID [2-4](#)
 - maintenance [3-9, 3-10](#)
 - modifying information
 - how to [9-12](#)
 - properties [10-6](#)
 - restricting [8-42, 10-25](#)
 - User list [9-10](#)
- User Display
 - Connection Table Preferences [5-6](#)
- user icon
 - logical window pane element [3-20](#)
 - physical window pane element [3-24](#)
- user interface locally
 - running [1-9](#)
- user interface remotely
 - running [1-9](#)
- User menu [10-14](#)
- user mobility
 - enabling and disabling domain wide [6-41](#)

user operations
 launched from menu bar/popup menu 10-14

User Persistence 6-26
 disabling for all new users 6-28
 disabling for users in a domain 6-29
 enabling for all new users 6-28
 enabling for individual user 10-8
 enabling for users in a domain 6-27

User Port A-4

users
 criteria-based groups 9-1
 delete 10-17
 delete, how to 10-5
 discover before network connection 10-1
 managing from Directory window 10-1
 remove from switch
 directory pop-up menu 10-17
 remove, how to 10-3, 10-4

users (#)
 Ports list 7-14

Users fields
 functions 9-10, 10-16

using search/filter 7-15

V

VCC A-3

VCI A-3

view
 Directory menu 10-15
 menu commands 10-15

view layout
 topology preferences 5-4

view menu
 commands 3-11
 Connection table, functions 11-6
 domain topologies, selections 13-3
 topology view 13-3

Viewing Connection Information 10-14

violations
 description 6-32
 remedying 10-32

violations table
 launching 6-33

virtual 1-1

Virtual Router Redundancy Protocol
 enabling on router port 8-47

virtual workgroups 1-2

Virus Disclaimer iii

VLAN 1-1, A-3

administered manually 1-9

administration 4-1, 5-1, 6-1, 7-1, 8-1, 9-1, 10-1, 11-1, 13-1, 16-1
 adding switch ports to VLAN 9-14
 adding switch ports to VLANs 9-17
 creating new switches 7-2
 creating VLAN 9-2
 deleting entire VLAN 9-4
 displaying VLAN details 9-9
 listing all users 10-14
 removing switches 7-3
 switch discovery 6-12, 6-16, 6-33

advantages of 1-2

AMR 9-20

assigning port membership 9-15
 selected users 9-17

assigning switch membership 9-14

change status/policy 9-12

delete 9-1, 9-4

detail window 9-9

details window, functions 9-9

display 9-1

domain 1-4, 1-8, 1-9, 6-1

dynamic management 1-2

flooding, selections 9-3

icon 3-20

implementation 1-3

IP multicast 1-6, 3-19, 12-1

manager main window 9-9

member 1-4

monitor
 switches 1-4

network 1-4

network security 1-3

policy, selections 9-3

properties 9-6

restricted communication 9-3, 9-7

search/filter feature 9-9

segmenting networks 1-3

status, selections 9-2

user fields, modifications 9-9

user membership
 automatic 9-13

verification of 1-8

VLAN database
 restore VLAN database 2-18

VLAN details window
 flooding 9-10
 name 9-9
 policy 9-10

-
- status [9-9](#)
 - total entries [9-10](#)
 - users [9-10](#)
 - VLAN Manager [1-2, 1-4](#)
 - client functions [1-9](#)
 - information windows [3-3](#)
 - network maintenance [1-8](#)
 - shutdown [2-8](#)
 - starting from control panel [2-5](#)
 - unlisted connection [2-5](#)
 - use of [1-4](#)
 - use of SNMP commands [1-9](#)
 - window [3-1](#)
 - File menu [3-6](#)
 - logical pane [3-2](#)
 - Menu Bar [3-1](#)
 - physical pane [3-2](#)
 - Scroll Bars [3-2](#)
 - Status Bar [3-2](#)
 - Title Bar [3-1](#)
 - Tool Bar [3-2](#)
 - window panes, adjusting [3-17](#)
 - wizard [6-1](#)
 - VLAN Manager compatibility
 - with Cabletron Workgroup switches [1-4](#)
 - VLAN Manager Documentation
 - Installation Guide [3-14](#)
 - VLAN Manager graphical user interface
 - launching [1-9](#)
 - VLAN Manager menus
 - administration commands [3-6](#)
 - VLAN Manager software
 - client/server model [1-9](#)
 - VLAN MANAGER STATUS
 - indicator [3-2](#)
 - VLAN membership [1-2](#)
 - assigned by dragging [9-16](#)
 - configuration [1-4](#)
 - VLAN submenu [3-12](#)
 - VLAN tasks [3-9](#)
 - VLAN users
 - remove [9-5](#)
 - VLAN window
 - customizing [5-1](#)
 - VLAN wizard
 - explanation [2-6, 2-7](#)
 - VLANs over ATM [14-1](#)
 - VLANServer
 - communications port number [2-22](#)
 - description [1-10](#)
 - incorrect name [2-5, 2-7](#)
 - intelligence [1-10](#)
 - knowledge base [1-9](#)
 - SNMP comm. port number [2-22](#)
 - unlisted connection [2-7](#)
 - VLANServer database
 - restoring [2-18](#)
 - VLANServer message window
 - functions [2-13](#)
 - VLANServer performance tuning
 - mail queue size [2-22](#)
 - max. number of polling threads [2-22](#)
 - max. number of request threads [2-21](#)
 - max. total work threads [2-22](#)
 - unsolicited queue size [2-22](#)
 - VLSP [A-3](#)
 - VPI [A-3](#)
 - VRRP [A-3](#)
 - enabling and disabling on router ports [8-11](#)
 - VRRP multicast
 - disabling on router port [8-48](#)
 - enabling on router port [8-47](#)
- ## W
- Wild Card VLAN [9-2](#)
 - wizard
 - from File->Domain menu [3-7](#)
 - functions [6-1](#)
 - how to [6-2](#)
 - restart [2-6](#)
 - wizard window
 - button purpose [6-2](#)
- ## Y
- year 2000 compliant [xv](#)
- ## Z
- zoom
 - Setting preferences, functions [13-9](#)
 - Topology view->View [13-3](#)