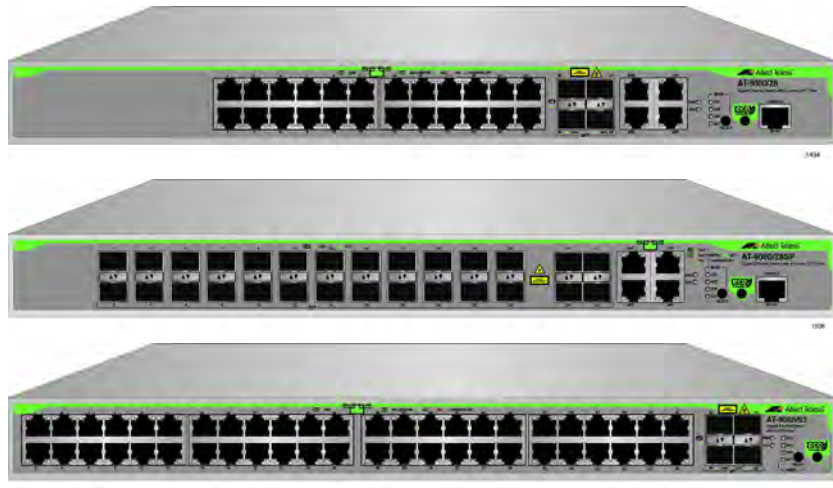




AT-9000 Series

Gigabit Ethernet Switches

- ❑ AT-9000/12PoE
- ❑ AT-9000/28
- ❑ AT-9000/28PoE
- ❑ AT-9000/28SP
- ❑ AT-9000/52



Management Software Web Interface User's Guide

AlliedWare Plus Version 2.1.8.0

Copyright

Copyright © 2014, Allied Telesis, Inc.

All rights reserved.

This product includes software licensed under the BSD License. As such, the following language applies for those portions of the software licensed under the BSD License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Allied Telesis, Inc. nor the names of the respective companies above may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1989, 1991, 1992 by Carnegie Mellon University. Derivative Work - 1996, 1998-2000. Copyright 1996, 1998-2000 by The Regents of the University of California - All rights reserved. Copyright (c) 2001-2003 by Networks Associates Technology, Inc. - All rights reserved. Copyright (c) 2001-2003 by Cambridge Broadband Ltd. - All rights reserved. Copyright (c) 2003 by Sun Microsystems, Inc. - All rights reserved. Copyright (c) 2003-2005 by Sparta, Inc. - All rights reserved. Copyright (c) 2004 by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications. - All rights reserved. Copyright (c) 2003 by Fabasoft R&D Software GmbH & Co KG - All rights reserved. Copyright (c) 2004-2006 by Internet Systems Consortium, Inc. ("ISC") - All rights reserved. Copyright (c) 1995-2003 by Internet Software Consortium - All rights reserved. Copyright (c) 1992-2003 by David Mills - All rights reserved. Copyright (c) 1995 by Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland - All rights reserved. Copyright (c) 1998 by CORE SDI S.A., Buenos Aires, Argentina - All rights reserved. Copyright 1995, 1996 by David Mazieres - All rights reserved. Copyright 1983, 1990, 1992, 1993, 1995 by The Regents of the University of California - All rights reserved. Copyright (c) 1995 Patrick Powell - All rights reserved. Copyright (c) 1998-2005 The OpenSSL Project - All rights reserved. Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) - All rights reserved. Copyright (c) 2008, Henry Kwok - All rights reserved. Copyright (c) 1995, 1998, 1999, 2000, 2001 by Jef Poskanzer <jef@mail.acme.com>. - All rights reserved.

Some components of the SSH software are provided under a standard 2-term BSD license with the following names as copyright holders: Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller, Kevin Steves, Daniel Kouril, Wesley Griffin, Per Allansson, Nils Nordman, and Simon Wilkinson,

Portable OpenSSH includes code from the following copyright holders, also under the 2-term BSD license: Ben Lindstrom, Tim Rice, Andre Lucas, Chris Adams, Corinna Vinschen, Cray Inc., Denis Parker, Gert Doering, Jakob Schlyter, Jason Downs, Juha Yrjola, Michael Stone, Network Associates, Solar Designer, Todd C. Miller, Wayne Schroeder, William Jones, Darren Tucker, Sun Microsystems, The SCO Group.

Some Portable OpenSSH code is licensed under a 3-term BSD style license to the following copyright holders: Todd C. Miller, Theo de Raadt, Damien Miller, Eric P. Allman, The Regents of the University of California, and Constantin S. Svintsoff. Some Portable OpenSSH code is licensed under an ISC-style license to the following copyright holders: Internet Software Consortium, Todd C. Miller, Reyk Floeter, and Chad Mynhier. Some Portable OpenSSH code is licensed under a MIT-style license to the following copyright holder: Free Software Foundation, Inc.

This product also includes software licensed under the GNU General Public License available from:

<http://www.gnu.org/licenses/gpl2.html>

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in this product, please send us a request by registered mail including a check for US\$15 to cover production and shipping costs, and a CD with the GPL code will be mailed to you.

GPL Code Request

Allied Telesis, Inc.

3041 Orchard Parkway

San Jose, California 95134

No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis, AlliedWare Plus, and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

| | |
|--|----|
| Preface | 11 |
| Document Conventions | 12 |
| Downloading Management Software and Web-based Guides | 13 |
| Contacting Allied Telesis | 14 |
| Online Support | 14 |
| Email and Telephone Support..... | 14 |
| Returning Products | 14 |
| Sales or Corporate Information | 14 |
| Management Software Updates..... | 14 |
| Chapter 1: AlliedWare Plus™ Version 2.1.8 Web Browser Interface | 15 |
| Management Sessions | 16 |
| Web Manager Accounts | 17 |
| Chapter 2: Starting a Management Session | 19 |
| Starting a Web Management Session | 20 |
| Selecting Items from a Web Page | 26 |
| What to Configure First..... | 27 |
| Assigning a Name to the Switch | 27 |
| Adding a Management IP Address | 27 |
| Setting System Time | 27 |
| Saving Your Changes..... | 28 |
| Ending a Web Management Session | 29 |
| Chapter 3: Basic Switch Parameters | 31 |
| Setting the System Date and Time..... | 32 |
| Setting System Time Manually..... | 33 |
| Setting an SNTP or NTP Server | 34 |
| Setting a Telnet or SSH Server | 37 |
| Setting a Remote Log Server | 39 |
| Setting the Switch Information..... | 40 |
| Setting the Configuration File | 42 |
| Displaying and Setting the Active Configuration File | 42 |
| Uploading a Configuration File..... | 43 |
| Managing User Accounts | 44 |
| Adding a User | 44 |
| Changing a User Password | 45 |
| Changing the User Privilege | 47 |
| Deleting a User | 48 |
| Rebooting a Switch..... | 49 |
| Upgrading the Software..... | 50 |
| Returning the AlliedWare Plus Configuration to the Factory Default Values..... | 52 |
| Displaying System Information | 53 |
| Chapter 4: Setting Port Parameters | 57 |
| Displaying the Port Parameters..... | 58 |
| Changing the Port Settings..... | 62 |

| | |
|---|------------|
| Displaying the Storm Control Settings | 66 |
| Modifying the Storm Control Settings | 68 |
| Chapter 5: Setting Port Statistics | 71 |
| Displaying Port Statistics | 72 |
| Displaying Transmit and Receive Port Statistics | 72 |
| Displaying Receive Statistics..... | 73 |
| Displaying Transmit Statistics..... | 75 |
| Displaying Interface Statistics..... | 77 |
| Clearing Port Statistics..... | 79 |
| Refreshing Port Statistics..... | 80 |
| Chapter 6: Setting Port Mirroring | 81 |
| Overview | 82 |
| Displaying Port Mirroring Settings..... | 83 |
| Assigning a Destination Port..... | 85 |
| Specifying Direction Type | 86 |
| Chapter 7: Setting the Port Spanning Tree Protocol | 89 |
| Overview | 90 |
| Displaying Port Spanning Tree Protocol Settings | 91 |
| Modifying Port Spanning Tree Protocol Settings | 93 |
| Chapter 8: Setting the MAC Address | 95 |
| Displaying the MAC Address | 96 |
| Displaying Unicast MAC Addresses | 96 |
| Displaying Multicast MAC Addresses..... | 97 |
| Assigning a MAC Address | 98 |
| Assigning a Unicast Address..... | 98 |
| Assigning a Multicast Address..... | 99 |
| Deleting a MAC Address..... | 101 |
| Deleting a Unicast Address | 101 |
| Deleting a Multicast Address | 101 |
| Chapter 9: Setting LACP | 103 |
| Overview | 104 |
| Displaying LACP Trunks | 105 |
| Adding an LACP Trunk | 107 |
| Modifying an LACP Trunk..... | 109 |
| Deleting an LACP Trunk | 111 |
| Chapter 10: Setting Static Port Trunks | 113 |
| Overview | 114 |
| Displaying Static Trunk Settings | 115 |
| Adding Static Trunks..... | 117 |
| Modifying the Static Trunk Settings | 120 |
| Deleting Static Trunks..... | 123 |
| Chapter 11: Setting Port-based and Tagged VLANs | 125 |
| Overview | 126 |
| Port-based VLANs..... | 126 |
| Tagged VLANs | 126 |
| Tagged and Untagged Ports | 127 |
| Displaying VLANs | 128 |
| Adding a VLAN | 130 |
| Modifying VLANs | 132 |
| Assigning a Native VLAN..... | 134 |
| Deleting VLANs..... | 136 |

| | |
|---|-----|
| Chapter 12: Setting Internet Group Management Protocol (IGMP) Snooping | 137 |
| Overview..... | 138 |
| Displaying and Modifying IGMP Snooping Configuration..... | 139 |
| Clearing the Routers List..... | 141 |
| Disabling IGMP Snooping | 143 |
| Displaying the Routers List..... | 144 |
| Displaying the Hosts List | 145 |
| Chapter 13: Setting Switch Spanning Tree Protocols | 147 |
| Overview..... | 148 |
| Displaying Switch Spanning Tree Protocol Settings..... | 149 |
| Modifying Switch Spanning Tree Protocol Settings..... | 152 |
| Chapter 14: Power Over Ethernet (PoE) | 155 |
| Overview..... | 156 |
| Power Sourcing Equipment (PSE)..... | 156 |
| Powered Device (PD)..... | 156 |
| PD Classes | 156 |
| Power Budget..... | 157 |
| Port Prioritization..... | 157 |
| Displaying PoE Settings | 158 |
| PoE Configuration | 160 |
| Configuring Global PoE Settings..... | 160 |
| Configuring Individual Port PoE Settings | 160 |
| Chapter 15: Setting MAC Address-based Port Security | 163 |
| Overview..... | 164 |
| Static Versus Dynamic Addresses | 164 |
| Intrusion Actions..... | 164 |
| Guidelines | 165 |
| Displaying MAC Address-based Port Security Settings | 166 |
| Modifying MAC Address-based Port Security Settings | 168 |
| Disabling MAC Address-based Port Security Settings | 170 |
| Chapter 16: Setting RADIUS and TACACS+ Clients | 171 |
| Overview..... | 172 |
| Remote Manager Accounts..... | 172 |
| Accounting Information | 173 |
| Configuring RADIUS and TACACS+ | 173 |
| Placing RADIUS and TACACS+ Servers in the Client's List | 173 |
| Configuring RADIUS for Remote Manager Authentication..... | 175 |
| Configuring Remote Manager Authentication Using RADIUS | 175 |
| Adding a RADIUS Server..... | 177 |
| Configuring TACACS+ for Remote Manager Authentication..... | 179 |
| Configuring Remote Manager Authentication Using TACACS+ | 179 |
| Adding a TACACS+ Server..... | 182 |
| Deleting an Authentication Server | 184 |
| Chapter 17: Setting 802.1x Port-based Network Access | 185 |
| Overview..... | 186 |
| Enabling 802.1x Port-based Authentication on the Switch..... | 187 |
| Configuring 802.1x Port-based Authentication | 188 |
| Displaying the 802.1x Authentication Port Settings..... | 194 |
| Disabling 802.1x Port-based Authentication on the Switch | 195 |
| Disabling 802.1x Port-based Authentication on a Port | 196 |
| Chapter 18: Setting IPv4 and IPv6 Management | 197 |
| Overview..... | 198 |

| | |
|--|------------|
| IP Management Guidelines | 199 |
| Assigning an IPv4 Address | 200 |
| Assigning a Static IPv4 Address..... | 200 |
| Assigning a DHCP IPv4 Address | 201 |
| Assigning an IPv6 Address | 204 |
| Displaying IP Addresses | 206 |
| Modifying IP Addresses | 207 |
| Modifying an IPv4 Static Address..... | 207 |
| Changing a DHCP IPv4 Address to Static..... | 207 |
| Modifying an IPv6 Address..... | 208 |
| Chapter 19: Setting LLDP and LLDP-MED | 209 |
| Overview | 210 |
| Setting LLDP Locations | 211 |
| Creating a Civic Location..... | 211 |
| Creating a Coordinate Location..... | 215 |
| Creating an ELIN Location | 217 |
| Configuring LLDP and LLDP-MED | 219 |
| Setting the Basic LLDP Configuration | 219 |
| Setting LLDP Port Assignments | 220 |
| Assigning Port Locations | 222 |
| Enabling LLDP TLV | 224 |
| Enabling LLDP- MED TLV | 228 |
| Displaying LLDP Neighbor Information..... | 231 |
| Displaying LLDP Neighbor Information | 231 |
| Displaying LLDP Neighbor Detail | 232 |
| Displaying LLDP Statistics | 236 |
| Displaying LLDP Locations | 238 |
| Displaying Civic Locations..... | 238 |
| Displaying Coordinate Locations..... | 239 |
| Displaying ELIN Locations..... | 240 |
| Displaying LLDP and LLDP-MED Settings | 241 |
| Displaying the Basic LLDP Configuration..... | 241 |
| Displaying LLDP Port Assignments..... | 242 |
| Displaying Port Locations | 243 |
| Displaying LLDP TLV | 243 |
| Displaying LLDP-MED TLV | 245 |
| Disabling LLDP on the Switch..... | 247 |
| Chapter 20: Setting sFlow | 249 |
| Overview | 250 |
| Ingress Packet Samples..... | 250 |
| Packet Counters | 250 |
| sFlow Collectors | 251 |
| Guidelines..... | 251 |
| Configuring sFlow on a Port..... | 252 |
| Specifying an sFlow Collector..... | 254 |
| Enabling sFlow on the Switch | 256 |
| Displaying the sFlow Settings | 257 |

Figures

| | |
|---|-----|
| Figure 1: Login Menu..... | 20 |
| Figure 2: Displaying the IP address..... | 21 |
| Figure 3: Login Page..... | 22 |
| Figure 4: Dashboard Page..... | 23 |
| Figure 5: System Contact Information Page..... | 28 |
| Figure 6: System Settings Tab..... | 33 |
| Figure 7: System Time Settings Page..... | 33 |
| Figure 8: Calendar Page..... | 34 |
| Figure 9: System Time Settings Page with Network Time Settings Tab..... | 35 |
| Figure 10: System Services Page..... | 37 |
| Figure 11: System Contact Information Page..... | 40 |
| Figure 12: Configuration Files Page..... | 42 |
| Figure 13: File Upload Page..... | 43 |
| Figure 14: User Management Page..... | 44 |
| Figure 15: User Management Page with Change Password Tab..... | 46 |
| Figure 16: User Management Page with Change Privilege Tab..... | 47 |
| Figure 17: User Management Page with Delete User Tab..... | 48 |
| Figure 18: System Upgrade Page..... | 51 |
| Figure 19: Port Numbering System..... | 58 |
| Figure 20: Switching Tab with Port Tab..... | 59 |
| Figure 21: Port Configuration Page..... | 59 |
| Figure 22: Port Configuration Modify Page..... | 63 |
| Figure 23: Storm Control List Page..... | 66 |
| Figure 24: Storm Control Settings Page..... | 68 |
| Figure 25: Port Statistics Page with Tx + Rx Tab..... | 72 |
| Figure 26: Port Statistics with Receive Tab..... | 74 |
| Figure 27: Port Statistics with Transmit Tab..... | 76 |
| Figure 28: Port Statistics Page with Interface Tab..... | 77 |
| Figure 29: Port Mirroring List Page..... | 83 |
| Figure 30: Modify Port Mirroring Page..... | 86 |
| Figure 31: Port Spanning Tree Settings Page..... | 91 |
| Figure 32: Modify Port Spanning Tree Settings Page..... | 93 |
| Figure 33: Switching Tab..... | 96 |
| Figure 34: Unicast MACs Page..... | 96 |
| Figure 35: Multicast MACs Page..... | 97 |
| Figure 36: Add Unicast Mac Address Page..... | 98 |
| Figure 37: Add Multicast Mac Address Page..... | 99 |
| Figure 38: Switching Tab with Link Aggregation Selected..... | 105 |
| Figure 39: LACP Trunks Page..... | 105 |
| Figure 40: Add LACP Trunk Page..... | 107 |
| Figure 41: Modify LACP Trunk Page..... | 109 |
| Figure 42: Switching Tab with Link Aggregation Selected..... | 115 |
| Figure 43: Switching Tab with Static Trunks Selected..... | 115 |
| Figure 44: Static Trunks Page..... | 116 |
| Figure 45: Add Static Trunk Page..... | 118 |
| Figure 46: Modify Static Trunk Page..... | 121 |
| Figure 47: VLANs Page..... | 128 |
| Figure 48: Add VLAN Page..... | 130 |
| Figure 49: Modify VLAN Page..... | 132 |
| Figure 50: Native VLAN Page..... | 134 |

| | |
|--|-----|
| Figure 51: IGMP Snooping Page with Configuration Tab | 139 |
| Figure 52: IGMP Snooping Page with Routers List Tab | 141 |
| Figure 53: IGMP Snooping Page with Hosts List Tab..... | 145 |
| Figure 54: Spanning Tree Settings Page..... | 149 |
| Figure 55: PoE Page | 158 |
| Figure 56: Modify Port PoE Settings Page | 161 |
| Figure 57: Security Tab..... | 166 |
| Figure 58: MAC Based Port Security Page..... | 166 |
| Figure 59: Modify MAC Based Port Security Page..... | 168 |
| Figure 60: Authentication Server Configuration Page with RADIUS Tab | 175 |
| Figure 61: Radius Server Add Page | 177 |
| Figure 62: Authentication Server Configuration Page with TACACS+ Tab | 180 |
| Figure 63: TACACS+ Server Add Page..... | 183 |
| Figure 64: 802.1x Authentication Page..... | 187 |
| Figure 65: Modify 802.1x Authentication Page | 188 |
| Figure 66: Modify 802.1x Authentication Page Expanded..... | 189 |
| Figure 67: 802.1x Authentication View Page..... | 194 |
| Figure 68: 802.1x Authentication Page with Status Enabled..... | 195 |
| Figure 69: Management Tab..... | 200 |
| Figure 70: IP Management Configuration Page with Static IP Address..... | 200 |
| Figure 71: IP Management Configuration Page with DHCP..... | 202 |
| Figure 72: IPv6 Management Configuration Page..... | 204 |
| Figure 73: Discovery & Monitoring Tab..... | 211 |
| Figure 74: Locations Tab | 212 |
| Figure 75: LLDP Civic Location Page..... | 212 |
| Figure 76: Add LLDP Civic Location Page..... | 214 |
| Figure 77: LLDP Coordinate Location Page | 215 |
| Figure 78: Add LLDP Coordinate Location Page..... | 216 |
| Figure 79: LLDP ELIN Location List Page | 217 |
| Figure 80: LLDP ELIN Location Page..... | 218 |
| Figure 81: LLDP Configuration Page..... | 219 |
| Figure 82: LLDP Port Config Page | 221 |
| Figure 83: Modify LLDP Port Configuration Page..... | 222 |
| Figure 84: LLDP Port Location Page | 223 |
| Figure 85: Modify LLDP Port Location Page..... | 224 |
| Figure 86: LLDP TLV Tab | 225 |
| Figure 87: LLDP TLV Page..... | 225 |
| Figure 88: Modify LLDP TLV Page | 226 |
| Figure 89: LLDP MED TLV Page..... | 228 |
| Figure 90: Modify LLDP Med TLV Page | 229 |
| Figure 91: LLDP Neighbors Information Page..... | 231 |
| Figure 92: LLDP Neighbor Detail Page..... | 233 |
| Figure 93: LLDP Statistics Page with Port Statistics Tab | 236 |
| Figure 94: LLDP Statistics Page with Summary Tab | 237 |
| Figure 95: sFlow Port Modify Page..... | 252 |
| Figure 96: sFlow Page with Collectors Tab | 254 |
| Figure 97: sFlow Collector Page..... | 255 |
| Figure 98: sFlow Page with Port Configurations Tab..... | 256 |

Preface

This is the web browser management guide for the AT-9000/12POE, AT-9000/28, AT-9000/28POE, AT-9000/28SP, and AT-9000/52 Managed Layer 2-4 Gigabit Ethernet EcoSwitches. The instructions in this guide explain how to start a management session, use the web interface of the AlliedWare Plus™ Management Software, and configure the features of the switch.

For hardware installation instructions, refer to the *AT-9000 Manager Layer 2 GB EcoSwitch Series Installation Guide*.

This preface contains the following sections:

- “Document Conventions” on page 12
- “Downloading Management Software and Web-based Guides” on page 13
- “Contacting Allied Telesis” on page 14



Caution

The customer, re-seller, sub-contractor, distributor, software developer or any buyer of an Allied Telesis “ATI” product known as “customer”, hereby agrees to have all licenses required by any governmental agency and to comply with all applicable laws and regulations in its performance under this Agreement, including export control, maintained by U.S. Commerce Department’s Bureau of Industry and Security (BIS) and the U.S. Treasury Department’s Office of Foreign Assets Control (OFAC), international boycotts regulations and all anti-corruption laws, including the U.S. Foreign Corrupt Practices Act (FCPA). The customer understands that U.S. Government authorization may be required to export the software, commodity or technology, or to re-export or re-transfer to a third country, another end-user or another end-use. The customer agrees to assume all such obligations.

Document Conventions

This document uses the following conventions:

Note

Notes provide additional information.

**Caution**

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

**Warning**

Warnings inform you that performing or omitting a specific action may result in bodily injury.

Downloading Management Software and Web-based Guides

Both new releases of management software and product documentation are available from the Allied Telesis web sites. The management software is available at www.alliedtelesis.com/support/software. To display all of the network management software for a product, use the pull-down menu labeled "All" to select a hardware product model such as "AT-9000/28SP." Then, double-click the software version that you want to download onto your local work station or server.

The installation and user guides for all Allied Telesis products are available in PDF at www.alliedtelesis.com/support/documentation/. To display all of the product documentation for a product, use the pull-down menu labeled "All" to select a hardware product model such as "AT-9000/52." Then, double-click the document that you want to view. You can view the documents online or download them onto your local workstation or server.

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support and for sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: www.alliedtelesis.com/support/kb.aspx. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Allied Telesis web site at www.alliedtelesis.com. Select your country from the list on the web site and then select the appropriate tab.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense. For instructions on how to obtain an RMA number, go to our web site at www.alliedtelesis.com and then select **Support and Replacement Services**.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site at www.alliedtelesis.com.

Management Software Updates

New releases of the management software for our managed products are available from the Allied Telesis web site: www.alliedtelesis.com. For downloading instructions, see "Downloading Management Software and Web-based Guides" on page 13.

Chapter 1

AlliedWare Plus™ Version 2.1.8 Web Browser Interface

This chapter describes the types of web management sessions on the AlliedWare Plus web interface and the web interface manager accounts. See the following sections:

- ❑ “Management Sessions” on page 16
- ❑ “Web Manager Accounts” on page 17

Management Sessions

This manual provides procedures that guide you through the AlliedWare Plus web interface. The AlliedWare Plus Management Software supports the AT-9000/12POE, AT-9000/28, AT-9000/28POE, AT-9000/28SP, and AT-9000/52 Layer 2-4 Gigabit Ethernet EcoSwitches in both the web interface and the Command Line Interface (CLI).

The initial management session of the switch must be from a local (serial port console) management session because you must assign the switch an IP address from a local session. After you have assigned an IP address to the switch and enabled web management, you can log onto the web with either an encrypted (HTTPS) or a non-encrypted (HTTP) web browser management session.

In addition, the web interface allows access to a subset of the AlliedWare Plus features. For access to all of the AlliedWare Plus features, you must use the CLI.

Detailed feature descriptions are not provided in this guide. For thorough explanations of the features, see the *AlliedWare Plus Management Software Command Line User's Guide*.

Note

The initial management session of the switch must be from a local (serial port console) management session.

Web Manager Accounts

You must log on to manage the switch. This requires a valid username and password. The switch comes with one web manager account with a username of “manager” and the default password of “friend.” Both the username and password are case sensitive. This account gives you access to all management modes and commands.

In the web interface, you can create two additional remote manager accounts. For instructions, see “Managing User Accounts” on page 44. The switch supports up to three manager sessions (this is configurable) at one time.

Chapter 2

Starting a Management Session

This chapter describes how to start a management session using the AlliedWare Plus web interface as well as how to select fields, save your changes, and end a management session. See the following sections:

- ❑ “Starting a Web Management Session” on page 20
- ❑ “Selecting Items from a Web Page” on page 26
- ❑ “What to Configure First” on page 27
- ❑ “Saving Your Changes” on page 28
- ❑ “Ending a Web Management Session” on page 29

Starting a Web Management Session

Before you start a remote web management session, you must log onto the AlliedWare Plus CLI and assign an IP address to the switch. Also, you must enable web management on the switch, which is disabled by default.

To assign an IP address, enable web management, and start a web management session on an AT-9000 switch, do the following:

Note

If you have already assigned the switch an IP address and enabled the web management, start with Step 8.

1. Log on to the AlliedWare Plus CLI.

The Login Menu is shown in Figure 1.

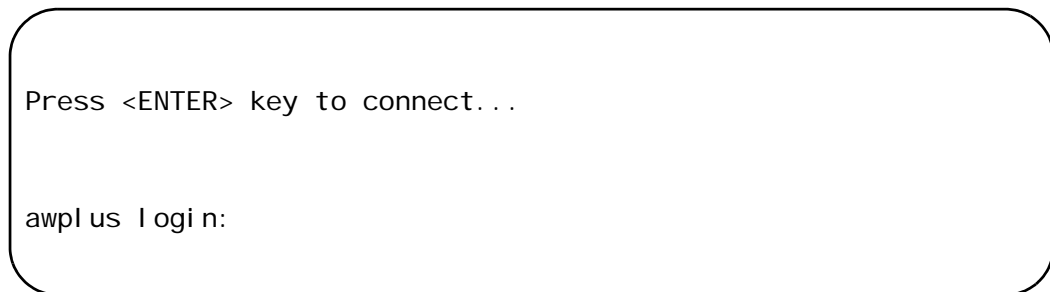


Figure 1. Login Menu

2. Enter “manager” for the login name and press Return.

You are prompted for a password.

3. Enter “friend” as the password and press Return.

The “awplus>” prompt indicates that you are logged on to the switch.

4. Assign an IP address and subnet mask to the switch by entering the following commands:

```
awpl us> enable  
  
awpl us# configure terminal  
  
awpl us(config)# interface vlan1  
  
awpl us(config-if)# ip address 167.142.10.5/16
```

5. Display the IP address assigned to VLAN 1 by entering the following commands:

```
awpl us(config-if)# exit
```

```
awpl us(config)# exit
```

```
awpl us# show ip interface
```

For a display of this command, see Figure 2.

```
awpl us# show ip interface
```

| Interface | IP-Address | Status | Protocol |
|-----------|-----------------|----------|----------|
| vlan1-0 | 167.142.10.5/16 | admin up | running |

Figure 2. Displaying the IP address

6. Enable the web browser on the switch by entering the following commands:

```
awpl us# configure terminal
```

```
awpl us(config)# http server
```

If using HTTPS, enter the following commands:

```
awpl us# configure terminal
```

```
awpl us(config)# service https
```

7. Save your changes on the switch by copying the running configuration file to the start-up configuration file. Enter the following command:

```
awpl us# copy running-config startup-config
```

8. Open a web browser, such as Microsoft Explorer, and enter one of the following:

- To start an HTTP session, enter: `http://` followed by the IP address of the switch.
- To start an HTTPS session, enter: `https://` followed by the IP address of the switch.

The Login Page is displayed. See Figure 3 on page 22.

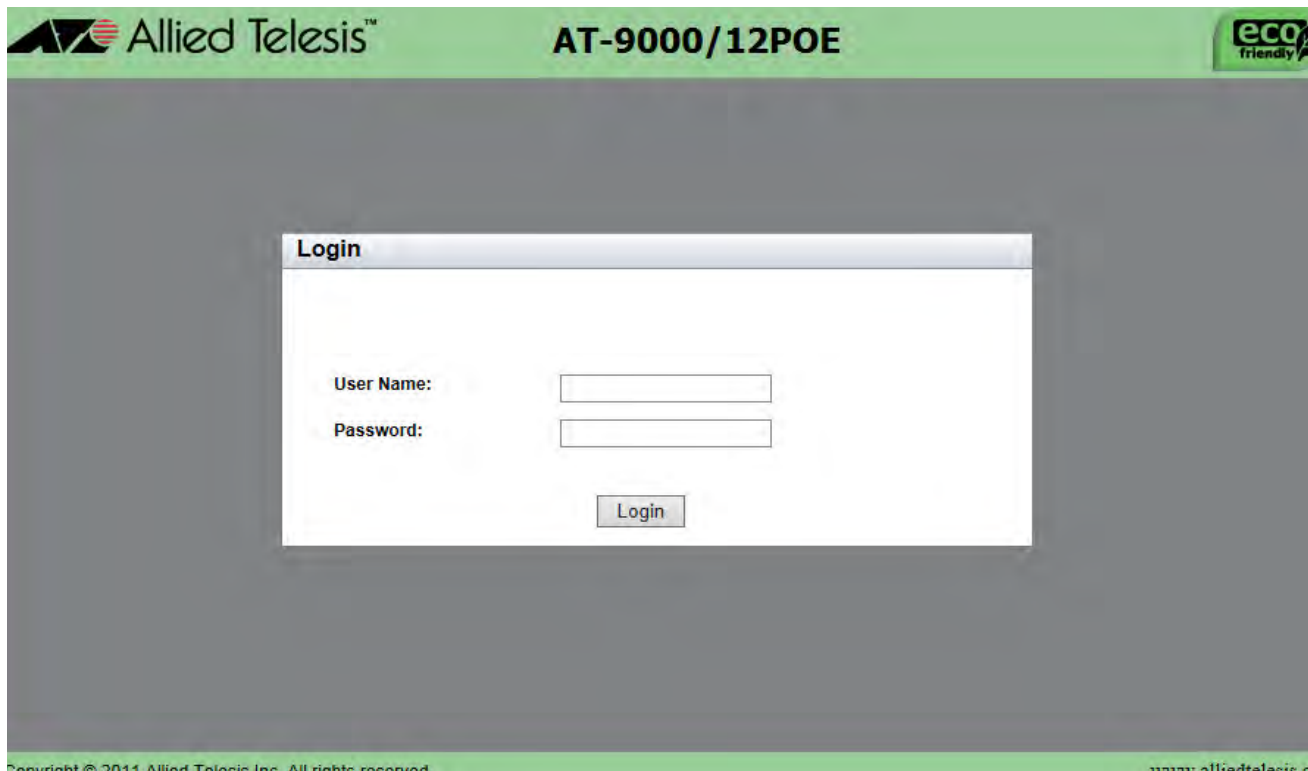


Figure 3. Login Page

9. Enter “manager” in the User Name field and “friend” in the Password field. Then, click the **Login** button.

The Dashboard page is displayed. See Figure 4 on page 23. The Dashboard page is the home page of the switch.

System Switching Security Management Discovery & Monitoring

Up Time: 0 Days, 2h : 35m : 12s [SAVE](#) [LOGOUT](#)

Dashboard

AT-9000/12POE

POWER LED

System

| | | | |
|------------------|-----------------------------|-----------------|--------------|
| Software Version | 2.1.8.0 | System Name | |
| Build Date/Time | Dec 17 2013 02:25:46 | System Contact | |
| Serial No. | A04800H130900008 | System Location | |
| MAC Address | eccd.6db4.39d4 | Management VLAN | VLAN1 |
| IPv4 Address | 192.168.1.1/24 | IPv6 Address | |
| IPv4 Gateway | 0.0.0.0 | IPv6 Gateway | |

Services

| | | | | | |
|----------|------------------|---------------|-----------------|----------------------------|-----------------|
| SNMP | Disabled | Spanning Tree | RSTP | 802.1x Port Authentication | Disabled |
| HTTP | Unsecured | QoS | Disabled | Remote Logging | Disabled |
| Teletnet | Enabled | LLDP | Disabled | IGMP Snooping | Disabled |
| SSH | Disabled | SFLOW | Disabled | | |

Administrative Options

[System Upgrade](#)

[Reboot](#)

Copyright © 2011 Allied Telesis Inc. All rights reserved. www.alliedtelesis.com

Figure 4. Dashboard Page

The following fields are displayed:

- Up Time**— Length of time since the switch was last reset or power cycled in days, hours, minutes and seconds. This field is located in the upper right-hand corner of the page.

The System section displays the following information:

- Software Version**— Software version number of the AlliedWare Plus software.
- Build Date/Time**— Month, date, year and time (in the hour:minute:second format) the software version was built.
- Serial No.**— Unique serial number of the switch.
- MAC Address**— MAC address of the switch.

- ❑ **IPv4 Address**— IPv4 address and subnet mask of the web interface. The IPv4 management address is assigned to the switch. The address is specified in the following format:

xxx.xxx.xxx.xxx

Each xxx is a number from 0 to 255. There are four groups of numbers that are separated by periods.

Note

For IPv4 addresses, the subnet mask is a decimal number that represents the number of bits, from left to right, that constitute the network portion of the address. Here are some examples:

- The decimal mask 16 is equivalent to the mask 255.255.0.0.
 - The decimal mask 24 is equivalent to the mask 255.255.255.0.
-

- ❑ **IPv4 Gateway**— IPv4 address of the next hop of the switch's default route. The switch uses a default route when it must communicate with a device that is not on the local IPv4 network.
- ❑ **System Name**— Name of the switch. To configure this field, see "Setting the Switch Information" on page 40.
- ❑ **System Contact**— Contact person for the switch. To configure this field, see "Setting the Switch Information" on page 40.
- ❑ **System Location**— Location of the switch. To configure this field, see "Setting the Switch Information" on page 40.
- ❑ **Management VLAN**— Management VLAN assigned to the switch. The default VLAN is "VLAN1."
- ❑ **IPv6 Address**— IPv6 address and subnet mask of the web interface. An IPv6 management address for the switch is entered in the following format:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

Where "n" is a hexadecimal digit from 0 to F. The eight groups of digits are separated by colons. Groups where all four digits are "0" can be omitted. Leading "0"s in groups can also be omitted.

For example, the following IPv6 addresses are equivalent:

12c4:421e:09a8:0000:0000:0000:00a4:1c50

12c4:421e:9a8::a4:1c50

- ❑ **IPv6 Gateway**— IPv6 address of the next hop of the switch's default route. The switch uses a default route when it must communicate with a device that is not on the local IPv6 network.

The Services section displays the following information:

- ❑ **SNMP**— SNMP setting of the switch.
- ❑ **HTTP**— HTTP setting of the switch
- ❑ **Telnet**— Indicates if Telnet is enabled or disabled on the switch.
- ❑ **SSH**— Indicates if SSH is enabled or disabled on the switch.
- ❑ **Spanning Tree**— Indicates if STP, RSTP, or MSTP is enabled on the switch. The default setting is "RSTP."
- ❑ **QoS**— Indicates if QoS is enabled or disabled on the switch.
- ❑ **LLDP**— Indicates if LLDP is enabled or disabled on the switch.
- ❑ **SFLOW**— Indicates if sFlow is enabled or disabled on the switch.
- ❑ **802.1x Port Authentication**— Indicates if 802.1x Port Authentication is enabled or disabled on the switch.
- ❑ **Remote Logging**— Indicates if the remote log is enabled or disabled on the switch.
- ❑ **IGMP Snooping**— Indicates if IGMP Snooping is enabled or disabled on the switch.

The Administration Options section displays the following information:

- ❑ **System Upgrade**— Select this field to upgrade your system software. See "Upgrading the Software" on page 50.
- ❑ **Reboot**— Select this field to reboot the switch. For instructions, see "Rebooting a Switch" on page 49.

Selecting Items from a Web Page

To select a feature or parameter, place your cursor over the selection and click on the selection.

What to Configure First

Here are a few suggestions on what to configure during your web management session on the switch. The initial management session must be a local management session from the Console port on the switch. For instructions on how to start a local management session, refer to “Starting a Web Management Session” on page 20.

Assigning a Name to the Switch

The switch is easier to identify if you assign it a name. The switch's name is displayed on the Dashboard page. See Figure 4 on page 23. To change the name of the switch, see “Setting the Switch Information” on page 40.

A name can be up to 39 alphanumeric characters. Spaces and quotation marks are not permitted.

Adding a Management IP Address

You must assign the switch a management IP address before you can access the web interface. In addition, you may assign the switch both an IPv4 and an IPv6 address. See Chapter 18, “Setting IPv4 and IPv6 Management” on page 197.

Here are the requirements:

- The switch can have one management IPv4 address and one management IPv6 address.
- The switch can have one IPv4 default gateway and one IPv6 default gateway.
- A management IP address must be assigned to a VLAN on the switch. It can be any VLAN, including the Default_VLAN which is “VLAN1.” For background information on VLANs, refer to the *AlliedWare Plus Version 2.1.8 Command Line User's Guide*.
- The network devices (such as, syslog servers, TFTP servers, etc.) must be members of the same subnet as a management IP address or have access to it through routers or other Layer 3 devices.
- The switch must have a default gateway if the network devices are not members of the same subnet as the management IP address. The default gateway specifies the IP address of a router interface that represents the first hop to the subnets or networks of the network devices.
- A default gateway address, if needed, must be a member of the same subnet as a management IP address.

Setting System Time

To set the system time, either manually or with an NTP server, see “Setting the System Date and Time” on page 32.

Saving Your Changes

In the web interface, there are two ways to save your changes.

After you complete a procedure, click **Apply** as shown on the System Contact Information page. See Figure 5. This temporarily saves the information to the running configuration file, but it is not saved when you reboot the switch.

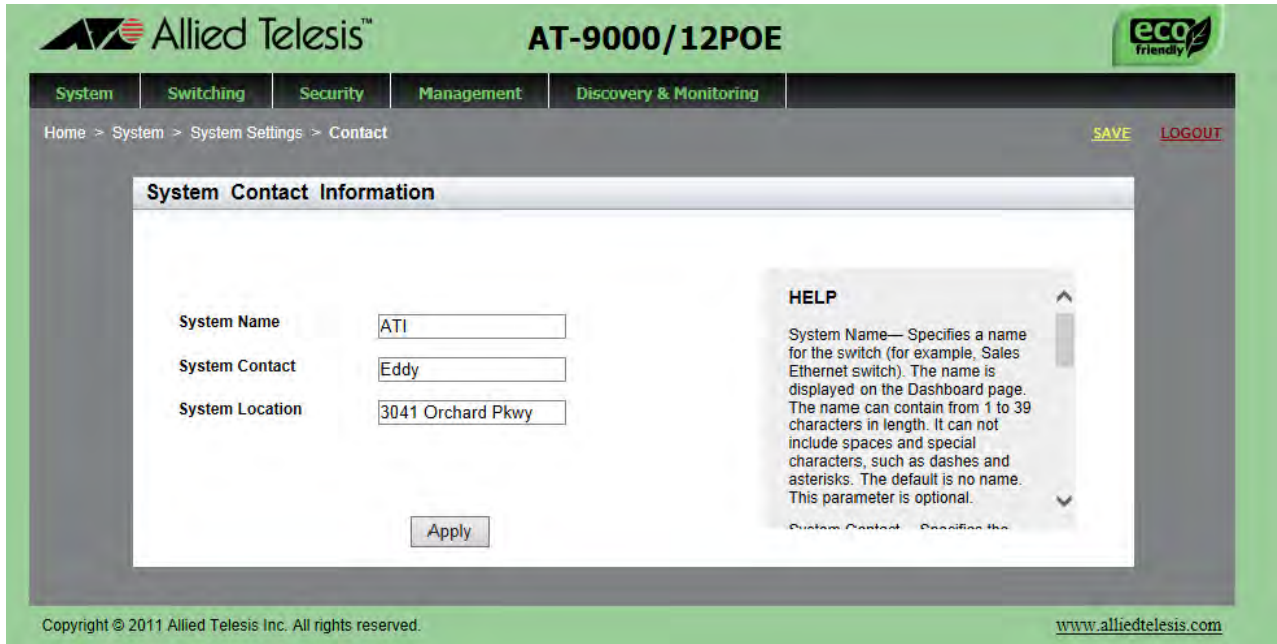


Figure 5. System Contact Information Page

To permanently save your changes in the start-up configuration file, click **SAVE** at the top of the web page.

Ending a Web Management Session

To end a web management session, select **LOGOUT** at the top of the web page. For an example, see the System Contact Information page in Figure 5 on page 28.

Chapter 3

Basic Switch Parameters

This chapter describes how to set up basic switch operations in the web interface. See the following sections:

- ❑ “Setting the System Date and Time” on page 32
- ❑ “Setting a Telnet or SSH Server” on page 37
- ❑ “Setting a Remote Log Server” on page 39
- ❑ “Setting the Switch Information” on page 40
- ❑ “Setting the Configuration File” on page 42
- ❑ “Managing User Accounts” on page 44
- ❑ “Rebooting a Switch” on page 49
- ❑ “Upgrading the Software” on page 50
- ❑ “Returning the AlliedWare Plus Configuration to the Factory Default Values” on page 52
- ❑ “Displaying System Information” on page 53

For additional information about basic port settings, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ Basic Switch Management
- ❑ Basic Switch Management Commands

Setting the System Date and Time

This procedure explains how to set the switch's date and time. Setting the date and time is important if you plan to view the events in the switch's event log or send the events to a syslog server. The correct date and time are also important if the management software sends traps to a management workstation or if you plan to create a self-signed SSL certificate. Events, traps, and self-signed certificates should contain the date and time of when they occurred or, in the case of certificates, when they were created.

There are two ways to set the switch's date and time. One method is to set it manually. This method is not recommended because the date and time are lost if you reboot the switch.

The second method uses the Simple Network Time Protocol (SNTP). The AlliedWare Plus Management Software comes with the client version of this protocol. You can configure the AlliedWare Plus software to obtain the current date and time from an SNTP or Network Time Protocol (NTP) server located on your network or the Internet.

SNTP is a reduced version of the NTP. However, the SNTP client software in the AlliedWare Plus Management Software is interoperable with NTP servers.

Note

In order for the management software on the switch to communicate with an SNTP or NTP server, there must be an interface on the local subnet from where the switch is able to reach the server. The switch uses the IP address of the interface as its source address when sending packets to the server.

Note

The default system time on the switch is midnight, January 1, 2000.

Choose from the following procedures:

- "Setting System Time Manually" on page 33
- "Setting an SNTP or NTP Server" on page 34

Setting System Time Manually

To set the system time manually, do the following:

1. Hover the cursor over the **System** tab.
2. From the System tab, hover over **System Settings**.

The System Settings Tab is displayed in Figure 6.



Figure 6. System Settings Tab

3. Move the cursor to the right and click **Time**.

The System Time Settings page is displayed. See Figure 7.

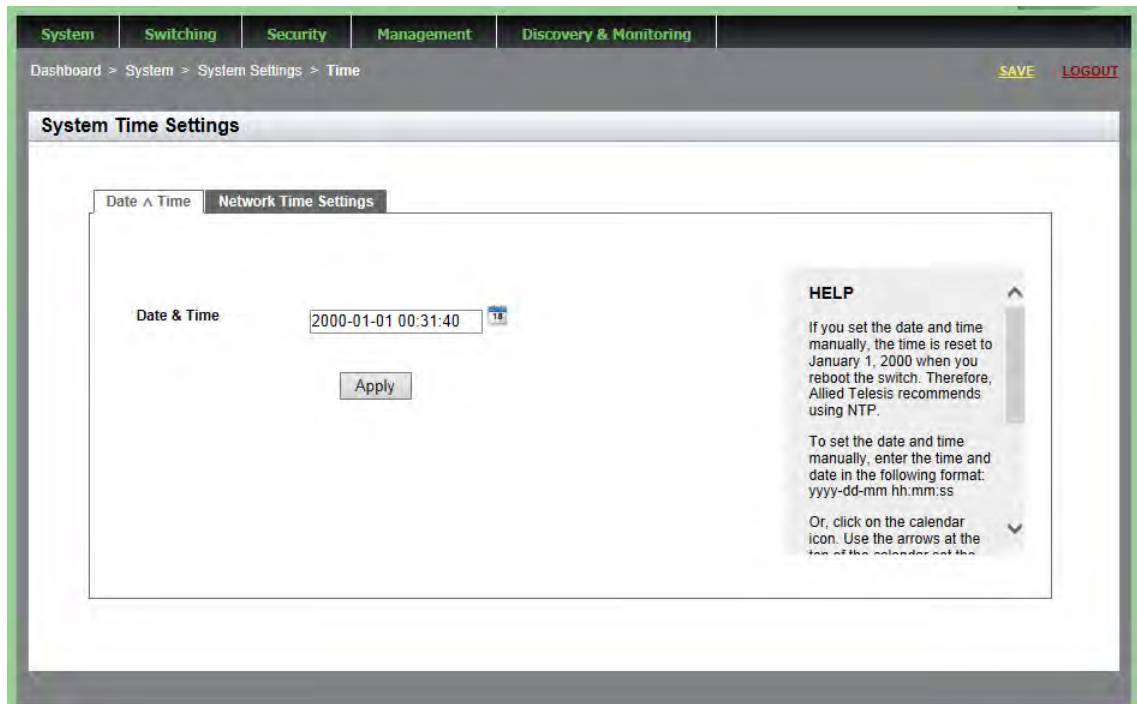


Figure 7. System Time Settings Page

4. There are two ways to set the date and time manually. Use either Step 4 or Step 5. To type in the system date and time in the **Date & Time** field, do the following:
 - a. Enter the time and date in the following format:
 yyyy-dd-mm hh:mm:ss
 - b. Click **Apply**.
5. Select the calendar icon.

The Calendar page is displayed. See Figure 8.

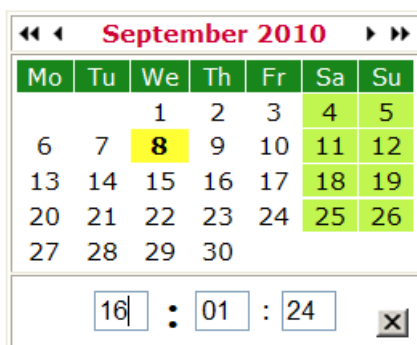


Figure 8. Calendar Page

- a. Use the arrows at the top of the Calendar to select the month and year.
 - b. Click on the day of the month.
 - c. Set the time of day using the following format:
hh:mm:ss
 - d. Close the Calendar page.
6. Click **Apply**.
 7. Click **SAVE** to save your changes on the switch.

Setting an SNTP or NTP Server

To configure an SNTP or NTP server, do the following:

1. Hover the cursor over the **System** tab.

The System Settings Tab is displayed. See Figure 6 on page 33.

2. From the System tab, hover over **System Settings**.
3. Move the cursor to the right and select **Time**.

The System Time Settings page is displayed. For an example of this page, see Figure 7 on page 33.

4. Select the **Network Time Settings** tab.

The Network Time Settings page is displayed. See Figure 9.

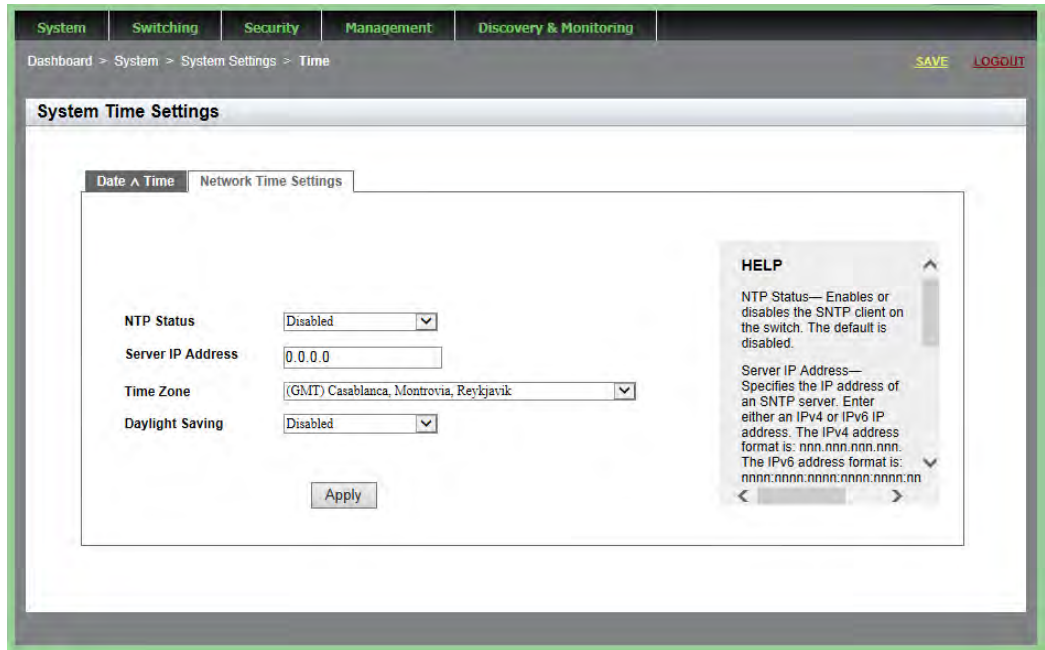


Figure 9. System Time Settings Page with Network Time Settings Tab

5. To configure the switch to obtain its date and time from an SNTP or NTP server on your network or the Internet, configure the following fields:
 - ❑ **NTP Status**— Enables or disables the SNTP client on the switch. The default is disabled.
 - ❑ **Server IP Address**— Specifies the IP address of an SNTP server. Enter either an IPv4 or IPv6 IP address.

The IPv4 format is: xxx.xxx.xxx.xxx where xxx is a decimal number from 0 to 255.

The IPv6 format is: nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn where n is a hexadecimal digit from 0 to F.

- ❑ **Time Zone**— Specifies the time zone as a measurement of Greenwich Mean Time (GMT) which is the default setting. Use the pull-down menu to select the other time zones.
- ❑ **Daylight Savings Time (DST)**— Enables or disables the system's adjustment for daylight savings time. The default is disabled.

Note

The switch does not set DST automatically. If the switch is in a locale that uses DST, you must remember to enable this when DST begins and disable it when DST ends. If the switch is in a locale that does not use DST, this option should be set to disabled all the time.

Note

If the local interface on the switch is obtaining its IP address and subnet mask from a DHCP server, you can configure the server to provide the interface with an IP address of an NTP or SNTP server. If you configured the server to provide this address, then you do not need to enter it here.

6. When you finish configuring the parameters, click **Apply**.

If you enabled the SNTP client, the switch immediately polls the SNTP or NTP server for the current date and time. (When SNTP is enabled, the switch automatically polls the server whenever a change is made to any of the fields on this page.)

7. Click **SAVE** to save your changes on the switch.

Setting a Telnet or SSH Server

The AlliedWare Plus Web Browser interface allows you to configure the switch as a Telnet or SSH server.

You can use the web browser interface to enable a Telnet server, but not as a Telnet client. The Telnet client is only supported from the CLI. For information about how to use a Telnet client, see the *AlliedWare Plus Management Software Command Line Interface User's Guide*.

To enable an SSH server in the web interface, you must first create an encryption key in the CLI interface. Then, you can enable the SSH server in the web interface.

The procedures in this section allow you to configure the switch as a Telnet or SSH server.

To enable Telnet or SSH server on the switch, do the following:

1. From the home page, hover the cursor over the **System** tab.
2. From the System tab, hover over System Settings.

The System Settings tab is displayed. See Figure 6 on page 33.

3. Move the cursor to the right and select **Services** from the drop-down menu.

The System Services page is displayed. See Figure 10.

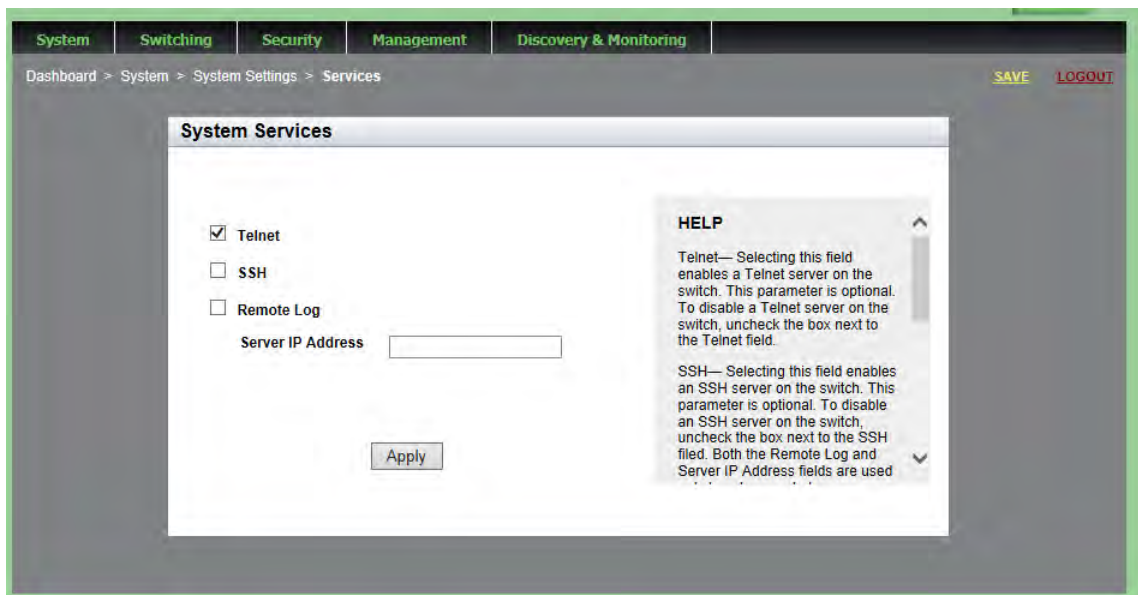


Figure 10. System Services Page

4. Configure the following parameters as necessary:
 - Telnet**— Selecting this field enables a Telnet server on the switch. To disable a Telnet server on the switch, uncheck the box next to the Telnet field. This parameter is optional.
 - SSH**— Selecting this field enables an SSH server on the switch. To disable an SSH server on the switch, uncheck the box next to the SSH field. This parameter is optional.

Note

Both the Remote Log and Server IP Address fields are used only to set a remote log server. For information on these fields, see “Setting a Remote Log Server” on page 39.

- Remote Log**— Check or uncheck the box to enable or disable remote logging.
 - Server IP Address**— This field is only used for the remote log server.
5. Click **Apply**.
 6. Click **SAVE** to save your changes on the switch.

Setting a Remote Log Server

You can use the AlliedWare Plus Web browser interface to enable logging to a remote log server, which is part of the Syslog feature. However, you must use the CLI to view or clear the event log. For information about the CLI, see the *Syslog* chapters in the *AlliedWare Plus Management Software Command Line Interface User's Guide*.

To activate remote logging on the switch, do the following:

1. Hover the cursor over the **System** tab.
2. From the System tab, hover over System Settings.

The System Settings tab is displayed. See Figure 6 on page 33.

3. Move the cursor to the right and select **Services**.

The System Services page is displayed. See Figure 10 on page 37.

4. Configure the following parameters as necessary:

- Remote Log**— Enables the switch to send status and error messages to a remote log server. This parameter is optional.
- Server IP Address**— Specifies the IP address of the remote log server. This field is mandatory if you selected the Remote Log field above. You can enter the IP address in the IPv4 format:
xxx.xxx.xxx.xxx.

where each xxx is a decimal number from 0 to 255. The numbers are separated by periods.

5. Click **Apply**.
6. Click **SAVE** to save your changes on the switch.

Setting the Switch Information

This procedure allows you to set information about the switch, such as a switch name, contact, and location. Assigning a name to the switch helps you identify your switches when you manage them and avoid performing a configuration procedure on the wrong switch.

To assign a name, location, and contact to a switch, perform the following procedure:

1. From the home page, hover the cursor over the **System tab**.
2. From the System tab, hover over **System Settings**.

The System Settings tab is displayed. See Figure 6 on page 33.

3. Move the cursor to the right and select **Contact Information**.

The System Contact Information page is displayed. See Figure 11.

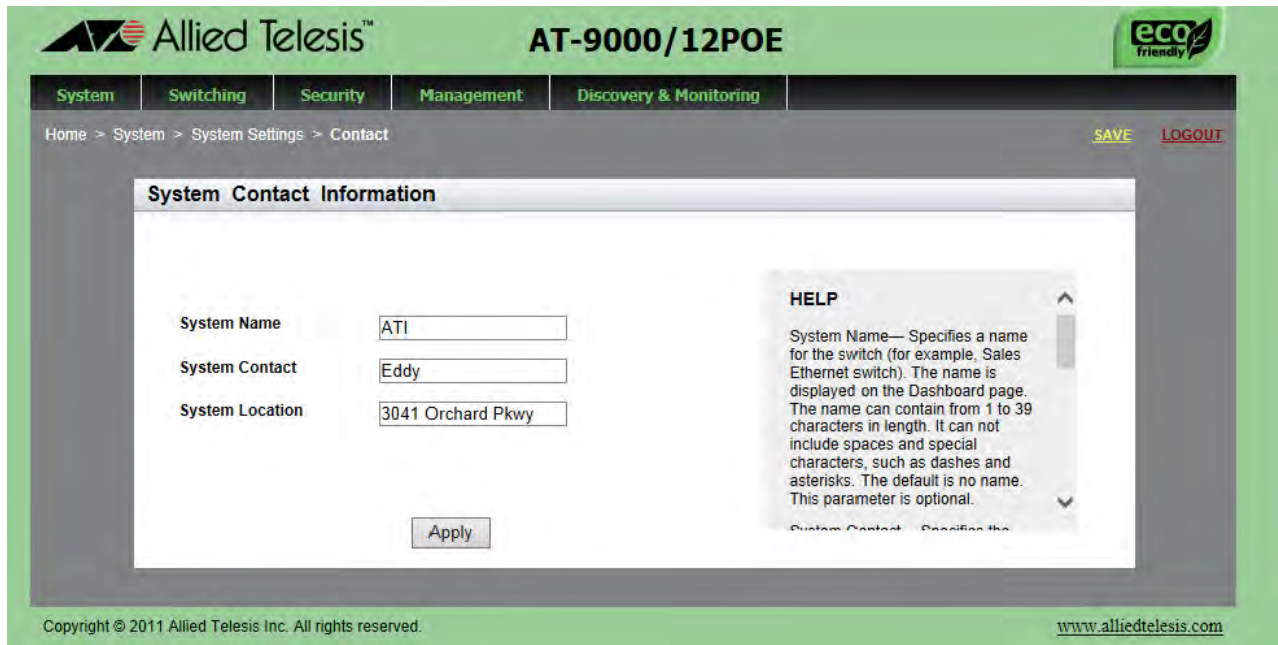


Figure 11. System Contact Information Page

Change the following parameters as necessary:

- ❑ **System Name** — Specifies a name for the switch (for example, Sales Ethernet switch). The name is displayed only on the Dashboard page. The name can be from 1 to 39 characters in length. It can include spaces and special characters, such as dashes and asterisks. By default, there is no system name. This parameter is optional.
 - ❑ **System Contact** — Specifies the name of the network administrator responsible for managing the switch. The name can be from 1 to 50 characters. It can include spaces and special characters, such as dashes and asterisks. The default is no name. This parameter is optional.
 - ❑ **System Location** — Specifies the location of the switch, (for example, 4th Floor - room 402B). The location can be from 1 to 50 characters. The location can include spaces and special characters, such as dashes and asterisks. The default is no location. This parameter is optional.
4. Click **Apply**.
 5. Click **SAVE** to activate your changes on the switch.

Setting the Configuration File

Within the web browser interface, you can upload a configuration file on to the switch, download a configuration file from the switch, or delete a configuration file. In addition, you can save your changes to the current configuration file. However, to create a new configuration file, you must access the switch through the CLI.

The file that you select in this procedure is the file that the switch uses the next time you reboot the switch.

See the following procedures:

- “Displaying and Setting the Active Configuration File”
- “Uploading a Configuration File” on page 43

Displaying and Setting the Active Configuration File

The file you select in this procedure is the active configuration file after you reboot the switch.

To select the active configuration file, do the following:

1. From the home page, hover the cursor over the **System** tab.
2. From the System tab, hover over **System Settings**.

The System Settings tab is displayed. See Figure 6 on page 33.

3. From the System tab, select **Configuration Files** from the pull-down menu.

For an example of the Configuration Files page, see Figure 12.

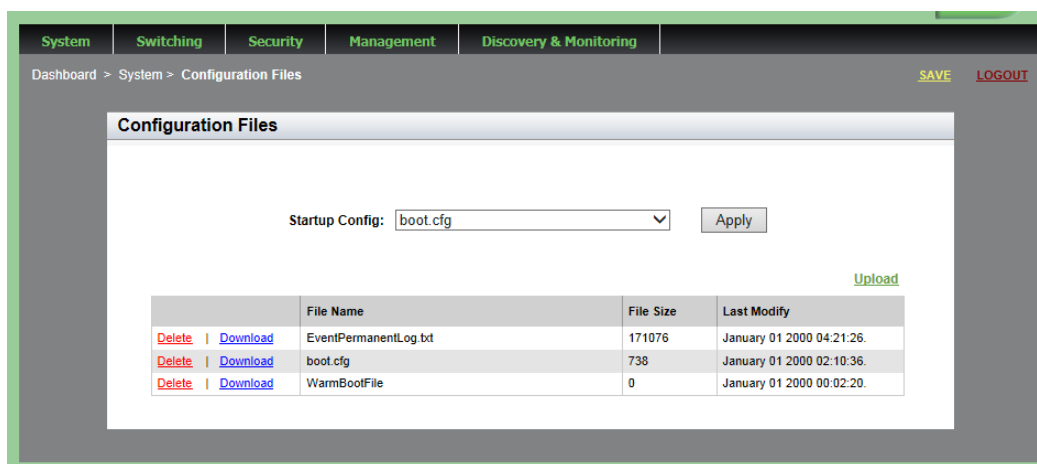


Figure 12. Configuration Files Page

The following fields are displayed:

- Startup Config**— Name of the active boot configuration file, which for the switch in the example is “boot.cfg.”
 - File Name**— Name of the file.
 - File Size**— File size in bytes.
 - Last Modify**— Date the configuration file was last modified. The format is month, date, year.
4. Use the pull-down menu to select the active configuration file. Then click **Apply**.

The file you select is the active configuration file after you reboot the switch.

5. Click **SAVE**.

Uploading a Configuration File

To upload a configuration file onto the switch, do the following:

1. From the home page, hover the cursor over the **System** tab.
For an example of the System tab, see Figure 6 on page 33.
2. From the System Settings tab, select **Configuration Files**.

For an example of the **Configuration Files** page, see Figure 12 on page 42.

3. Click **Upload**.

The File Upload page is displayed. See Figure 13.

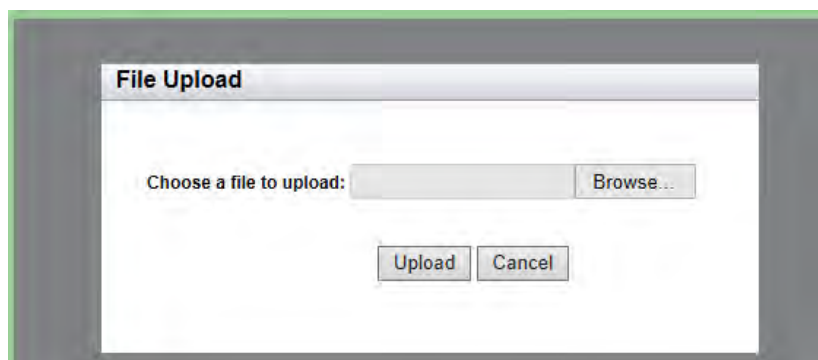


Figure 13. File Upload Page

4. Click **Browse** to select a file to upload onto the switch.
5. Select the file and then click **Upload**.

Managing User Accounts

The procedures in this section describe how to create user accounts, as well as change passwords and privileges. There is also a procedure that describes how to delete a user account. See the following:

- ❑ “Adding a User”
- ❑ “Changing a User Password” on page 45
- ❑ “Changing the User Privilege” on page 47
- ❑ “Deleting a User” on page 48

Adding a User

To add a user, do the following:

1. From the home page, hover the cursor over the **System** tab.

The System Settings tab is displayed, see Figure 6 on page 33.

2. From the System Settings tab, select **User Management**.

For an example of the User Management page, see Figure 14.

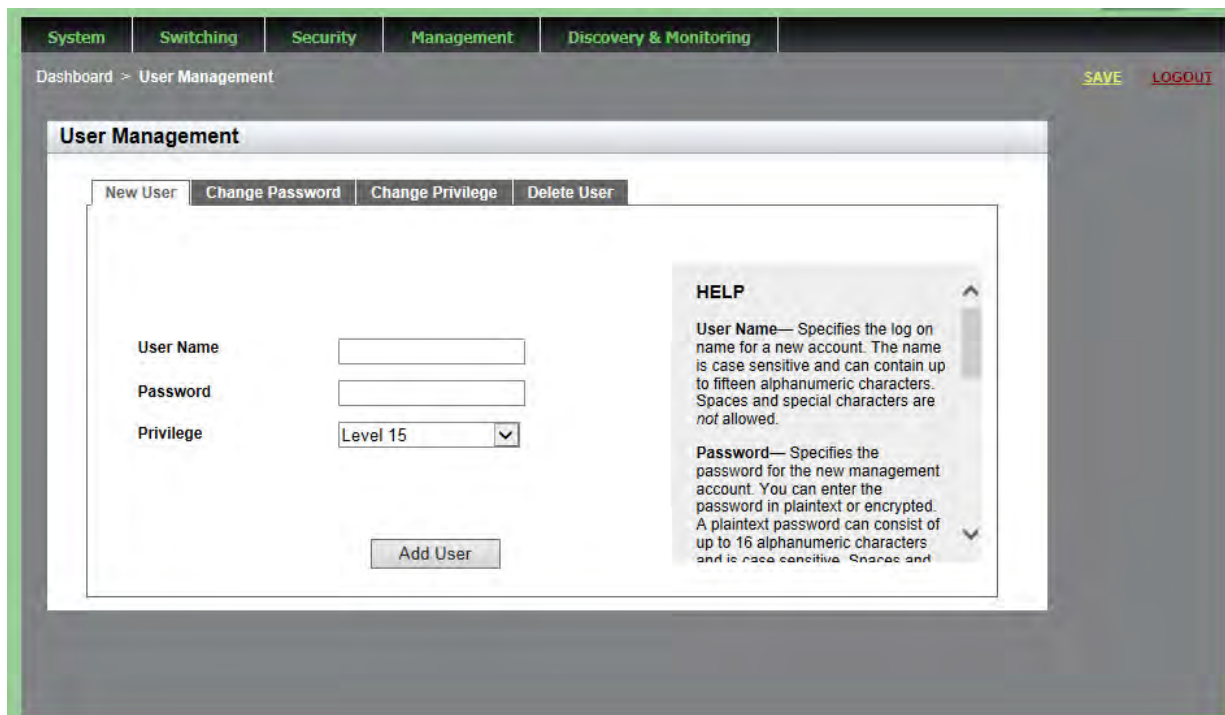


Figure 14. User Management Page

3. Enter a name in the **User Name** field.

This field specifies the log-on name for the new account. The name is case-sensitive and can contain up to fifteen alphanumeric characters. Spaces and special characters are not allowed.

4. Enter a password in the **Password** field.

This specifies the password for the new management account. You can enter the password in plaintext. A plaintext password can consist of up to 16 alphanumeric characters and is case-sensitive. Spaces and special characters are not allowed.

5. Use the pull-down menu in the **Privilege** field to select a user privilege level. Choose from the following:

- Level 15: Management accounts with a user level of 15 have unrestricted access to the software. This is the default setting.
- Level 1: Management accounts with a user level of 1 have restricted access to the software.

6. Click **Add User**.

7. Click **SAVE**.

Changing a User Password

To change a user password, do the following:

1. From the home page, hover the cursor over the **System** tab.

The System Settings Tab is displayed. See Figure 6 on page 33.

2. From the System Settings tab, select **User Management**.

The User Management page is displayed. See Figure 14 on page 44.

3. From the User Management page, select the **Change Password** tab.

The User Management page with the Change Password tab is displayed. See Figure 15 on page 46.

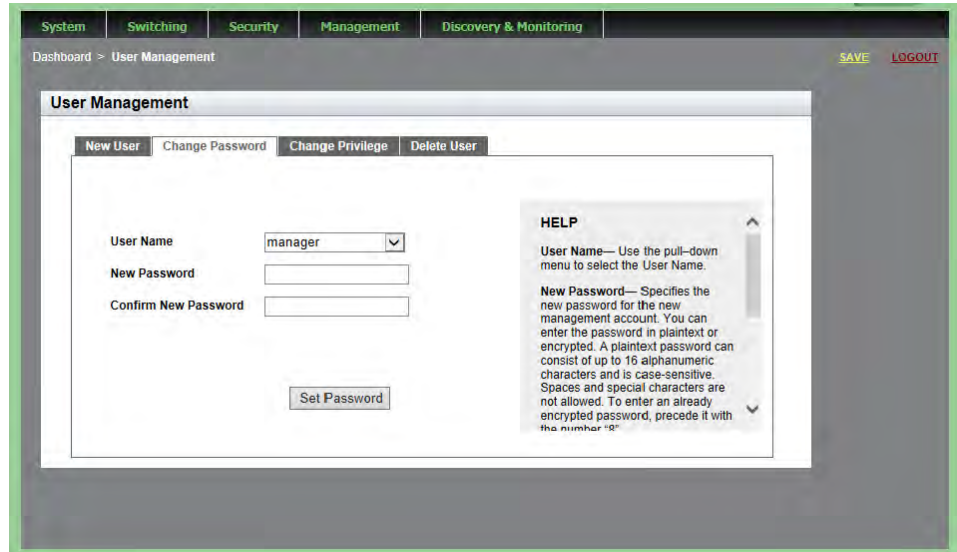


Figure 15. User Management Page with Change Password Tab

4. Use the pull-down menu next to the **User Name** field to select the username.

The username must already exist.

5. Enter a new password in the **New Password** field.

You can enter the password in plaintext. A plaintext password can consist of up to 16 alphanumeric characters and is case-sensitive. Spaces and special characters are not allowed.

6. Re-enter the new password in the **Confirm New Password** field.
7. Click **Set Password**.
8. Click **SAVE**.

Changing the User Privilege

To change the privilege of a user, do the following:

1. From the home page, hover the cursor over the **System** tab.

The System Settings Tab is displayed. See Figure 6 on page 33.

2. From the System Settings tab, select **User Management**.

The User Management page is displayed. See Figure 14 on page 44.

3. From the User Management page, select the **Change Privilege** tab.

The User Management page with the Change Privilege tab is displayed. See Figure 16.

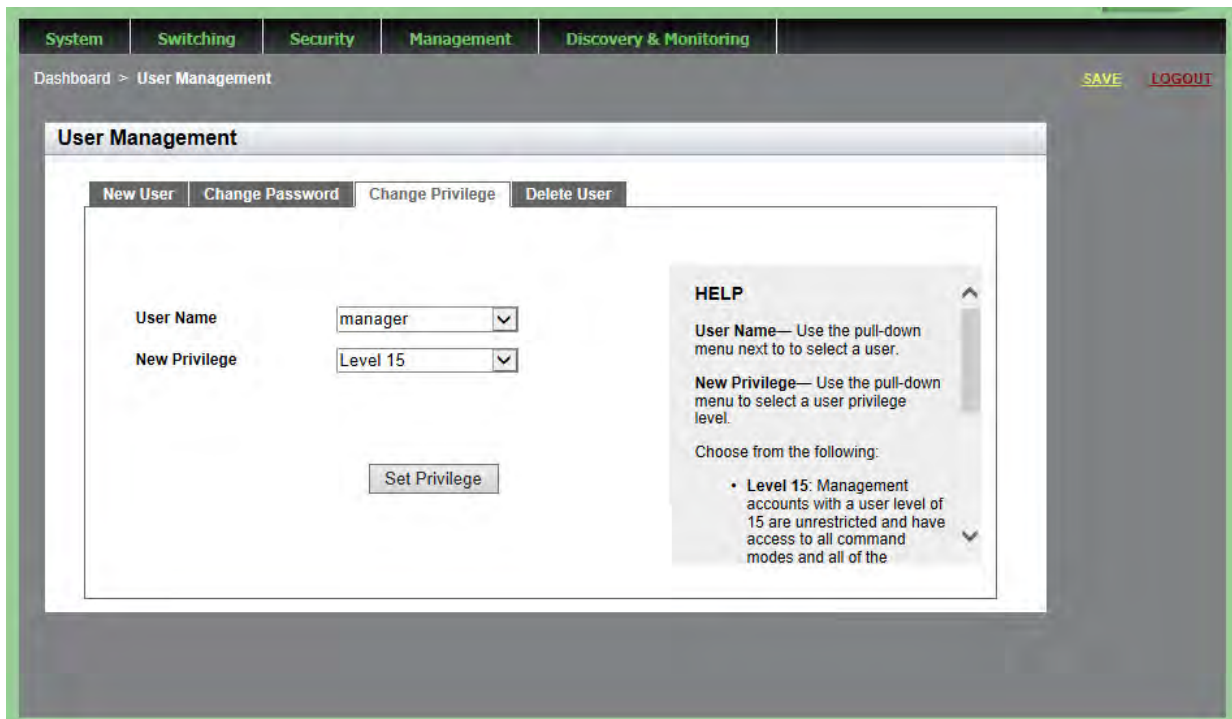


Figure 16. User Management Page with Change Privilege Tab

4. Use the pull-down menu next to the **User Name** field to select a user.
5. Use the pull-down menu next the **New Privilege** field to select a user privilege level. Choose from the following:
 - Level 15: Management accounts with a user level of 15 have unrestricted access to the software. This is the default setting.

- ❑ Level 1: Management accounts with a user level of 1 have restricted access to the switch.

6. Click **Set Privilege**.
7. Click **SAVE** to save your changes to the start-up configuration file.

Deleting a User

To delete a username from the switch, do the following:

1. From the home page, hover the cursor over the **System** tab.
The System Settings Tab is displayed. See Figure 6 on page 33.
2. From the System Settings tab, select **User Management**.
The User Management page is displayed. See Figure 14 on page 44.
3. From the User Management page, select the **Delete User** tab.
The User Management page with the Delete User tab is displayed. See Figure 17.

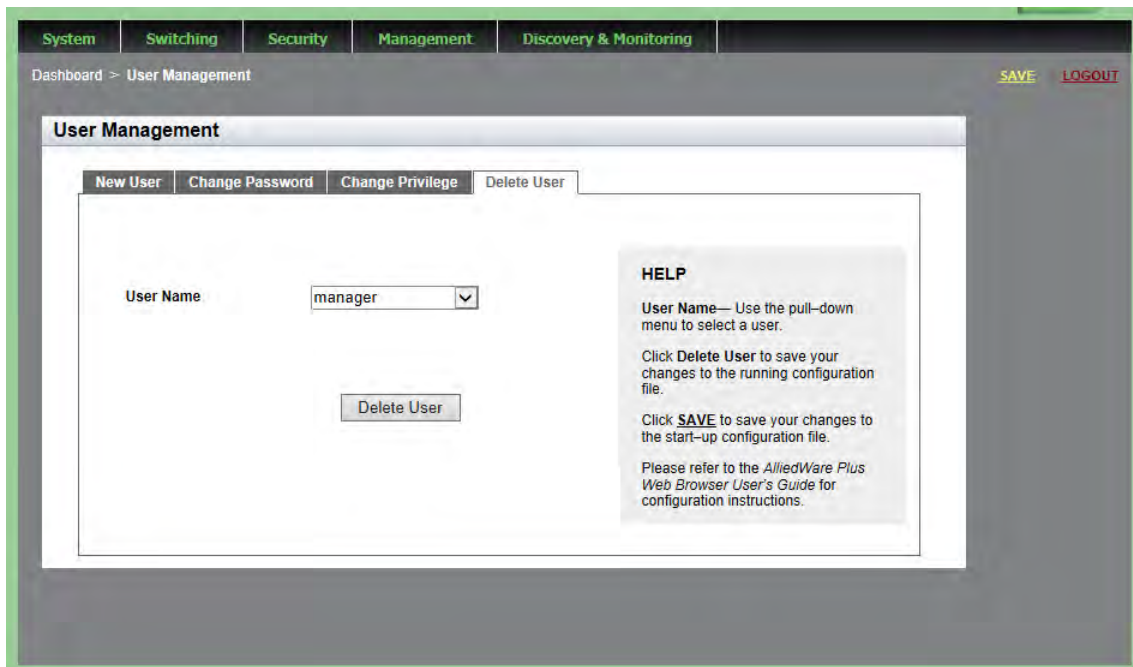


Figure 17. User Management Page with Delete User Tab

4. Use the pull-down menu to select a user.
5. Click **Delete User**.
6. Click **SAVE**.

Rebooting a Switch

Resetting the switch ends your web browser management session. To continue managing the switch, you must log in again.

Note

All unsaved changes are discarded when you reset a switch. To save your changes, click **SAVE** on the home page.

To reboot a switch, perform the following procedure:

1. Hover the cursor over the **System Tab**.

The System Settings Tab is displayed. See Figure 6 on page 33.

2. From the drop-down menu, select **Dashboard**.

The Dashboard Page is displayed. See Figure 4 on page 23.

3. Click **Reboot** at the bottom of the page.

A confirmation prompt is displayed that indicates that the connection to the web is lost during a reboot.

4. Click **OK** to reset the switch or **Cancel** to cancel the procedure.

Note

The switch does not forward packets while it initializes the AlliedWare Plus software and loads its active configuration file. This process takes between 20 seconds to 2 minutes to complete, depending on the number and types of commands in the configuration file.

Upgrading the Software

You can obtain the latest version of the AlliedWare Plus software from the Allied Telesis web site. You must have access to a TFTP server from your PC to upgrade the AlliedWare Plus software on your switch. Allied Telesis does not include this application with the software. The upgrade process takes approximately three minutes.

Upgrading the system software on the switch ends your current web browser management session. To continue managing the switch, you must log in again.

Note

All unsaved changes are discarded when you upgrade the software on a switch. To save your changes, click **SAVE**.

To upgrade the AlliedWare Plus software, perform the following procedure:

1. Open your TFTP server software and provide it with the IP address of your PC.

2. Hover the cursor over the **System Tab**.

The System Settings Tab is displayed. See Figure 6 on page 33.

3. From the drop-down menu, select **Dashboard**.

The Dashboard Page is displayed. See Figure 4 on page 23.

4. Click **System Upgrade** at the bottom of the page.

The System Upgrade page is displayed. See Figure 18 on page 51.

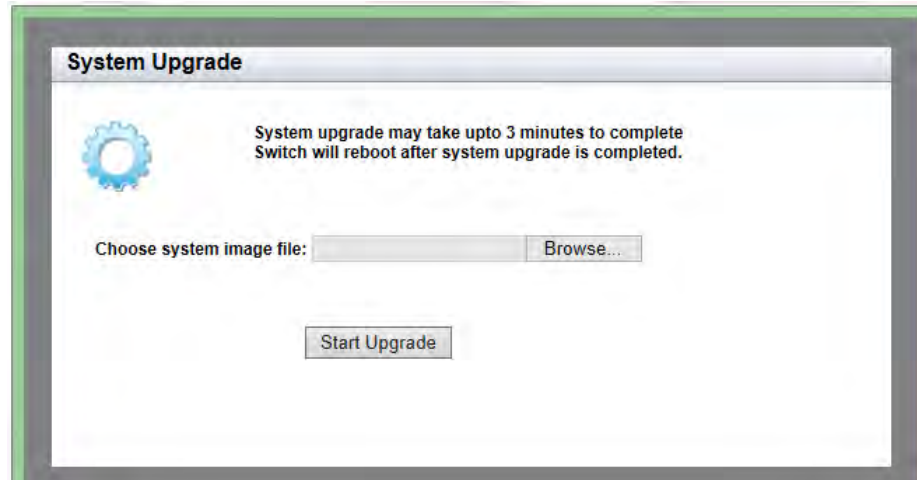


Figure 18. System Upgrade Page

5. Click **Browse** to select an image file from your PC.
6. Click **Open** to select a file.
7. Click **Start Upgrade** to begin the software upgrade or close the System Upgrade page to cancel the procedure.

Returning the AlliedWare Plus Configuration to the Factory Default Values

To reset the AlliedWare Plus Management Software parameters to their default values, you must use the Command Line Interface. You cannot reset the management software to its factory settings in the web interface. For instructions, see the *Basic Switch Management* chapter in the *AlliedWare Plus Management Software Command Line User's Guide* on our web site. To locate manuals online, see "Downloading Management Software and Web-based Guides" on page 13.

Displaying System Information

To view basic information about the switch, do the following:

1. Hover the cursor over the **System** Tab.
2. From the drop-down menu, click **Dashboard**.

The Dashboard Page is displayed. See Figure 4 on page 23.

The following fields are displayed:

- ❑ **Up Time**— Length of time since the switch was last reset or power cycled in days, hours, minutes and seconds.

The System section displays the following information:

- ❑ **Software Version**— Software version number of the AlliedWare Plus software.
- ❑ **Build Date/Time**— Month, date, year and time (in the hour:minute:second format) the software version was built.
- ❑ **Serial No.**— Unique serial number of the switch.
- ❑ **MAC Address**— MAC address of the switch.
- ❑ **IPv4 Address**— IPv4 management address assigned to the switch and subnet mask of the web interface. The address is specified in the following format:

xxx.xxx.xxx.xxx

Each “xxx” is a decimal number from 0 to 255. The numbers must be separated by periods.

Note

For both the IPv4 and IPv6 addresses, the subnet mask is a decimal number that represents the number of bits, from left to right, that constitute the network portion of the address. Here are some examples:

- The decimal mask 16 is equivalent to the mask 255.255.0.0.
 - The decimal mask 24 is equivalent to the mask 255.255.255.0
 - The IPv6 decimal mask 24 is equivalent to the mask FFFF:FF00::0.
-

- ❑ **IPv4 Gateway**— IPv4 address of the next hop of the switch's default route. The switch uses a default route to reach a remote subnet.
- ❑ **System Name**— Name of the switch. To configure this field, see “Setting the Switch Information” on page 40.

- ❑ **System Contact**— Contact person for the switch. To configure this field, see “Setting the Switch Information” on page 40.
- ❑ **System Location**— Location of the switch. To configure this field, see “Setting the Switch Information” on page 40.
- ❑ **Management VLAN**— Management VLAN assigned to the switch. The default VLAN is “VLAN1.”
- ❑ **IPv6 Gateway**— IPv6 address of the next hop of the switch’s default route. The switch uses a default route to reach a remote subnet.
- ❑ **IPv6 Address**— IPv6 address and subnet mask of the web interface. An IPv6 management address for the switch is entered in the following format:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

Where “n” is a hexadecimal digit from 0 to F. The eight groups of digits are separated by colons. Groups where all four digits are “0” can be omitted. Leading “0”s in groups can also be omitted. For example, the following IPv6 addresses are equivalent:

12c4:421e:09a8:0000:0000:0000:00a4:1c50

12c4:421e:9a8::a4:1c50

The Services section displays the following information:

- ❑ **SNMP**— SNMP setting of the switch.
- ❑ **HTTP**— HTTP setting of the switch
- ❑ **Telnet**— Indicates if Telnet is enabled or disabled on the switch.
- ❑ **SSH**— Indicates if SSH is enabled or disabled on the switch.
- ❑ **Spanning Tree**— Indicates if STP, RSTP, or MSTP is enabled on the switch. The default setting is “RSTP.”
- ❑ **QoS**— Indicates if QoS is enabled or disabled on the switch.
- ❑ **LLDP**— Indicates if LLDP is enabled or disabled on the switch.
- ❑ **SFLOW**— Indicates if sFlow is enabled or disabled on the switch.
- ❑ **802.1x Port Authentication**— Indicates if 802.1x Port Authentication is enabled or disabled on the switch.
- ❑ **Remote Logging**— Indicates if the remote log is enabled or disabled on the switch.
- ❑ **IGMP Snooping**— Indicates if IGMP Snooping is enabled or disabled on the switch.

The Administration Options section displays the following information:

- ❑ **System Upgrade**— Click this field to upgrade your system software. See “Upgrading the Software” on page 50.
- ❑ **Reboot**— Click this field to reboot the switch. For instructions, see “Rebooting a Switch” on page 49.

Chapter 4

Setting Port Parameters

This chapter describes how to display and modify the port settings, such as back pressure and flow control. In addition, it provides procedures to display and modify storm control settings.

This chapter contains the following sections:

- ❑ “Displaying the Port Parameters” on page 58
- ❑ “Changing the Port Settings” on page 62
- ❑ “Displaying the Storm Control Settings” on page 66
- ❑ “Modifying the Storm Control Settings” on page 68

For additional information about the port parameters and the storm control feature, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ Port Parameters
- ❑ Port Parameter Commands

Displaying the Port Parameters

The port numbering system in the AlliedWare Plus web browser interface has the format shown in Figure 19.

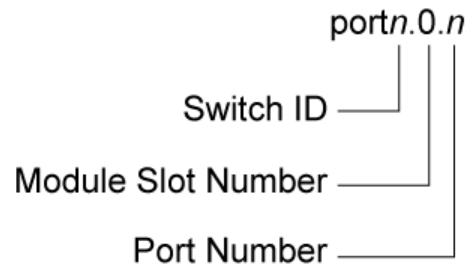


Figure 19. Port Numbering System

The port numbering system is defined as follows:

- ❑ **Switch ID:** This number is used if the switch supports stacking. It is the switch's ID number in a stack. This number is always 1 for AT-9000 Series switches because they do not support stacking.
- ❑ **Module Slot ID:** This number is used for modular switches that have slots for networking modules. It is used to identify the networking modules by their slot numbers. This number is always 0 for AT-9000 Series switches because they are not modular switches.
- ❑ **Port number:** This is a port number.

For example, port 1 would be displayed as `port1.0.1`.

Within the display, there is no differentiation between ports 25 through 28 and ports 25R through 28R. In the web interface, if you want to see if port 25 is connected versus port 25R, go to the home page and look at the illustration of the switch. For an example of the home page, see Figure 4 on page 23.

To display the settings for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.



Figure 20. Switching Tab with Port Tab

- From the Switching tab, hover over **Port**.

The Port tab expands to the right.

- From the Port tab, move the cursor to the right and select **Port Configuration** from the drop-down menu.

The Port Configuration page is displayed. See Figure 21.

Dashboard > Switching > Port > Port Configuration [SAVE](#) [LOGOUT](#)

Port Configuration

| | Interface | Type | Status | Link | Negotiation | Speed | Duplex | Polarity | Back Pressure | Back Pressure Limit | Flow Control | Flow Control Limit |
|----------------------|------------|---------|---------|------|-------------|-------|--------|----------|---------------|---------------------|--------------|--------------------|
| Edit | port1.0.1 | 1000-TX | Enabled | Up | Auto | 100mb | Full | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.2 | 1000-TX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.3 | 1000-TX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.4 | 1000-TX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.5 | 1000-TX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.6 | 1000-TX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.7 | 1000-TX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.8 | 1000-TX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.9 | 1000-FX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.10 | 1000-FX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.11 | 1000-FX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |
| Edit | port1.0.12 | 1000-FX | Enabled | Down | Auto | | | AUTO | Disabled | 7935 | Disabled | 7935 |

Figure 21. Port Configuration Page

4. The following fields are displayed:
- Interface**— Port number.
 - Type**— Indicates if the port is fiber or copper. If fiber: 1000Base-SX/LX/CX; if copper: 10/100/1000Base-T.
 - Status**— Indicates if the port is enabled or disabled. The default setting is “Enabled.” Disabling ports turns off their receivers and transmitters so that they cannot forward traffic.
 - Link**— Indicates whether the port has successfully connected to a port on another switch or unit.
 - Negotiation**— Indicates Autonegotiation or Manual. By default, Autonegotiation is enabled.
 - Speed**— Speed of the port. The default setting is “1 Gbps” for 1000Mbps. The other possible options are 10Mbps and 100Mbps.
 - Duplex**— Duplex mode of the twisted pair ports or Auto Negotiation. The three settings are half, full, and Auto Negotiation.
 - Polarity**— Indicates if the port’s wiring configuration is MDI (medium dependent interface) or MDI-X (medium dependent interface crossover). This setting only applies to a twisted pair port that is operating at 10 or 100 Mbps.

Note

You can enable or disable backpressure on ports where you disabled Auto-Negotiation, and set the speeds and duplex modes manually to 10 or 100 Mbps in half-duplex mode.

- Back Pressure**— Indicates if back pressure is enabled or disabled on a port. Backpressure is used by ports during periods of packet congestion to temporarily stop their network counterparts from transmitting more packets. This prevents a buffer overrun, and the subsequent loss and retransmission of network packets. A port initiates backpressure by transmitting on the shared link to cause a data collision, which causes its link partner to cease transmission. The default setting is “Disabled.”
- Back Pressure Limit**— Indicates the threshold level for back pressure on a port. Specifies the number of cells for back pressure. The default value is 7935 cells.

- ❑ **Flow Control**— Indicates if flow control (send and receive) is enabled or disabled on a port. When flow control is enabled, a port sends pause packets when it reaches the point of packet congestion. Also, the port stops transmitting packets when it receives pause packets from its local or remote counterpart. When flow control is disabled, the port sends pause packets regardless of packet congestion. In addition the port continues transmitting packets when it receives pause packets from its local or remote counterpart. The default is “Disabled.”
- ❑ **Flow Control Limit**— Indicates the threshold level for flow control on a port. The default value is 7935.

Changing the Port Settings

You can change the settings of one port at a time. Use the following procedure to change the port settings or reset a port to its default value.

To change the port settings, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.

The Port tab expands to the right.

3. From the Port tab, move the cursor to the right and select **Port Configuration**.

The Port Configuration page is displayed. See Figure 21 on page 59.

4. Click Edit next to the port that you want to modify.

The Port Configuration Modify page is displayed. See Figure 22 on page 63.

System Switching Security Management Discovery & Monitoring

Home > Port Configuration > Modify SAVE LOGOUT

Port Configuration

| | |
|------------------------------|---|
| Interface | port1.0.1 |
| Port Type | 1000-TX |
| Status | Enabled <input type="button" value="v"/> |
| Negotiation | Auto <input type="button" value="v"/> |
| Speed | 100mb <input type="button" value="v"/> |
| Duplex Mode | Full <input type="button" value="v"/> |
| Polarity | AUTO <input type="button" value="v"/> |
| Back Pressure Status | Disabled <input type="button" value="v"/> |
| Back Pressure Limit (1-7935) | 7935 |
| Flow Control Status | Disabled <input type="button" value="v"/> |
| Flow Control Limit (1-7935) | 7935 |

HELP

Interface— Indicates the port number.

Port Type— Specifies the if the port is fiber, indicated by 1000-FX, or copper, indicated by 100-FX.

Status— Indicates if the port is enabled or disabled. The default setting is Enabled. Disabling ports turns off their receivers and transmitters so that they cannot forward traffic.

Negotiation— Indicates the state of Auto Negotiation on a port. Select "Auto" to enable Auto Negotiation on a port or "Manual" to disable Auto Negotiation. The default setting is Auto. When the setting for this field is "Auto," the Speed and Duplex fields are brown and you cannot select them. To change the Speed and Duplex Mode fields, change the Negotiation setting to "Manual."

Speed— Specifies the speed of the port. The default setting is "1000-FX" for 1000Mbps. The other

Figure 22. Port Configuration Modify Page

5. Configure the following parameters as needed:

- Interface**— Port number. You cannot modify this field.
- Port Type**— Type of port, fiber or copper. You cannot modify this field.
- Status**— Specifies if the port is enabled or disabled. Choose between "Enabled" or "Disabled." The default setting is "Enabled." Disabling ports turns off their receivers and transmitters so that they cannot forward traffic. You may want to disable a port if there is a problem with a cable or network device.

- ❑ **Negotiation**— State of Auto Negotiation on a port. Select “Auto” to enable Auto Negotiation on a port or “Manual” to disable Auto Negotiation. The default setting is Auto. When the setting for this field is “Auto,” the Speed and Duplex fields change from white to brown, and you cannot select them. To change the Speed and Duplex Mode fields, change the Negotiation setting to “Manual.”
- ❑ **Speed**— Port speed. Select 10mb, 100mb, or 1000mb.
- ❑ **Duplex Mode**— Sets the duplex modes of the twisted pair ports or activates Auto-Negotiation manually. The settings are half, full, or Auto Negotiation. Ports operating in half-duplex mode can either receive or transmit packets, but not both at the same time. Ports operating in full-duplex can both send and receive packets, simultaneously.
- ❑ **Polarity**— Sets the wiring configuration of the twisted pair ports when they are operating at 10 or 100 Mbps, in either half- or full-duplex mode.

A twisted pair port that is operating at 10 or 100 Mbps can have one of two wiring configurations. The configurations are known as MDI and MDI-X. To forward traffic, a port on the switch and a port on a network device must have different settings. For instance, the wiring configuration of a switch port has to be MDI if the wiring configuration on a port on a network device is MDIX.

To set this parameter on a port, you must set the speed and duplex mode manually. A port that is using Auto-Negotiation sets its wiring configuration automatically using auto-MDI/MDIX.

- ❑ **Back Pressure Status**— Activates or deactivates back pressure on the ports. Use this field to enable or disable back pressure on ports that are operating at 10 or 100 Mbps in half-duplex mode. Back pressure is used by ports during periods of packet congestion to temporarily stop their network counterparts from transmitting more packets. This prevents a buffer overrun and the subsequent loss and retransmission of network packets. A port initiates back pressure by transmitting on the shared link to cause a data collision, which causes its link partner to cease transmission.
- ❑ **Back Pressure Limit (1 - 7935)**— Threshold level for back pressure on a port. Specifies the number of cells for back pressure. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.
- ❑ **Flow Control Status**— Enables or disables the flow control feature. By default, flow control is disabled on a port.
- ❑ **Flow Control Limit (1 - 7935)**— Threshold levels for flow control on the ports. Specifies the number of cells for flow control. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.

6. To set the port to the default port value, click **Default**. Otherwise, skip this step.
7. Click **Apply**.
8. Click **SAVE**.

Displaying the Storm Control Settings

To display the storm control settings, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.

The Port tab expands to the right.

3. From the Port tab, move the cursor to the right and select **Storm Control**.

The Storm Control List page is displayed. See Figure 23.

| | Interface | Broadcast | Broadcast Level | Multicast | Multicast Level | Dif | Dif Level |
|----------------------|------------|-----------|-----------------|-----------|-----------------|-----|-----------|
| Edit | port1.0.1 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.2 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.3 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.4 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.5 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.6 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.7 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.8 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.9 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.10 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.11 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |
| Edit | port1.0.12 | OFF | 33554431 | OFF | 33554431 | OFF | 33554431 |

Figure 23. Storm Control List Page

The following fields are displayed:

- Interface**— Port number.
- Broadcast**— Indicates whether Broadcast storm-control setting is enabled (ON) or disabled (OFF).
- Broadcast Level**— Maximum number of ingress packets per second of broadcast packets the port will forward. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
- Multicast**— Indicates whether Multicast storm-control setting is enabled (ON) or disabled (OFF).

- ❑ **Multicast Level**— Maximum number of ingress packets per second of multicast packets the port will forward. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
- ❑ **Dif**— Indicates whether unknown unicast storm-control setting is Enabled (ON) or Disabled (OFF).
- ❑ **Dif Level**— Maximum number of ingress packets per second of unknown unicast packets the port forwards. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.

Modifying the Storm Control Settings

To modify the storm control settings, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.

The Port tab expands to the right.

3. From the Port tab, move the cursor to the right and select **Storm Control**.

The Storm Control List page is displayed. See Figure 23 on page 66.

4. Click Edit on the port that you want to modify.

The Storm Control Settings page is displayed. See Figure 24.

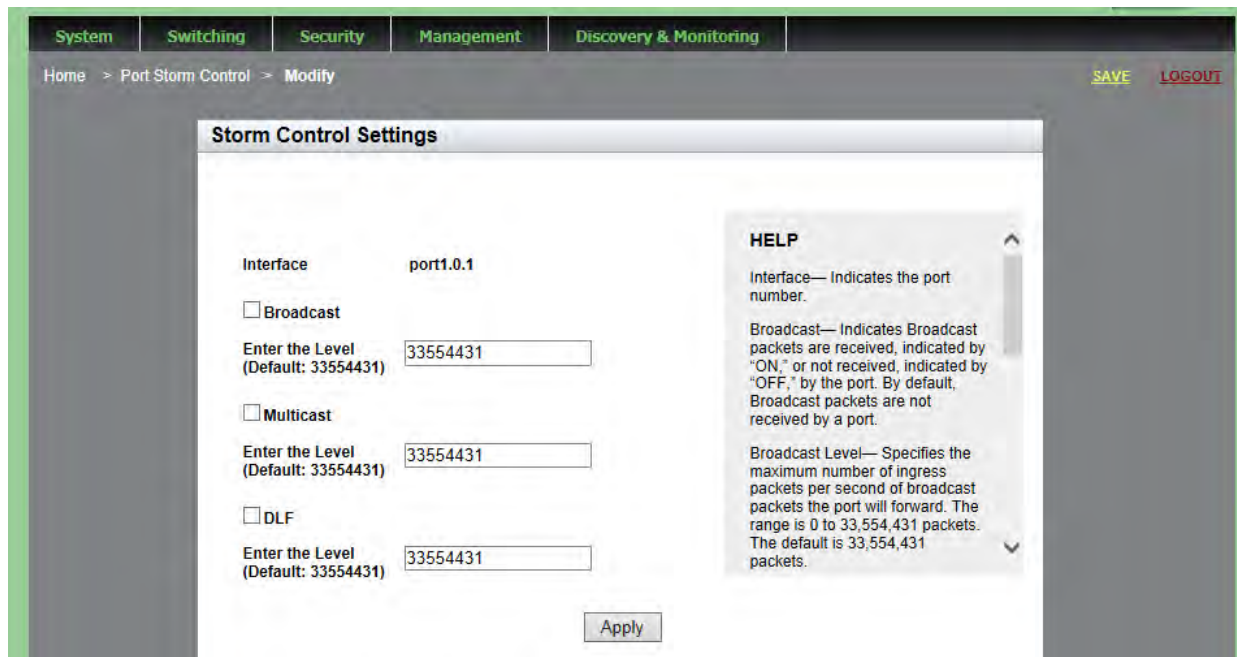


Figure 24. Storm Control Settings Page

5. Change the following fields as needed:

- Interface**— Indicates the port number. You cannot change this field.
- Broadcast**— Specifies Broadcast packets are received by the port: “ON”, or not received by the port: “OFF”. By default, Broadcast packets are not received by a port.
- Broadcast Level**— Maximum number of ingress packets per second of broadcast packets the port will forward. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
- Multicast**— Specifies multicast packets are “ON” or “OFF” on the port. By default, this field is set to “OFF” which indicates multicast packets are *not* received by a port.
- Multicast Level**— Maximum number of ingress packets per second of multicast packets the port forwards. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
- DLF**— Specifies unknown unicast packets are “ON” or “OFF” on the port. By default, the setting is “ON” indicating that unknown unicast packets are received by a port.
- DLF Level**— Maximum number of ingress packets per second of unknown unicast packets the port forwards. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.

6. Click **Apply**.

7. Click **SAVE**.

Chapter 5

Setting Port Statistics

This chapter describes how to display and clear port statistics. Within the AlliedWare Plus software, you can display and clear transmit, receive, and interface port statistics.

This chapter contains the following topics:

- ❑ “Displaying Port Statistics” on page 72
- ❑ “Clearing Port Statistics” on page 79
- ❑ “Refreshing Port Statistics” on page 80

For additional information about port statistics, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ Port Parameters
- ❑ Port Parameter Commands

Displaying Port Statistics

You can display several types of port statistics. See the following sections:

- “Displaying Transmit and Receive Port Statistics”
- “Displaying Receive Statistics” on page 73
- “Displaying Transmit Statistics” on page 75
- “Displaying Interface Statistics” on page 77

Displaying Transmit and Receive Port Statistics

To display the transmit and receive statistics for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.
The Switching tab is displayed. See Figure 20 on page 59.
2. From the Switching tab, hover over **Port**.
3. Move the cursor to the right and select **Statistics**.

The Port Statistics page is displayed with the Tx + Rx tab automatically selected. See Figure 25.

| | Interface | 0-64 Byte Frames | 65-127 Byte Frames | 128-255 Byte Frames | 256-511 Byte Frames | 512-1023 Byte Frames | 1024-1518 Byte Frames | 1519-1522 Byte Frames |
|-----------------------|------------|------------------|--------------------|---------------------|---------------------|----------------------|-----------------------|-----------------------|
| Clear | port1.0.1 | 768 | 172 | 20 | 43 | 33 | 174 | 0 |
| Clear | port1.0.2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Figure 25. Port Statistics Page with Tx + Rx Tab

The following fields are displayed:

- ❑ **Interface**— Port number.
- ❑ **0-64 Byte Frames**— Number of frames transmitted by the port that contain 0 to 64 bytes.
- ❑ **65-127 Byte Frames**— Number of frames transmitted by the port that contain 65 to 127 bytes.
- ❑ **128-255 Byte Frames**— Number of frames transmitted by the port that contain 128 to 255 bytes.
- ❑ **256-511 Byte Frames**— Number of frames transmitted by the port that contain 256 to 511 bytes.
- ❑ **512-1023 Byte Frames**— Number of frames transmitted by the port that contain 512 to 1023 bytes.
- ❑ **1024-1518 Byte Frames**— Number of frames transmitted by the port that contain 1024 to 1518 bytes.
- ❑ **1519-1522 Byte Frames**— Number of frames transmitted by the port that contain 1519 to 1522 bytes.

Displaying Receive Statistics

To display the statistics on the Receive Statistics tab, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.
3. Move the cursor to the right and select **Statistics**.

The Port Statistics page with the Tx + Rx tab selected is displayed. See Figure 25 on page 72.

4. Click on the **Receive** Tab.

The Port Statistics with the Receive tab selected is displayed. See Figure 26 on page 74.

| | Interface | Total Bytes | Total Frames | Total Error Frames | Multicast Frames | Broadcast Frames | CRC Error Frames | FCS Error Frames | Pause Frames | Oversized Frames | Fragmented Frames | Jabber Frames |
|-----------------------|------------|-------------|--------------|--------------------|------------------|------------------|------------------|------------------|--------------|------------------|-------------------|---------------|
| Clear | port1.0.1 | 61329 | 517 | 0 | 28 | 184 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Figure 26. Port Statistics with Receive Tab

The following fields are displayed:

- Interface**— Port number.
- Total Bytes**— Number of received bytes.
- Total Frames**— Number of received frames.
- Total Error Frames**— Total number of received frames with errors.
- Multicast Frames**— Number of received multicast frames.
- Broadcast Frames**— Number of received broadcast frames.
- CRC Frame Errors**— Number of frames with a cyclic redundancy check (CRC) error, but with the proper length (64 -1518 bytes) received by the port.
- FCS Error Frames**— Number of ingress frames that had frame check sequence (FCS) errors.
- Pause Frames**— Number of received flow control pause frames.
- Oversize Frames**— Number of received frames that exceeded the maximum size as specified by IEEE 802.3 (1518 bytes including the CRC).

- ❑ **Fragmented Frames**— Number of undersized frames and frames with alignment errors.
- ❑ **Jabber Frames**— Number of occurrences of corrupted data or useless signals the port has encountered.

Note

The following fields are not displayed in Figure 26 on page 74.

- ❑ **Undersize Frames**— Number of received frames that were less than the minimum length as specified by IEEE 802.3 (64 bytes including the CRC).
- ❑ **Dropped Frames**— Number of frames successfully received and buffered by the port, but discarded and not forwarded.
- ❑ **MTU Exceed Discarded Frames**— Number of received frames with an MTU that exceeds the MTU of the switch. These frames are discarded.
- ❑ **MAC Error Frames**— Number of Receive Error events seen by the receive side of the MAC.

Displaying Transmit Statistics

To display the statistics on the Transmit Statistics tab, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.
3. Move the cursor to the right and select **Statistics**.

The Port Statistics page with the Tx + Rx tab selected is displayed. See Figure 25 on page 72.

4. Click the **Transmit** tab.

The Port Statistics with the Transmit tab selected is displayed. See Figure 27.

| | Interface | Total Byte | Total Frames | Total Error Frames | Multicast Frames | Broadcast Frames | Pause Frames Sent | Deferred | Single Collision | Multi Collision | Late Collision | Excessive Collision |
|-----------------------|------------|------------|--------------|--------------------|------------------|------------------|-------------------|----------|------------------|-----------------|----------------|---------------------|
| Clear | port1.0.1 | 301497 | 693 | 0 | 415 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Figure 27. Port Statistics with Transmit Tab

The following fields are displayed:

- Interface**— Port number.
- Total Bytes**— Number of transmitted bytes.
- Total Frames**— Number of transmitted frames.
- Total Error Frames**— Number of transmitted frames with errors.
- Multicast Frames**— Number of transmitted multicast frames.
- Broadcast Frames**— Number of transmitted broadcast frames.
- Pause Frames Sent**— Number of transmitted flow control pause frames.
- Deferred**— Number of egress frames that the port could not immediately transmit.
- Single Collision**— Number of frames that were transmitted after at least one collision.
- Multi Collision**— Number of frames that were transmitted after more than one collision.
- Late Collision**— Number of late collisions.
- Excessive Collision**— Number of excessive collisions.

Note

The following fields are not displayed in Figure 27 on page 76.

- ❑ **Total Collision Frames**— Total number of collisions on the port.
- ❑ **MAC Error Frames**— Number of frames not transmitted correctly or dropped due to an internal MAC transmit error.

Displaying Interface Statistics

To display the interface statistics, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.
3. Move the cursor to the right and select **Statistics**.

The Port Statistics page with the Tx + Rx tab selected is displayed. See Figure 25 on page 72.

4. Click the **Interface** tab.

The Port Statistics Page with the Interface tab selected is displayed. See Figure 28.

| | Interface | Rx Unicast Packets | Rx Discard Packets | Rx IP Header Error Packets | Tx Unicast Packets | Tx Discard Packets | TX Error Packets |
|-----------------------|------------|--------------------|--------------------|----------------------------|--------------------|--------------------|------------------|
| Clear | port1.0.1 | 305 | 204 | 0 | 278 | 4 | 0 |
| Clear | port1.0.2 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.3 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.4 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.5 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.6 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.7 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.8 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.9 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.10 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.11 | 0 | 0 | 0 | 0 | 0 | 0 |
| Clear | port1.0.12 | 0 | 0 | 0 | 0 | 0 | 0 |

Figure 28. Port Statistics Page with Interface Tab

The following fields are displayed:

- ❑ **Interface**— Port number.
- ❑ **Rx Unicast Packets**— Number of ingress unicast packets.
- ❑ **Rx Discard Packets**— Number of ingress packets that were discarded prior to transmission because of an error.
- ❑ **Rx IP Header Error Packets**— Number of ingress packets that were discarded because of an IP Header error.
- ❑ **Tx Unicast Packets**— Number of egress unicast packets.
- ❑ **Tx Discard Packets**— Number of egress packets that were discarded prior to transmission because of an error.
- ❑ **Tx Error Packets**— Number of egress error packets.

Clearing Port Statistics

To clear the statistics for a port, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.
3. Move the cursor to the right and select **Statistics**.

The Port Statistics Page with Tx + Rx tab selected is displayed. See Figure 25 on page 72.

4. Select the desired Port Statistics tab. Choose from the following:
 - Tx+Rx**— Displays the transmit and receive statistics. (This is the default.)
 - Receive**— Displays the receive statistics.
 - Transmit**— Displays the transmit statistics.
 - Interface**— Displays the interface statistics.
5. Click **Clear** on the port that you want to clear.

Refreshing Port Statistics

To refresh the port statistics, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.
3. Move the cursor to the right and select **Statistics**.

The Port Statistics Page with Tx + Rx tab selected is displayed. See Figure 25 on page 72.

4. Select the desired Port Statistics tab. Choose from the following:
 - Tx+Rx**— Displays the transmit and receive statistics. (This is the default.)
 - Receive**— Displays the receive statistics.
 - Transmit**— Displays the transmit statistics.
 - Interface**— Displays the interface statistics.
5. Click the **Reload Page** button.

Chapter 6

Setting Port Mirroring

The port mirror is a management tool that allows you to monitor the traffic on one or more ports on the switch. It works by copying the traffic from designated ports to another port where the traffic can be monitored with a network analyzer. The port mirror can be used to troubleshoot network problems or to investigate possible unauthorized network access. The performance and speed of the switch is not affected by the port mirror.

This chapter provides a brief description of the port mirroring feature and explains how to display and set port mirroring. See the following sections:

- ❑ “Overview” on page 82
- ❑ “Displaying Port Mirroring Settings” on page 83
- ❑ “Assigning a Destination Port” on page 85
- ❑ “Specifying Direction Type” on page 86

For more information about port mirroring, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User's Guide*:

- ❑ Port Mirror
- ❑ Port Mirror Commands

Overview

To use the port mirroring feature, you must designate one or more source ports and one destination port. The source ports are the ports whose packets are mirrored and monitored. The destination port is the port where the packets from the source ports are copied and where the network analyzer is connected. There can be only one destination port on the switch.

Here are guidelines for setting the port mirroring feature:

- ❑ The switch supports only one mirroring port.
- ❑ Port mirroring can have one destination port.
- ❑ Port mirroring can have more than one source port. This allows you to monitor the traffic on multiple ports at the same time. For example, you might monitor the traffic on all the ports of a particular VLAN.
- ❑ You can select whether to mirror the receive traffic, the transmit traffic, or both, on the source ports.
- ❑ The destination port must not be a member of a static port trunk or an LACP trunk.

Displaying Port Mirroring Settings

To display the port mirroring assignments for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.

The Port tab is displayed.

3. From the Port tab, move the cursor to the right and select **Mirroring**.

The Port Mirroring List page is displayed. See Figure 29.

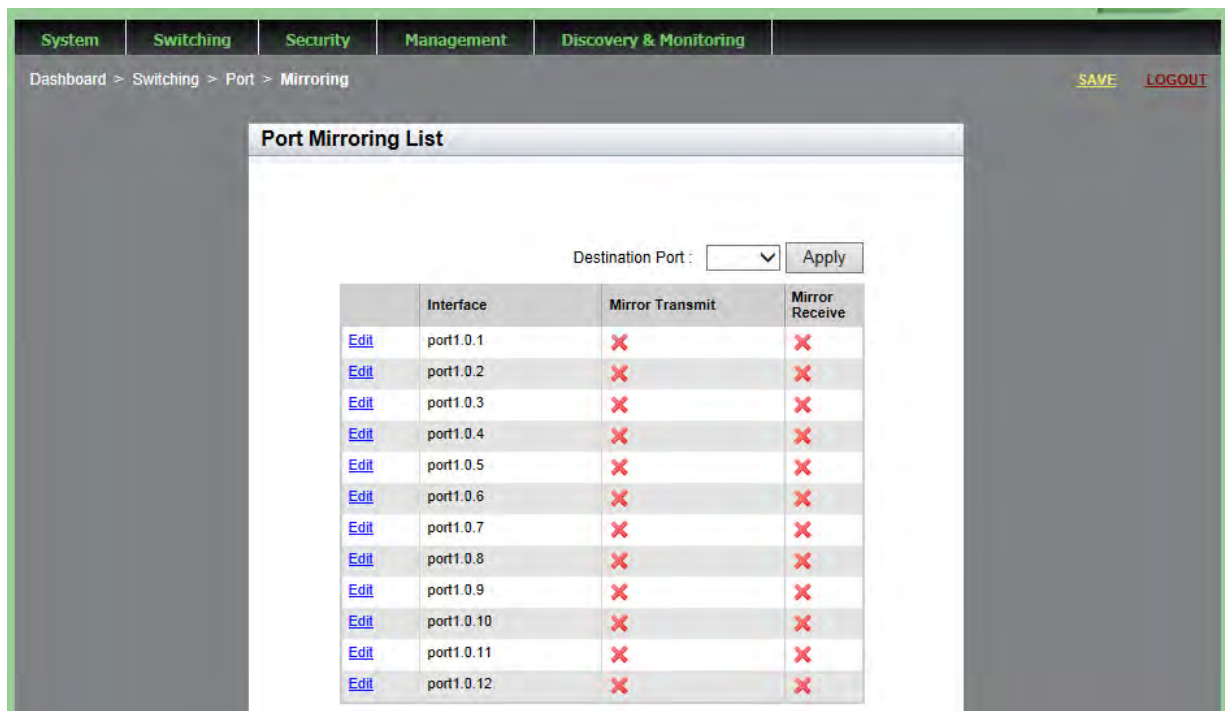


Figure 29. Port Mirroring List Page

The following fields are displayed:

- **Destination Port**— Port where the packets from the source ports are copied and where the network analyzer is connected. There can be only one destination port assigned to the switch. In Figure 29, the Destination Port has not yet been assigned.
- **Interface**— Port number.
- **Mirror Transmit**— Source port whose transmitted (egress)

packets are mirrored and monitored. In this case, transmit is the specified direction the packets mirror. There can be multiple source ports on the switch.

- ❑ **Mirror Receive**— Source port whose received (ingress) packets are mirrored and monitored. In this case, receive is the specified direction the packets mirror. There can be multiple source ports on the switch.

Assigning a Destination Port

The destination port is the source port where the packets are copied. You can only assign one destination port to the switch.

To assign a destination port, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.

The Port tab is displayed.

3. From the Port tab, move the cursor to the right and select **Mirroring** from the drop-down menu.

The Port Mirroring List page is displayed. See Figure 29 on page 83.

4. Select the pull-down menu next to the **Destination Port** field at the top of the page.

5. Click on the port that you want to designate as the destination port.

You can only assign one destination port to a switch.

6. Click **Apply**.

The **Edit** option is removed from the port. This indicates the destination port for the switch.

7. Click **SAVE**.

Specifying Direction Type

To specify source ports and type of packet direction, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.

The Port tab is displayed.

3. From the Port tab, move the cursor to the right and select **Mirroring** from the drop-down menu.

The Port Mirroring List page is displayed. See Figure 29 on page 83.

4. Click Edit next to the port that you want to specify as a transmitting or receiving port mirror.

Note

You cannot select the destination port.

The Modify Port Mirroring Page is displayed. See Figure 30.

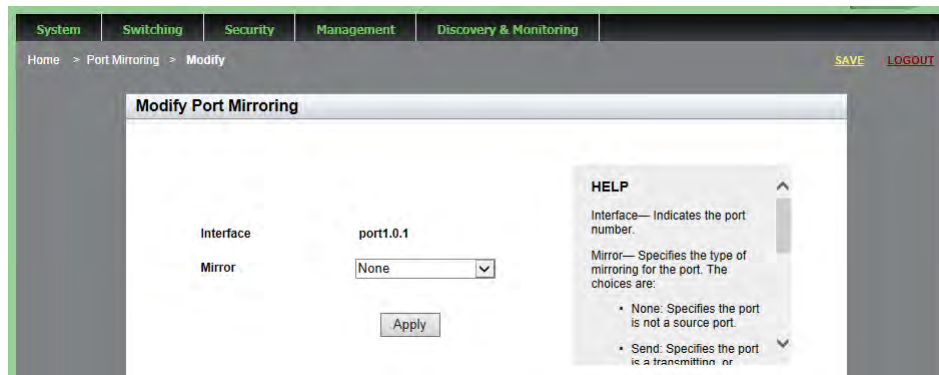


Figure 30. Modify Port Mirroring Page

Note

The **Interface** field indicates the port number.

5. Select the type of mirroring for the port. The choices are:

- None**— Port is not a source port.
- Send**— Port is a transmitting (egress) source port.
- Receive**— Port is a receiving (ingress) source port.
- Both**— Port is both a transmitting and a receiving source port.

By default, there is no mirror port assigned.

6. Click **Apply**.

7. Click **SAVE**.

Chapter 7

Setting the Port Spanning Tree Protocol

The Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP) guard against the formation of loops in an Ethernet network topology. A topology has a loop when two or more nodes can transmit packets to each other over more than one data path. Packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and that can significantly reduce network performance.

This chapter provides a brief description of the spanning tree protocols and explains how to set spanning tree on a port. See the following sections:

- ❑ “Overview” on page 90
- ❑ “Displaying Port Spanning Tree Protocol Settings” on page 91
- ❑ “Modifying Port Spanning Tree Protocol Settings” on page 93

Note

For information about how to set a spanning tree protocol for the switch, see Chapter 13, “Setting Switch Spanning Tree Protocols” on page 147.

For more information about spanning tree, see *Section VI: Spanning Tree Protocols* in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*.

Overview

STP and RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode. In addition, STP and RSTP can activate redundant paths if primary paths go down. These protocols guard against multiple links between segments and the risk of broadcast storms, and maintain network connectivity by activating backup redundant paths.

One of the primary differences between the two protocols is in the time each takes to complete the process referred to as convergence. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol determines whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain communications between the various network segments. This is the process of convergence.

With STP, convergence can take up to a minute to complete in a large network. This can result in the loss of communication between various parts of the network during the convergence process, and the subsequent loss of data packets.

RSTP is much faster than STP. It can complete a convergence in seconds, and so greatly diminish the possible impact the process can have on your network. Only one spanning tree can be active on the switch at a time. The default setting is RSTP.

Displaying Port Spanning Tree Protocol Settings

To display the Spanning Tree Protocol settings for all of the switch ports, do the following:

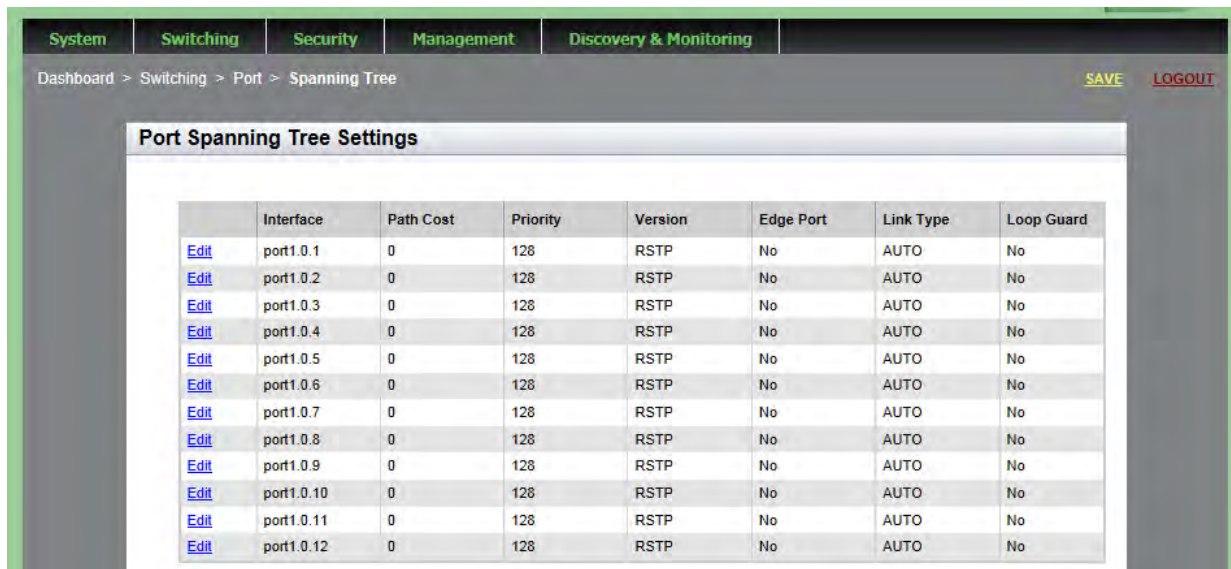
1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.

3. Move the cursor to the right and select **Spanning Tree**.

The Port Spanning Tree Settings page is displayed. See Figure 31.



| | Interface | Path Cost | Priority | Version | Edge Port | Link Type | Loop Guard |
|----------------------|------------|-----------|----------|---------|-----------|-----------|------------|
| Edit | port1.0.1 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.2 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.3 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.4 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.5 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.6 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.7 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.8 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.9 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.10 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.11 | 0 | 128 | RSTP | No | AUTO | No |
| Edit | port1.0.12 | 0 | 128 | RSTP | No | AUTO | No |

Figure 31. Port Spanning Tree Settings Page

The following fields are displayed:

- Interface**— Port number.
- Path Cost**— Cost of a port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. The lower the numeric value, the higher the priority of the path. The range is 1 to 200000000.
- Priority (0-15)**— Bridge priority number for the switch. The device with the lowest priority number in the spanning tree domain becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.

- ❑ **Version**— Spanning Tree Protocol version. (STP or RSTP). The default setting is RSTP.
- ❑ **Edge Port**— Indicates whether there are edge ports on the switch (Yes) or not (No). Edge ports are not connected to spanning tree devices or to LANs that have spanning tree devices. As a consequence, edge ports do not receive BPDUs. If an edge port starts to receive BPDUs, it is no longer considered an edge port by the switch.
- ❑ **Link Type**— Indicates whether ports are Auto, point-to-point, or shared.
- ❑ **Loop Guard**— Indicates the BPDU loop-guard feature on the ports is enabled (Yes) or disabled (No). If a port that has this feature activated stops receiving BPDU packets, the switch automatically disables it. A port that has been disabled by the feature remains in that state until it begins to receive BPDU packets again or the switch is reset. The default setting for BPDU loop-guard on the ports is disabled.

Modifying Port Spanning Tree Protocol Settings

To modify port settings for Spanning Tree Protocol, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Port**.
3. Move the cursor to the right and select **Spanning Tree**.

The Port Spanning Tree page is displayed. See Figure 31 on page 91.

4. Click Edit on the port that you want to change.

The Modify Port Spanning Tree Settings page is displayed. See Figure 32.

The screenshot shows the 'Modify Port Spanning Tree Settings' page. At the top, there are navigation tabs: System, Switching, Security, Management, and Discovery & Monitoring. Below the tabs is a breadcrumb trail: Home > Port Spanning Tree > Modify. On the right side, there are 'SAVE' and 'LOGOUT' buttons. The main content area is titled 'Modify Port Spanning Tree Settings' and contains the following fields:

- Interface:** port1.0.1
- Version:** RSTP
- Path Cost (1-200000000):** 0
- Priority (0-15) (Actual value is multiple of 16):** 8
- Edge Port:** No
- Link Type:** AUTO
- Loop Guard:** No

An 'Apply' button is located at the bottom center. On the right side, there is a 'HELP' section with the following text:

HELP

Interface— Indicates the port number.

Version— Indicates the Spanning Tree Protocol version. The default is RSTP.

Path Cost (1–200000000)— Use this field to specify the cost of a port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. The lower the numeric value, the higher the priority of the path. The range is 1 to 200000000.

Priority (0–15)— Indicates a bridge

Figure 32. Modify Port Spanning Tree Settings Page

5. Change the following settings as needed:

- Interface**— Port number. You cannot change this parameter from this page.
- Version**— Spanning Tree Protocol version. The default setting is RSTP. You cannot change this parameter from this page.

- ❑ **Path Cost (1-200000000)**— Use this field to specify the cost of a port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. The lower the numeric value, the higher the priority of the path. The range is 1 to 200000000.
- ❑ **Priority (0-15) (Actual value is multiple of 16)**— Specifies a bridge priority number for the switch. The device with the lowest priority number in the spanning tree domain becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.
- ❑ **Edge Port**— Designates the edge ports on the switch. Choose “Yes” to active an edge type or “No” to make an edge port inactive. Edge ports are not connected to spanning tree devices or to LANs that have spanning tree devices. As a consequence, edge ports do not receive BPDUs. If an edge port starts to receive BPDUs, it is no longer considered an edge port by the switch.
- ❑ **Link Type**— Choose from the following settings:

| | |
|----------------------|---|
| AUTO | If a port is set to full-duplex mode, AUTO indicates the Link Type is point-to-point. If a port is set to half-duplex mode, AUTO indicates the Link Type is shared. |
| PTP (point-to-point) | Allows for rapid transition of a port to the forwarding state during the convergence process of the spanning tree domain. |
| Shared | Disables rapid transition of a port. You may want to set the link type to shared if a port is connected to a hub with multiple switches connected to it. |
- ❑ **Loop Guard**— Specifies if the BPDU loop-guard feature on the ports is enabled (Yes) or disabled (No). If a port with the loop guard activated stops receiving BPDU packets, the switch automatically disables the port. A port that has been disabled by the feature remains in that state until it begins to receive BPDU packets again or the switch is reset. The default setting for BPDU loop-guard on the ports is disabled.

6. Click **Apply**.

7. Click **SAVE**.

Chapter 8

Setting the MAC Address

The procedures in this chapter describe how to display the MAC address table that resides on the switch, as well as how to add a unicast or multicast MAC addresses to the table. Procedures to modify and delete MAC addresses within the table are also included in this chapter.

See the following sections:

- ❑ “Displaying the MAC Address” on page 96
- ❑ “Assigning a MAC Address” on page 98
- ❑ “Deleting a MAC Address” on page 101

For more information about MAC addresses, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ MAC Address Table
- ❑ MAC Address Table Commands

Displaying the MAC Address

You can display both the unicast and multicast addresses in the MAC address table. See the following procedures:

- ❑ “Displaying Unicast MAC Addresses”
- ❑ “Displaying Multicast MAC Addresses” on page 97

Displaying Unicast MAC Addresses

To display the unicast MAC addresses, do the following:

1. Hover the cursor over the Switching Tab.

The Switching Tab is displayed. See Figure 33.

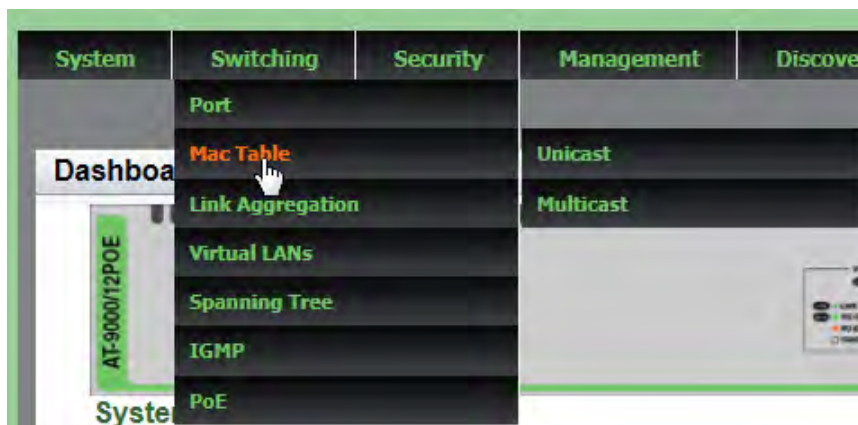


Figure 33. Switching Tab

2. Hover over **Mac Table** and then move the cursor to the right to select **Unicast**.

The Unicast MACs page is displayed. See Figure 34.

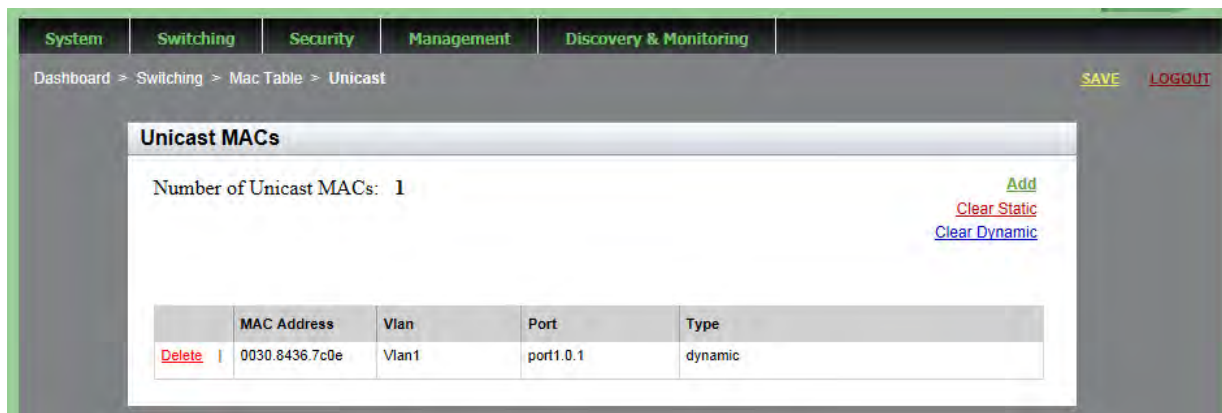


Figure 34. Unicast MACs Page

The following fields are displayed:

- ❑ **MAC Address**— Dynamic or static unicast MAC address learned on or assigned to the port.
- ❑ **Vlan**— ID number of the VLAN where the node designated by the MAC address is a member. The default VLAN is Vlan1.
- ❑ **Port**— Port where the address was learned or assigned.
- ❑ **Type**— Type of MAC address, static or dynamic.

Displaying Multicast MAC Addresses

To display the multicast addresses in the MAC address table, do the following:

1. Hover the cursor over the Switching tab.

The Switching tab is displayed. See Figure 33 on page 96.

2. Hover over **Mac Table** and then move the cursor to the right to select **Multicast**.

The Multicast MACs Page is displayed. See Figure 35.

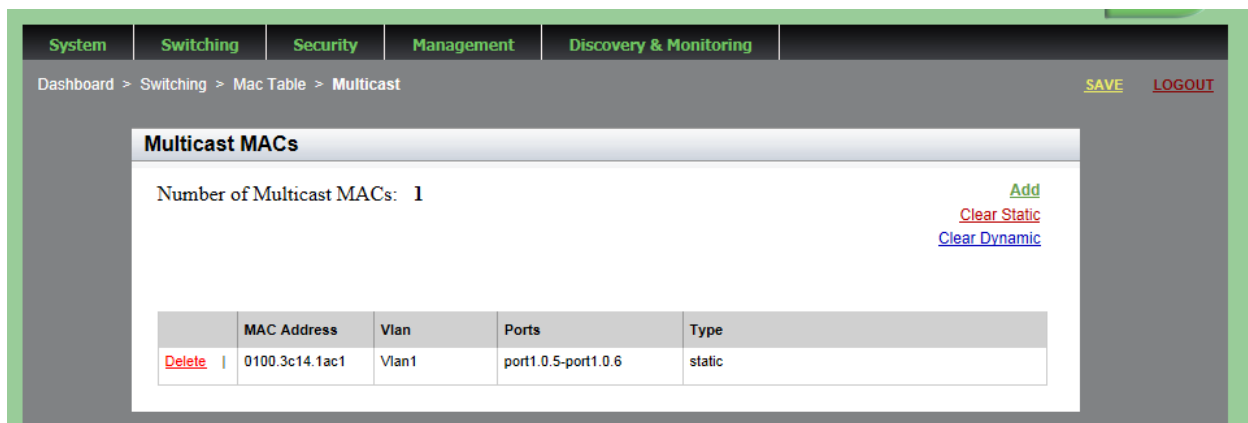


Figure 35. Multicast MACs Page

The following fields are displayed:

- ❑ **MAC Address**— Dynamic or static unicast MAC address learned on or assigned to the port.
- ❑ **Vlan**— ID number of the VLAN where the multicast application and the host nodes are members. The default VLAN is Vlan1.
- ❑ **Port**— Port where the address was learned or assigned.
- ❑ **Type**— Type of MAC address: static or dynamic.

Assigning a MAC Address

You can assign a new unicast or multicast MAC address to the MAC address table. See the following procedures:

- ❑ “Assigning a Unicast Address”
- ❑ “Assigning a Multicast Address” on page 99

Assigning a Unicast Address

To assign a unicast MAC address to the MAC address table, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. Hover over **Mac Table** and then move the cursor to the right to select **Unicast**.

The Unicast MACs page is displayed. See Figure 34 on page 96.

3. Click **Add**.

The Add Unicast Mac Address Page is displayed. See Figure 36.

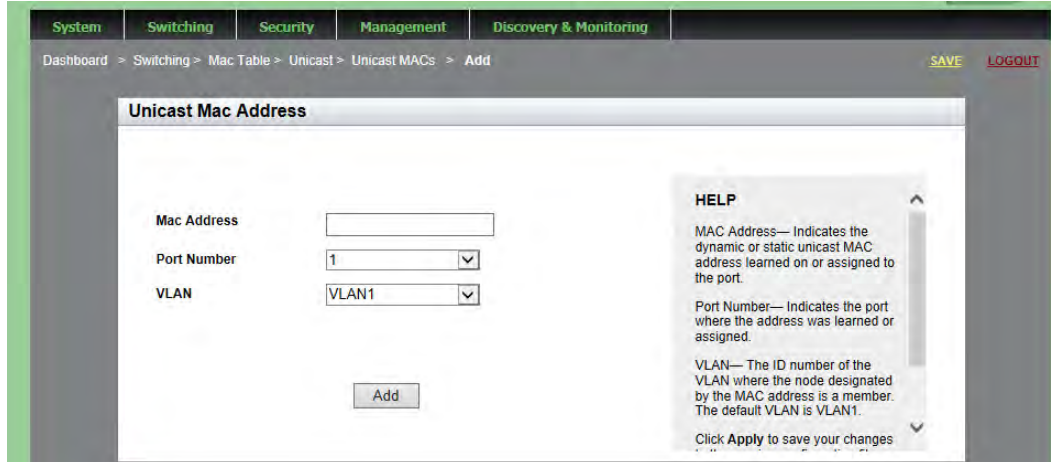


Figure 36. Add Unicast Mac Address Page

4. Enter a unicast MAC address in the **Mac Address** field. Use the following format: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

5. Select a port number with the **Port Number** pull-down menu.

You can only assign one port number to a unicast MAC address.

6. Select a VLAN with the **VLAN** pull-down menu.

For a unicast address, this field specifies the name of the VLAN where the node designated by the MAC address is a member.

7. Click **Add**.
8. Click **SAVE**.

Assigning a Multicast Address

To assign a multicast MAC address to the MAC address table, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. Hover over **Mac Table** and then move the cursor to the right to select **Multicast**.

The Multicast MACs Page is displayed. See Figure 35 on page 97.

3. Click **Add**.

The Add Multicast Mac Address Page is displayed. See Figure 37.

System Switching Security Management Discovery & Monitoring

Dashboard > Switching > Mac Table > Multicast > Add SAVE LOGOUT

Multicast Mac Address

Mac Address

Port List

Vlan

HELP

MAC Address— Indicates the dynamic or static unicast MAC address learned on or assigned to the port.

Port List— Selects a port list with the Port List pull-down menu. For a multicast address, you can assign more than one port number. Enter multiple ports separated by commas. Or, enter a range of ports separated by a dash.

Vlan— Specifies the ID number of

Figure 37. Add Multicast Mac Address Page

4. To assign a MAC Address, enter a multicast MAC address in the **Mac Address** field. Use the following format: xx:xx:xx:xx:xx:xx or xxxx.xxxx.xxxx

5. Assign a port or multiple ports in the **Port List** field.

For a multicast address, you can assign more than one port number. Enter multiple ports separated by commas. Or, enter a range of ports separated by a dash.

6. Select a VLAN with the **Vlan** pull-down menu.

For a multicast address, this field specifies the name of the VLAN where the node designated by the MAC address is a member.

7. Click **Add**.

8. Click **SAVE**.

Deleting a MAC Address

To delete a MAC address from the MAC address table, see the following procedures:

- “Deleting a Unicast Address”
- “Deleting a Multicast Address” on page 101

Deleting a Unicast Address

To delete a unicast address or clear all static or dynamic unicast addresses, do the following:

1. Hover the cursor over the Switching tab.

The Switching tab is displayed. See Figure 33 on page 96.

2. Hover over **Mac Table** and then move the cursor to the right to select **Unicast**.

The Unicast MACs page is displayed. See Figure 34 on page 96.

3. Do one of the following:

- To clear all of the static unicast addresses in the MAC address table, click Clear Static.
- To clear the dynamic unicast addresses in the MAC address table, click Clear Dynamic.
- To delete a specific MAC address, click Delete next to the MAC address that you want to delete.

4. Click **SAVE**.

Deleting a Multicast Address

To delete a multicast address or clear all static or dynamic multicast addresses, do the following:

1. Hover the cursor over the Switching Tab.

The Switching Tab is displayed. See Figure 33 on page 96.

2. Hover over **Mac Table** and then move the cursor to the right to select **Multicast**.

The Multicast MACs page is displayed. See Figure 35 on page 97.

3. Do one of the following:
 - To clear all of the static multicast addresses in the MAC address table, click Clear Static.
 - To clear all of the dynamic multicast addresses in the MAC address table, click Clear Dynamic.
4. Click **SAVE**.
 - To delete a specific MAC address, click Delete next to the MAC address that you want to delete.

Chapter 9

Setting LACP

The Link Aggregation Control Protocol (LACP) is used to increase the bandwidth between the switch and other LACP compatible devices by grouping ports together to form single virtual links.

This chapter provides a brief description of LACP and explains how to display and set LACP. See the following sections:

- ❑ “Overview” on page 104
- ❑ “Displaying LACP Trunks” on page 105
- ❑ “Adding an LACP Trunk” on page 107
- ❑ “Modifying an LACP Trunk” on page 109
- ❑ “Deleting an LACP Trunk” on page 111

For more information about LACP trunks, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ Link Aggregation Control Protocol (LACP)
- ❑ LACP Commands

Overview

LACP trunks are similar in function to static port trunks, but they are more flexible. The implementations of static trunks tend to be vendor-specific and so may not always be compatible. In contrast, the implementation of LACP in the switch is compliant with the IEEE 802.3ad standard. It is interoperable with equipment from other vendors that also comply with the standard. This makes it possible to create LACP trunks between the switch and network devices from other manufacturers.

The main component of an LACP trunk is an aggregator. An aggregator is a group of ports on the switch. The ports of an aggregator are further grouped into a trunk, referred to as an aggregate trunk. An aggregator can have only one trunk. You have to create a separate aggregator for each trunk on the switch.

An aggregate trunk can consist of any number of ports on the switch, but only a maximum of eight ports can be active at a time. If an aggregate trunk contains more ports than can be active at one time, the extra ports are placed in standby mode. Ports in standby mode do not pass network traffic, but they do transmit and accept LACP data unit (LACPDU) packets, which the switch uses to search for LACP compliant devices.

Displaying LACP Trunks

To display the LACP trunk assignments for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Link Aggregation**.

For an example of the Link Aggregation menu, see Figure 38.



Figure 38. Switching Tab with Link Aggregation Selected

3. Move the cursor to the right and select **LACP**.

The LACP Trunks page is displayed. See Figure 39.

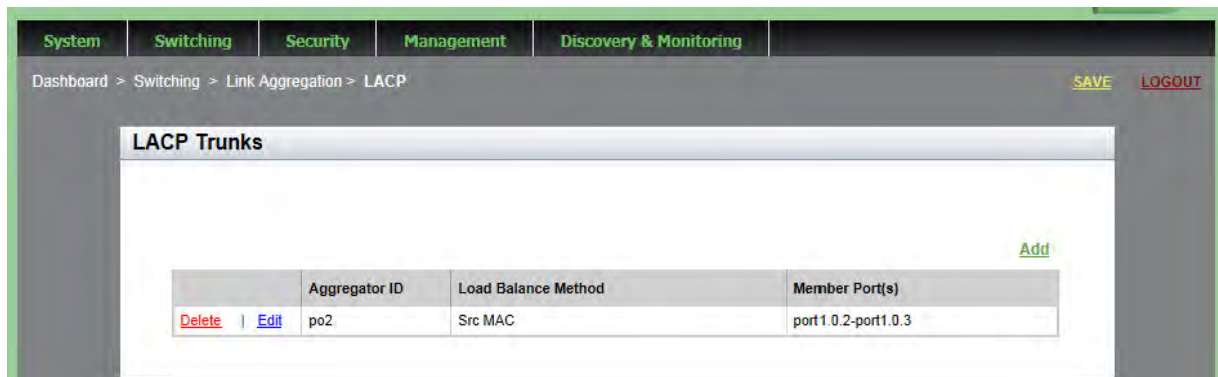


Figure 39. LACP Trunks Page

4. The following fields are displayed:

- ❑ **Aggregator ID**— Each aggregator must have an ID number. The ID number is the base port number (or lowest number) of an aggregator.

For instance, an aggregator of ports 12,16 and 17 must be assigned the ID number 12 because that is the base port.

- ❑ **Load Balance Method**— Load distribution methods of the aggregators. An aggregator can have only one load distribution method. The load distribution method determines the manner in which the switch distributes the egress packets among the active ports of an aggregator. The packets can be distributed by source MAC or IP address, destination MAC or IP address, or by both source and destination addresses.
- ❑ **Member Port(s)**— Member ports of the aggregators.

Adding an LACP Trunk

To create an LACP trunk, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 38 on page 105.

3. Move the cursor to the right and select **LACP**.

The LACP Trunks page is displayed. See Figure 39 on page 105.

4. From the LACP Trunks page, click Add.

The Add LACP Trunk page is displayed. See Figure 40.

Figure 40. Add LACP Trunk Page

5. Specify the Aggregator ID. The range is 1 to 32.
6. Select the Load Balance Method. Choose from the following:
 - Src MAC**— Specifies source MAC address as the load distribution method.
 - Dst MAC**— Specifies destination MAC address.

- Src-Dst MAC**— Specifies source address/destination MAC address.
 - Src IP**— Specifies source IP address.
 - Dst IP**— Specifies destination IP address.
 - Src-Dst IP**— Specifies source address/destination IP address.
7. Select the member ports of the aggregator by clicking on the ports.
 8. Click **Add**.
A confirmation message is displayed.
 9. Click **SAVE**.

Modifying an LACP Trunk

To modify the LACP Trunk settings, see the following procedure:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 38 on page 105.

3. Move the cursor to the right and select **LACP**.

The LACP Trunks page is displayed. See Figure 39 on page 105.

4. From the LACP Trunks page, click Edit next to the Aggregator ID that you want to change.

The Modify LACP Trunk page is displayed. See Figure 41.

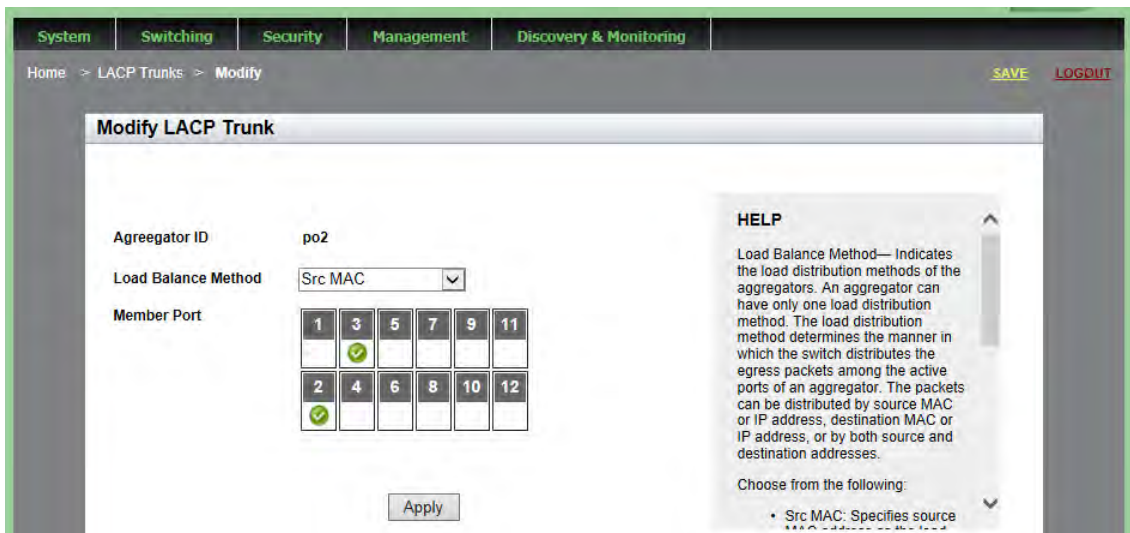


Figure 41. Modify LACP Trunk Page

5. Select the Load Balance Method. Choose from the following:

- Src MAC**— Specifies source MAC address as the load distribution method.
- Dst MAC**— Specifies destination MAC address.
- Src-Dst MAC**— Specifies source address/destination MAC address.
- Src IP**— Specifies source IP address.

- Dst IP**— Specifies destination IP address.
 - Src-Dst IP**— Specifies source address/destination IP address.
6. Add or remove the member ports of the aggregator by clicking on the ports.

A check mark indicates a port has been selected.

7. Click **Apply**.

A confirmation message is displayed.

8. Click **SAVE**.

Deleting an LACP Trunk

To delete an LACP trunk, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 38 on page 105.

3. Move the cursor to the right and select **LACP**.

The LACP Trunks page is displayed. See Figure 39 on page 105.

4. From the LACP Trunks page, click Delete next to the Aggregator ID that you want to delete.

5. Click **SAVE**.

Chapter 10

Setting Static Port Trunks

Static port trunks are groups of two to eight ports that act as single virtual links between the switch and other network devices. This chapter describes how to display, create, and modify static trunks. See the following sections:

- ❑ “Overview” on page 114
- ❑ “Displaying Static Trunk Settings” on page 115
- ❑ “Adding Static Trunks” on page 117
- ❑ “Modifying the Static Trunk Settings” on page 120
- ❑ “Deleting Static Trunks” on page 123

For additional guidelines and information regarding static port trunks, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ Static Port Trunks
- ❑ Static Port Trunk Commands

Overview

Static port trunks are commonly used to improve network performance by increasing the available bandwidth between the switch and other network devices as well as to enhance the reliability of the connections between network devices.

When you create a static port trunk, you can designate how the traffic is distributed across the physical links by the switch by defining the load distribution method.

Static port trunks do not permit standby ports, unlike LACP trunks (which are described in Chapter 9, “Setting LACP” on page 103). If a link is lost on a port in a static port trunk, the trunk’s total bandwidth is reduced. Although the traffic carried by a lost link is shifted to one of the remaining ports in the trunk, the bandwidth remains reduced until a lost link is re-established or another port is manually added to the trunk.

Here are some guidelines regarding static port trunks:

- ❑ A static trunk can have up to eight ports.
- ❑ The switch supports up to a total of 32 static port trunks and LACP trunks at a time. An LACP trunk is counted against the maximum number of trunks when it is active.
- ❑ The ports of a static port trunk can be all twisted pair ports or all fiber optic ports. Static port trunks *cannot* have both types of ports.
- ❑ The ports of a trunk can be consecutive (for example, ports 5-9) or non-consecutive (for example, ports 4, 8, 11, 20).

Displaying Static Trunk Settings

To display the static port trunks for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Link Aggregation**.

For an example of the Link Aggregation tab, see Figure 42.



Figure 42. Switching Tab with Link Aggregation Selected

3. Move the cursor to the right and select **Static Trunks**, as shown in Figure 43.

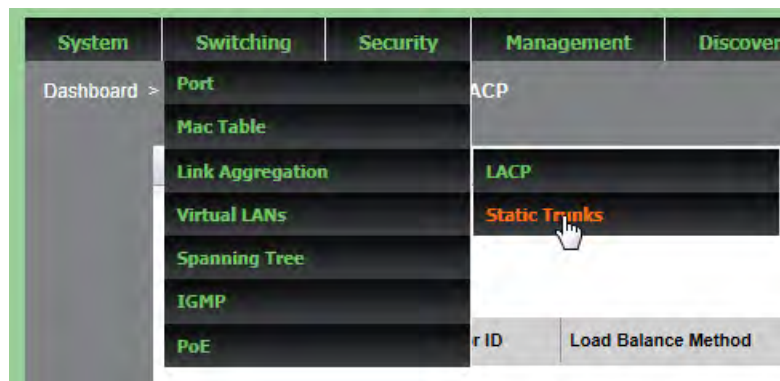


Figure 43. Switching Tab with Static Trunks Selected

The Static Trunks page is displayed. See Figure 44 on page 116. By default, no static trunks are configured on the switch.

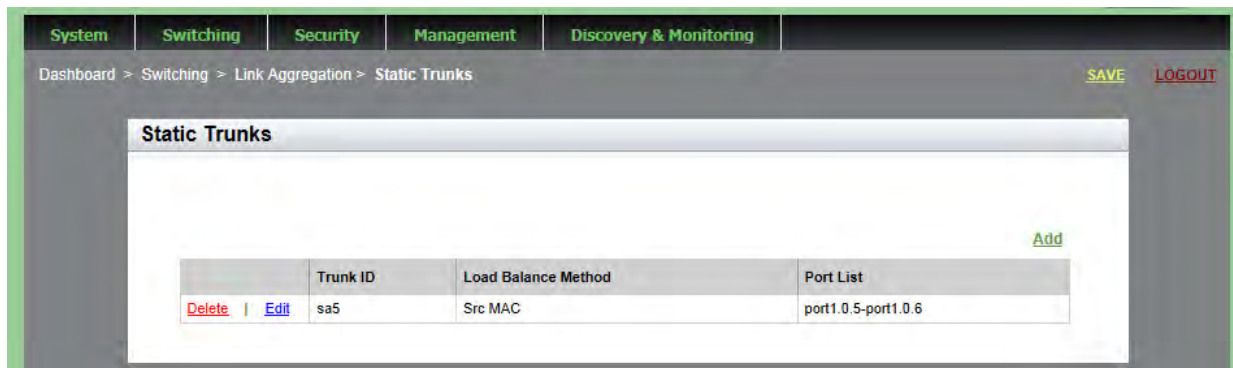


Figure 44. Static Trunks Page

The following fields are displayed:

- ❑ **Trunk ID**— Indicates the ID of the static trunk. This name must be the lowest port number appended with “sa.” For example, the trunk ID of “sa5” indicates a trunk with port 5 as the lowest port number in the trunk.
- ❑ **Load Balance Method**— Indicates one of the following:
 - Src MAC— Source MAC address is the load distribution method. This is a Layer 2 load balance method.
 - Dst MAC— Destination MAC address is the load distribution method. This is a Layer 2 load balance method.
 - Src-Dst MAC— Source address/destination MAC address is the load distribution method. This is a Layer 2 load balance method.
 - Src IP — Source IP address is the load distribution method. This is a Layer 3 load balance method.
 - Dst IP — Destination IP address is the load distribution method. This is a Layer 3 load balance method.
 - Src-Dst IP — Source address/destination IP address is the load distribution method. This is a Layer 3 load balance method.
- ❑ **Port List**— List of ports that are members of the static trunk.

Adding Static Trunks

Review the following information before creating a new static port trunk:

- ❑ When you create a new trunk, the settings of the lowest numbered port are copied to the other ports so that all the ports have the same settings. Therefore, you must examine and verify that the speed, duplex mode, and flow control settings of the lowest numbered port are correct for the network device to which the trunk is connected.
- ❑ All ports of a trunk must be members of the same VLAN.
- ❑ Ports can be a members of one static port trunk at a time. A port that is already a member of a trunk cannot be added to another trunk. To accomplish this, you must remove the member port from its current trunk assignment first. For instructions, see “Adding Static Trunks” on page 117.

To create a static port trunk, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 42 on page 115.

3. Move the cursor to the right and select **Static Trunks**.

The Static Trunks page is displayed. See Figure 44 on page 116.

4. From the Static Trunks page, click Add.

The Add Static Trunk page is displayed. See Figure 45 on page 118.

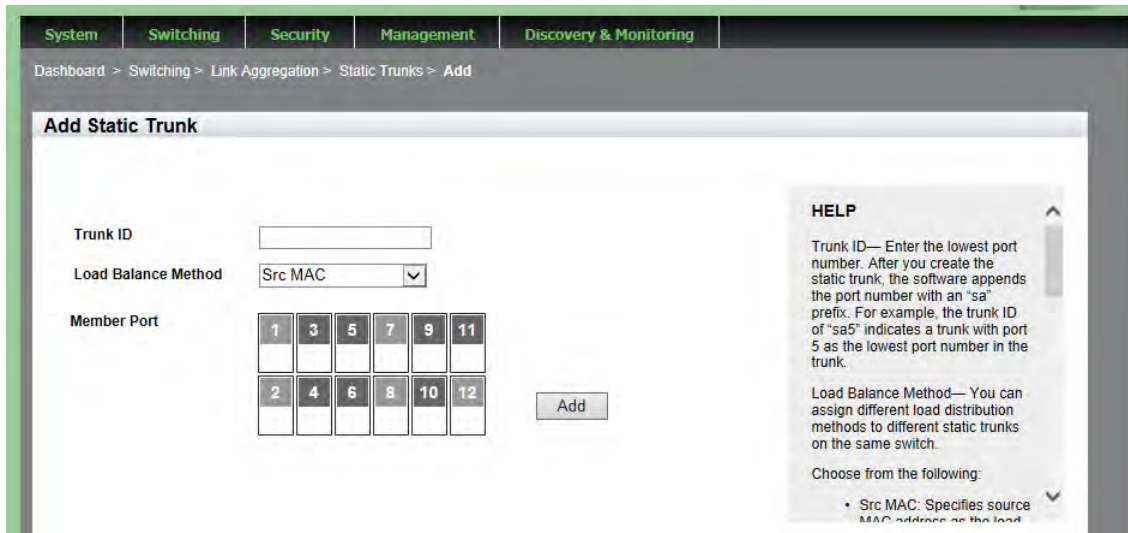


Figure 45. Add Static Trunk Page

5. Select the **Load Balance Method**. You can assign different load distribution methods to different static trunks on the same switch.

Choose from the following:

- Src MAC**— Specifies source MAC address as the load distribution method. This is a Layer 2 load balance method.
- Dst MAC**— Specifies destination MAC address as the load distribution method. This is a Layer 2 load balance method.
- Src-Dst MAC**— Specifies source address/destination MAC address as the load distribution method. This is a Layer 2 load balance method.
- Src IP**— Specifies source IP address as the load distribution method. This is a Layer 3 load balance method.
- Dst IP**— Specifies destination IP address as the load distribution method. This is a Layer 3 load balance method.
- Src-Dst IP**— Specifies source address/destination IP address as the load distribution method. This is a Layer 3 load balance method.

6. Select the Member Ports by clicking the box next to the port.

A green check mark indicates a port has been selected.

Note

Allied Telesis does not recommend using twisted pair ports 25R to 28R on the AT-9000/28 and AT-9000/28SP Managed Layer 2 ecoSwitches in static port trunks. The performance of a static port trunk that has these ports may not be predictable if the ports transition to the redundant state.

7. Enter the **Trunk ID**.

This name must be the lowest port number. After you create the static trunk, the software appends this port number with "sa." For example, the trunk ID of "sa5" indicates a trunk with port 5 as the lowest port number in the trunk.

8. Click **Add**.

A confirmation message is displayed.

9. Click **SAVE**.

Modifying the Static Trunk Settings

Review the following information if you are adding ports to an existing trunk:

- ❑ If the port you are adding is the lowest numbered port in the trunk, its parameter settings overwrites the settings of the existing ports in the trunk. Therefore, check if its settings are appropriate *before* adding it to the trunk. If the new port is not the lowest numbered port, its port settings are changed to match the settings of the existing ports in the trunk.
- ❑ If the new port added to a trunk is already a member of another static trunk, you must first remove it from its current trunk assignment.

To add or delete member ports from a static port trunk, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 42 on page 115.

3. Move the cursor to the right and select **Static Trunks**.

The Static Trunks page is displayed. See Figure 44 on page 116.

4. From the Static Trunks page, click Edit.

The Modify Static Trunk page is displayed. See Figure 46 on page 121.

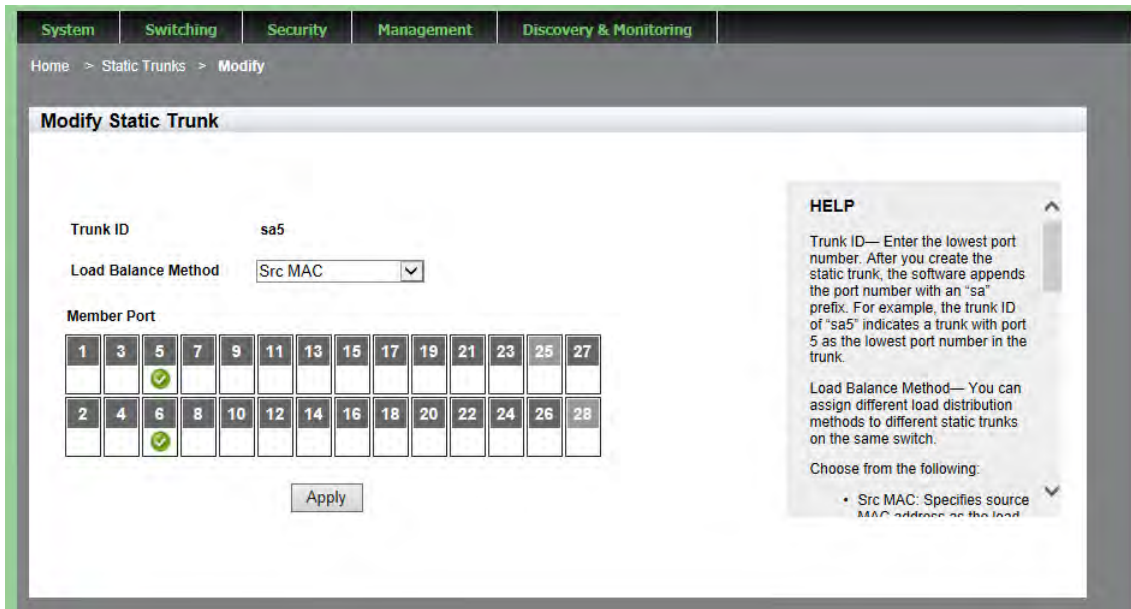


Figure 46. Modify Static Trunk Page

5. Select the **Load Balance Method**. You can assign different load distribution methods to different static trunks on the same switch.

Choose from the following:

- Src MAC**— Specifies source MAC address as the load distribution method. This is a Layer 2 load balance method.
- Dst MAC**— Specifies destination MAC address as the load distribution method. This is a Layer 2 load balance method.
- Src-Dst MAC**— Specifies source address/destination MAC address as the load distribution method. This is a Layer 2 load balance method.
- Src IP**— Specifies source IP address as the load distribution method. This is a Layer 3 load balance method.
- Dst IP**— Specifies destination IP address as the load distribution method. This is a Layer 3 load balance method.
- Src-Dst IP**— Specifies source address/destination IP address as the load distribution method. This is a Layer 3 load balance method.

6. Select the member ports that you want to add to or remove from the static trunk by clicking on the ports.



Caution

To prevent the formation of network loops in your network topology, do not remove ports from a static port trunk without first disconnecting their network cable. Network loops can result in broadcast storms that can adversely affect network performance.

Note

You cannot have a trunk that contains only one port. There must be a minimum of two ports in a trunk.

7. Click **Apply**.
A confirmation message is displayed.
8. Click **SAVE**.

Deleting Static Trunks

To delete a static port trunk, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab, hover over **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 42 on page 115.

3. Move the cursor to the right and select **Static Trunks**.

The Static Trunks page is displayed. See Figure 44 on page 116.

4. From the Static Trunks page, click Delete next to the Trunk ID that you want to delete.

5. Click **SAVE**.

Chapter 11

Setting Port-based and Tagged VLANs

This chapter provides a brief description of VLANs and explains how to display, create, and modify port-based and tagged Virtual LANs which are more commonly known as VLANs. See the following sections:

- ❑ “Overview” on page 126
- ❑ “Displaying VLANs” on page 128
- ❑ “Adding a VLAN” on page 130
- ❑ “Modifying VLANs” on page 132
- ❑ “Assigning a Native VLAN” on page 134
- ❑ “Deleting VLANs” on page 136

For additional information about VLANs, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ Port-based and Tagged VLANs
- ❑ Port-based and Tagged VLAN Commands

Overview

A VLAN is a group of ports that form a logical Ethernet segment on an Ethernet switch. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remains within the VLAN.

VLANs let you segment your network through the switch's management software so that you can group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you could create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting. Both port-based and tagged VLANs are supported in the web interface.

Port-based VLANs

A port-based VLAN is a group of ports on a Gigabit Ethernet Switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time. A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. In addition, a port-based VLAN can span switches and consist of ports from multiple Ethernet switches.

Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The names derive from the fact that the frames received on a port do not contain any information that indicates VLAN membership, and that VLAN membership is determined solely by a port's PVID.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to a port on which a frame is received, and forwards a frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. In addition, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, if you create a port-based VLAN on the switch and assign it the VID 5, the PVID for each port in the VLAN must be assigned the value of 5.

Tagged VLANs

The second type of VLAN is the tagged VLAN. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This differs from a port-based VLAN, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). This number uniquely identifies each VLAN in a network.

When the switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID.

A port that receives or transmits tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

Tagged and Untagged Ports

You need to specify which ports are members of the VLAN. In the case of a tagged VLAN, it is usually a combination of both untagged ports and tagged ports. You specify which ports are tagged and which are untagged when you create the VLAN.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs simultaneously.

Displaying VLANs

To display the VLAN assignments for all of the switch ports, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **Virtual LANs**.

The VLANs page is displayed. For an example of the VLANs page, see Figure 47.

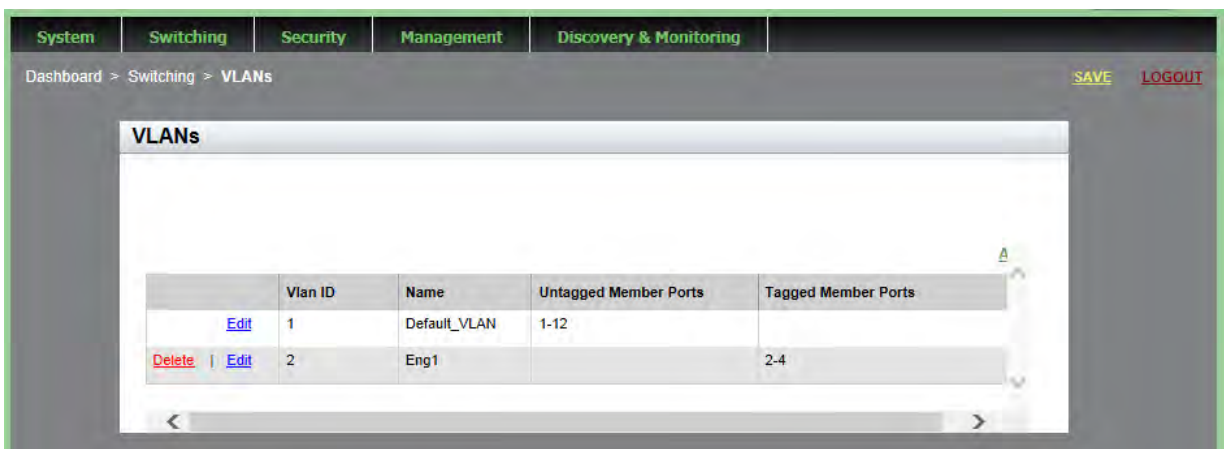


Figure 47. VLANs Page

The following fields are displayed:

- **Vlan ID**— VLAN identifier. The range is 2 to 4094. The VID of 1 is reserved for the default VLAN. The VID cannot be the same as the VID of an existing VLAN on the switch. If this VLAN is unique in your network, its VID must also be unique. However, if this VLAN is part of a larger VLAN that spans multiple switches, the VID value for the VLAN must be the same on each switch. For example, if you are creating a VLAN called Sales with a VID of 3 that spans three switches, assign the Sales VLAN on each switch the same VID value.
- **Name**— VLAN name. A name can be from 1 to 20 characters in length. The first character must be a letter; it cannot be a number. VLANs are easier to identify if their names reflect the functions of their subnetworks or workgroups (for example, Sales or Accounting). A name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). A name cannot be the same as a name of an existing VLAN on the switch. If a VLAN is unique in your network, then its name must be unique as well. A

VLAN that spans multiple switches must have the same name on each switch.

- Untagged Member Ports**— Indicates which ports are untagged ports.
- Tagged Member Ports**— Indicates which ports are tagged ports.

Note

By default, there is one VLAN configured. This is the default VLAN with a VLAN ID of 1. All ports on the switch are assigned to the default VLAN. All ports in Vlan ID 1 are untagged by default.

Note

For information about tagged and untagged ports, see “Overview” on page 126.

Adding a VLAN

To create a VLAN, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.
2. From the Switching tab drop-down menu, select **Virtual LANs**.

The VLANs page is displayed. See Figure 47 on page 128.
3. From the VLANs page, click Add.

The Add VLAN page is displayed. See Figure 48.

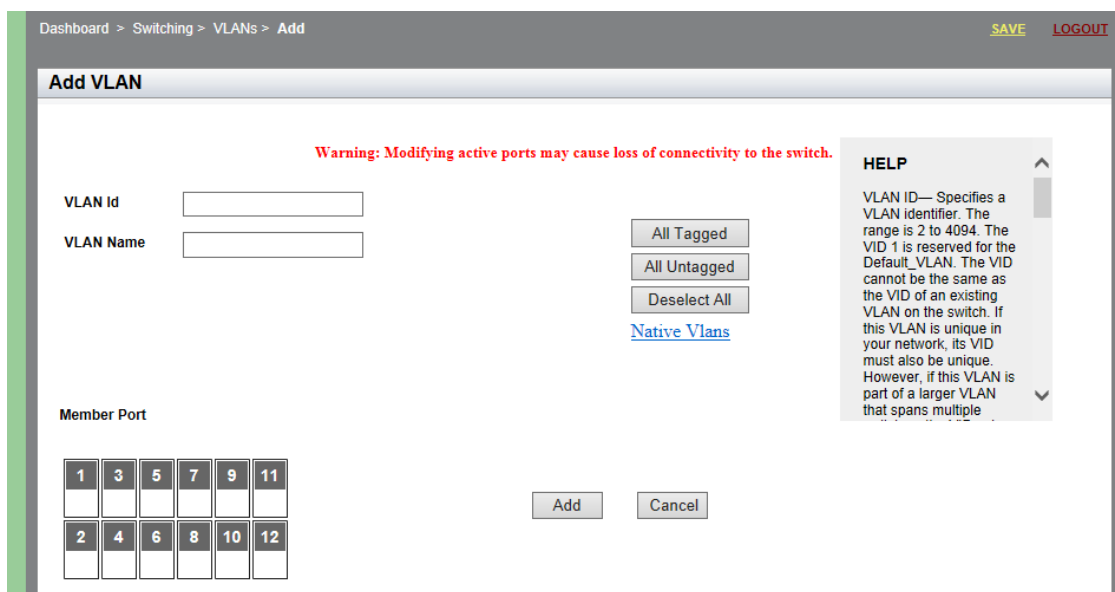


Figure 48. Add VLAN Page

4. Change the following settings as needed:
 - ❑ **VLAN ID**— Specifies a VLAN identifier. The range is 2 to 4094. The VID 1 is reserved for the Default_VLAN. The VID cannot be the same as the VID of an existing VLAN on the switch. If this VLAN is unique in your network, its VID must also be unique. However, if this VLAN is part of a larger VLAN that spans multiple switches, the VID value for the VLAN must be the same on each switch. For example, if you are creating a VLAN called Sales with a VID of 3 that spans three switches, assign the Sales VLAN on each switch a VID value of 3.
 - ❑ **VLAN Name**— Specifies a VLAN name. A name can be from 1 to

20 characters in length. The first character must be a letter; it cannot be a number. VLANs are easier to identify if their names reflect the functions of their subnetworks or workgroups (for example, Sales or Accounting). A name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). A name cannot be the same as a name of an existing VLAN on the switch. If a VLAN is unique in your network, then its name must be unique as well. A VLAN that spans multiple switches must have the same name on each switch.

- Member Port**— Click a port to add it to the VLAN. A “T” indicates a port is a tagged port. A “U” indicates the port is an untagged port.

Note

For information about tagged and untagged ports, see “Overview” on page 126.

- All Tagged**— Click this button to make all ports on the switch tagged ports.
 - All Untagged**— Click this button to make all ports on the switch untagged ports.
 - Deselect All**— Click this button to deselect, or uncheck, all of the selected ports.
5. Click **Add**.
A confirmation message is displayed.
 6. Click **SAVE**.

Modifying VLANs

To modify the VLAN settings, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **Virtual LANs**.

The VLANs page is displayed. See Figure 47 on page 128.

3. From the VLANs page, click Edit next to the VLAN ID that you want to modify.

The Modify VLAN page is displayed. See Figure 49.

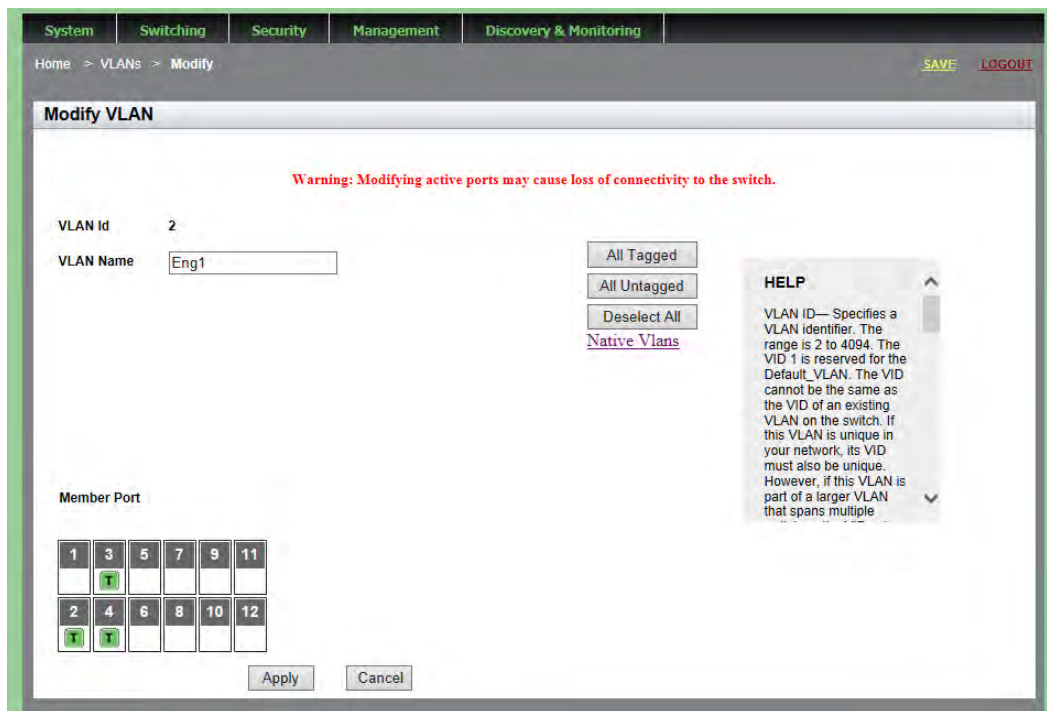


Figure 49. Modify VLAN Page

Note

The VLAN ID specifies a VLAN identifier. The range is 2 to 4094. The VID 1 is reserved for the Default_VLAN. The VID cannot be the same as the VID of an existing VLAN on the switch. If this VLAN is unique in your network, its VID must also be unique. However, if this VLAN is part of a larger VLAN that spans multiple switches, the VID value for the VLAN must be the same on each switch.

4. Change the following fields as needed:
 - VLAN Name**— Specifies a VLAN name. A name can be from 1 to 20 characters in length. The first character must be a letter; it cannot be a number. VLANs are easier to identify if their names reflect the functions of their subnetworks or workgroups (for example, Sales or Accounting). A name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). A name cannot be the same as a name of an existing VLAN on the switch. If a VLAN is unique in your network, then its name must be unique as well. A VLAN that spans multiple switches must have the same name on each switch.
 - All Tagged**— Click this button to make all ports on the switch tagged ports.
 - All Untagged**— Click this button to make all ports on the switch untagged ports.
 - Deselect All**— Click this button to deselect, or uncheck, all of the selected ports.
5. Click **Apply**.

A confirmation message is displayed.
6. Click **SAVE**.

Assigning a Native VLAN

A VLAN can be assigned to a tagged port so that untagged ingress traffic is placed on the VLAN. This VLAN is referred to as the native VLAN.

To assign a native VLAN to a tagged port, perform the following procedure:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **Virtual LANs**.

The VLANs page is displayed. See Figure 47 on page 128.

3. From the VLANs page, click Add.

The Add VLAN page is displayed. See Figure 48 on page 130.

4. From Add VLAN page, click Native VLAN.

The Native VLAN page is displayed. See Figure 50.

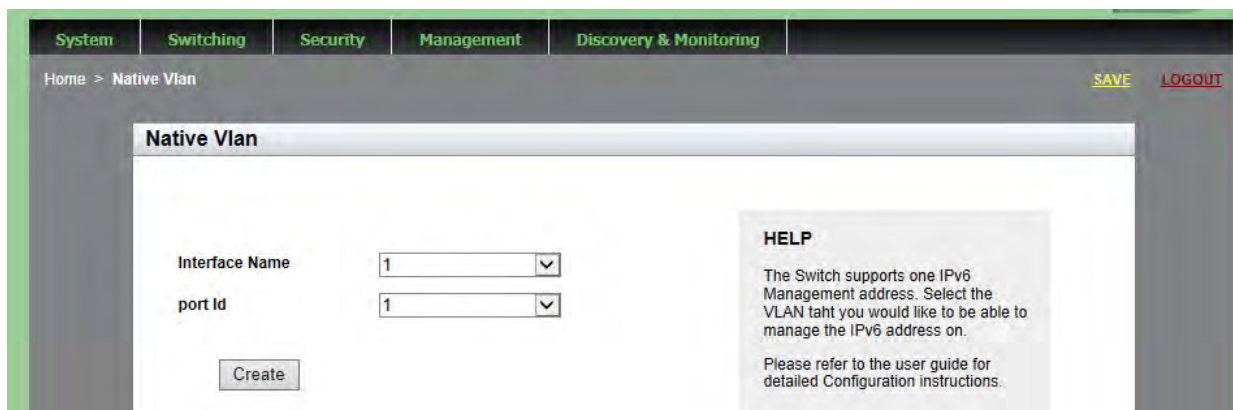


Figure 50. Native VLAN Page

5. Change the following fields as needed:

- Interface Name**— Select a VLAN ID from the pull-down menu. The selected VLAN Interface is assigned to a port as a native VLAN, which untagged frames are placed on.
- Port ID**— Select a port ID from the pull-down menu. You can only select a tagged port.

6. Click **Create**.

A confirmation message is displayed.

7. Click **SAVE**.

Deleting VLANs

To delete a VLAN, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **Virtual LANs**.

For an example of the Virtual LANs page is displayed, see Figure 47 on page 128.

3. From the VLANs page, click Delete next to the VLAN that you want to remove.

The selected VLAN is removed.

Note

You cannot remove the default VLAN, which has a VLAN ID of 1.

4. Click **SAVE**.

Chapter 12

Setting Internet Group Management Protocol (IGMP) Snooping

This chapter provides a brief description of IGMP Snooping and explains how to set this feature on the switch. See the following sections:

- ❑ “Overview” on page 138
- ❑ “Displaying and Modifying IGMP Snooping Configuration” on page 139
- ❑ “Clearing the Routers List” on page 141
- ❑ “Disabling IGMP Snooping” on page 143
- ❑ “Displaying the Routers List” on page 144
- ❑ “Displaying the Hosts List” on page 145

For more information about IGMP, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ Internet Group Management Protocol (IGMP) Snooping
- ❑ IGMP Commands

Overview

IGMP snooping allows the switch to control the flow of multicast packets from its ports. It enables the switch to forward packets of multicast groups to those ports that have host nodes.

IGMP is used by IPv4 routers to create lists of nodes that are members of multicast groups. (A multicast group is a group of end nodes that want to receive multicast packets from a multicast application.) The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node that wants to become a member of a multicast group responds to a query by sending a report. A report indicates that an end node wants to become a member of a multicast group. Nodes that join a multicast group are referred to as host nodes. After joining a multicast group, a host node must continue to periodically issue reports to remain a member.

After the router has received a report from a host node, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router from the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets from the port. This improves network performance by restricting the multicast packets only to router ports where host nodes are located.

Displaying and Modifying IGMP Snooping Configuration

To display and modify the IGMP Configuration settings, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **IGMP**.

The IGMP Snooping page is displayed. By default, the Configuration tab is selected. See Figure 51.

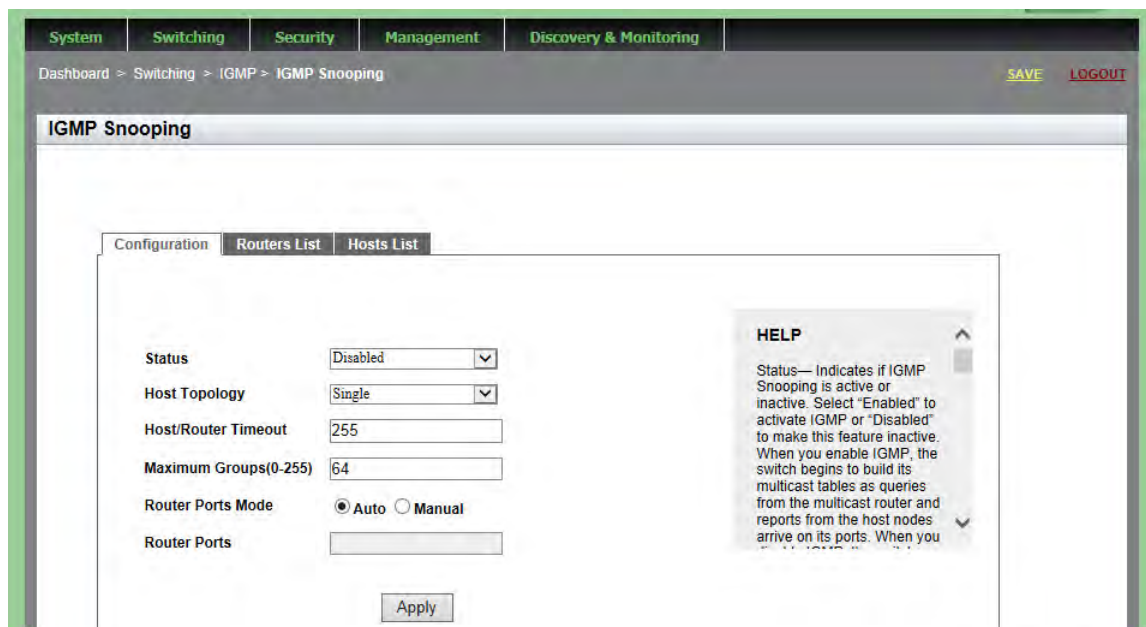


Figure 51. IGMP Snooping Page with Configuration Tab

3. Change the following settings as needed:

- ❑ **Status**— Specifies if IGMP Snooping is active or inactive. Select “Enabled” to activate IGMP or “Disabled” to make this feature inactive. When you enable IGMP, the switch begins to build its multicast tables as queries from the multicast router and reports from the host nodes arrive on its ports. When you disable IGMP, the switch floods the multicast packets on all of the ports except those that receive the packets.

- ❑ **Host Topology**— IGMP host topology. Choose between “Single” which indicates a single host per port and “Multiple” which indicates multiple hosts per port. Select the single-host per port setting when the switch has one host node per port. Select the multiple setting when the switch has more than one host node per port. By default, the switch is set to “Single.”
 - ❑ **Host/Router Timeout**— Time, in seconds, that the switch times out when it finds inactive host nodes and multicast routers. The range is from 0 to 86,400 seconds (24 hours). The default is 255 seconds. Setting the timeout to zero (0) disables the timer.
 - ❑ **Maximum Groups**— Maximum number of multicast addresses the switch is allowed to learn. The range is 0 to 255 multicast addresses. If your network has a large number of multicast groups, use this parameter to limit the number of multicast groups the switch supports. The default is 64.
 - ❑ **Router Ports Mode**— Specifies ports that are connected to multicast routers either manually or automatically. Manually specifying multicast router ports deactivates auto-detect. To reactivate auto-detect, select “Automatic.” Choose between “Manual” and “Automatic.”
 - ❑ **Router Ports**— Specifies ports that are manually connected to multicast routers. Manual Router Ports Mode must be selected to enter multicast router ports.
4. Click **Apply**.
 5. Click **SAVE**.

Clearing the Routers List

To clear the group membership on the IGMP Routers List, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **IGMP**.

The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 51 on page 139.

3. Click the **Routers List** tab.

The IGMP Snooping page with the Routers tab selected is displayed. See Figure 52.

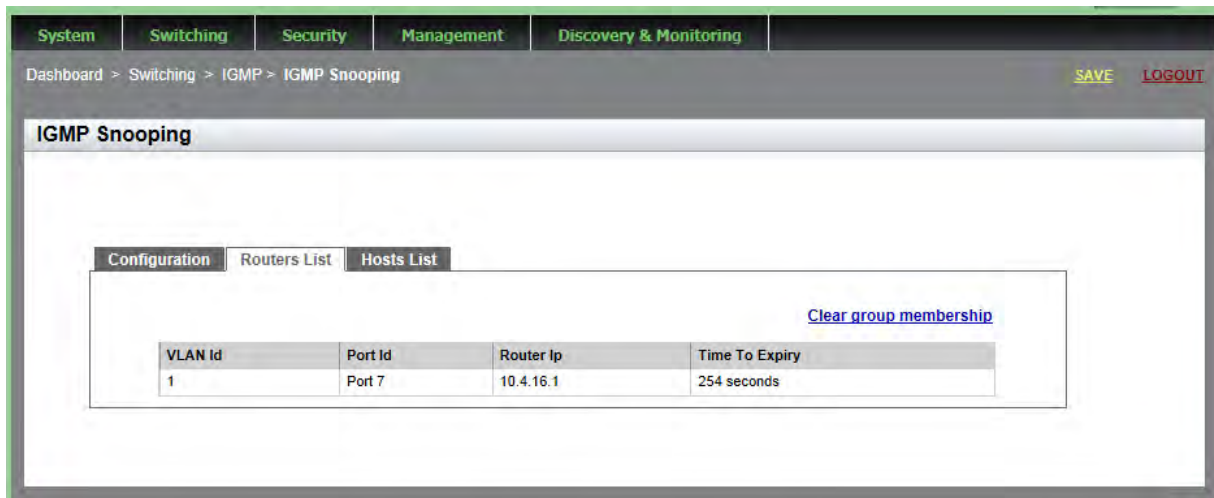


Figure 52. IGMP Snooping Page with Routers List Tab

The following settings are displayed:

- VLAN ID**— ID numbers of the VLANs of the router ports.
- Port ID**— The port of a multicast router. If the switch learned a router on a port trunk, a trunk ID number is displayed, instead of a port number.
- Router IP**— IP addresses of the multicast routers.
- Time to Expiry**— Number of seconds remaining before the switch times out a multicast router if there are no further IGMP queries from it.

4. Click **Clear group membership** to remove the static multicast router ports.
5. Click **Apply**.
6. Click **SAVE**.

Disabling IGMP Snooping

To disable the IGMP Configuration on the switch, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **IGMP**.

The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 51 on page 139.

3. Use the pull-down menu next to the **Status** field to select "Disabled."

When you disable IGMP snooping, the switch floods the multicast packets on all of the ports except those that receive the packets.

4. Click **Apply**.

5. Click **SAVE**.

Displaying the Routers List

To display the IGMP Routers List, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **IGMP**.

The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 51 on page 139.

3. Click the **Routers List** tab.

The IGMP Snooping page with the Routers tab selected is displayed. See Figure 52 on page 141.

The following settings are displayed:

- VLAN ID**— ID numbers of the VLANs of the router ports.
- Port ID**— The port of a multicast router. If the switch learned a router on a port trunk, the trunk ID number, instead of a port number, is displayed.
- Router IP**— IP addresses of the multicast routers.
- Time to Expiry**— Number of seconds remaining before the switch times out a multicast router if there are no further IGMP queries from it.

Displaying the Hosts List

To display the IGMP Hosts List, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **IGMP**.

The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 51 on page 139.

3. Click the **Hosts List** tab.

The Hosts List page is displayed. See Figure 53.

Configuration Routers List Hosts List

Number of multicast groups : 3

| Group Address | VLAN Id | Port Id | Host Ip | IGMP Version | Time To Expiry |
|----------------|---------|-----------|-------------|--------------|----------------|
| 0100.5e02.0207 | 1 | port1.0.7 | 10.4.16.52 | V3 | 0 seconds |
| 0100.5e00.00fc | 1 | port1.0.3 | 10.4.16.135 | V3 | 188 seconds |
| 0100.5e00.00fc | 1 | port1.0.1 | 192.168.1.3 | V3 | 190 seconds |
| 0100.5e7f.ffff | 1 | port1.0.1 | 192.168.1.3 | V3 | 188 seconds |
| 0100.5e7f.ffff | 1 | port1.0.3 | 10.4.16.135 | V3 | 193 seconds |

Figure 53. IGMP Snooping Page with Hosts List Tab

The following settings are displayed:

- Group Address**— Multicast addresses of the groups.
- VLAN ID**— VLAN ID of the host nodes.
- Port ID**— Ports of the host nodes. If the host nodes are on port trunks, this field displays the trunk ID numbers, instead of the port numbers.
- Host IP**— IP addresses of the host nodes.

- ❑ **IGMP Version**— IGMP versions used by the host nodes.
- ❑ **Time to Expiry**— Number of seconds remaining before host nodes are timed out if they do not send IGMP reports.

Chapter 13

Setting Switch Spanning Tree Protocols

This chapter provides a brief description of both the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP), and explains how to set the spanning tree protocols on the switch. See the following sections:

- “Overview” on page 148
- “Displaying Switch Spanning Tree Protocol Settings” on page 149
- “Modifying Switch Spanning Tree Protocol Settings” on page 152

Note

For information about how to set a spanning tree protocol on the ports, see Chapter 7, “Setting the Port Spanning Tree Protocol” on page 89.

For more information about spanning tree, see *Section VI: Spanning Tree Protocols* in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*.

Overview

Both STP and RSTP guard against the formation of loops in an Ethernet network topology. A topology has a loop when two or more nodes can transmit packets to each other over more than one data path. Packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and that can significantly reduce network performance.

STP and RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode. In addition, STP and RSTP can activate redundant paths if primary paths go down. These protocols guard against multiple links between segments and the risk of broadcast storms, and maintain network connectivity by activating backup redundant paths.

One of the primary differences between the two protocols is in the time each takes to complete the process referred to as convergence. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol determines whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain communications between the various network segments. This is the process of convergence.

With STP, convergence can take up to a minute or more to complete in a large network. This can result in the loss of communication between various parts of the network during the convergence process, and the subsequent loss of data packets.

RSTP is much faster than STP. It can complete a convergence in seconds, and so greatly diminish the possible impact the process can have on your network. With STP or RSTP, only one spanning tree can be active on the switch at a time. The default setting is RSTP.

Displaying Switch Spanning Tree Protocol Settings

To display the switch Spanning Tree Protocol settings do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **Spanning Tree**.

The Spanning Tree Settings page is displayed. See Figure 54.

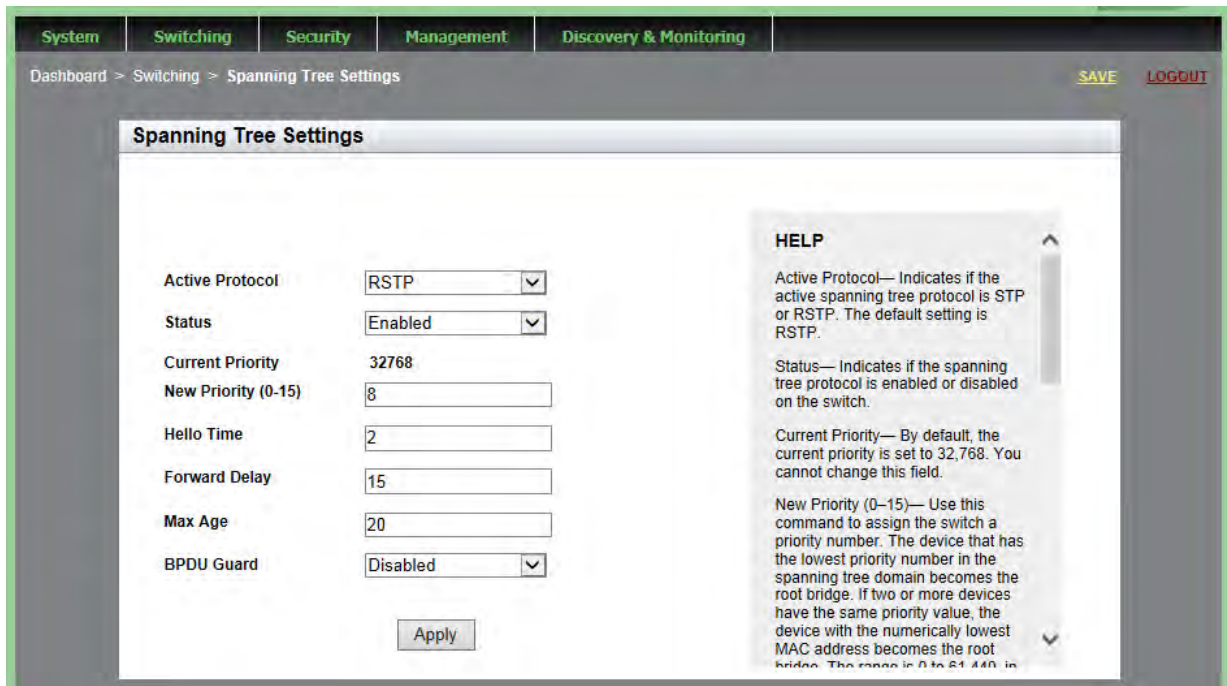


Figure 54. Spanning Tree Settings Page

The following fields are displayed:

- ❑ **Active Protocol**— Indicates if the active spanning tree protocol is STP or RSTP. The default setting is RSTP.
- ❑ **Status**— Indicates if the spanning tree protocol is enabled or disabled on the switch.
- ❑ **Current Priority**— By default, the current priority is set to 32,768. You cannot change this field.
- ❑ **New Priority (0-15)**— Switch priority number. The device that has the lowest priority number in the spanning tree domain becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.

The range is 0 to 61,440, in increments of 4,096. The range is divided into the sixteen increments listed in Table 1. You specify the increment that represents the desired bridge priority value. The default value is 32,768 (increment 8).

Table 1. STP Bridge Priority Value Increments

| Increment | Bridge Priority | Increment | Bridge Priority |
|-----------|-----------------|-----------|-----------------|
| 0 | 0 | 8 | 32768 |
| 1 | 4096 | 9 | 36864 |
| 2 | 8192 | 10 | 40960 |
| 3 | 12288 | 11 | 45056 |
| 4 | 16384 | 12 | 49152 |
| 5 | 20480 | 13 | 53248 |
| 6 | 24576 | 14 | 57344 |
| 7 | 28672 | 15 | 61440 |

Note

Set the hello time, forward delay, and max-age fields according to the following formulas, as specified in IEEE Standard 802.1d:
 max-age <= 2 x (forward time - 1.0 second)
 max-age => 2 x (hello time + 1.0 second)

- ❑ **Hello Time**— Frequency that the switch sends spanning tree configuration information when it is the root bridge or is trying to become the root bridge.
- ❑ **Forward Delay**— Forward time parameter on the switch. This field specifies how long the ports remain in the listening and learning states before they transition to the forwarding state.

The Forward Delay value is active only when the switch is acting as the root bridge of the spanning tree domain. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

- ❑ **Max Age**— How long bridge protocol data units (BPDUs) are stored by the switch before they are deleted.

- ❑ **BPDU Guard**— Indicates if the BPDU loop-guard feature is enabled or disabled on the switch. If a port that has this feature activated stops receiving BPDU packets, the switch automatically disables it. A port that has been disabled by the feature remains in that state until it begins to receive BPDU packets again or the switch is reset. The default setting for BPDU loop-guard on the ports is disabled.

Modifying Switch Spanning Tree Protocol Settings

To modify switch settings for Spanning Tree Protocol, do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **Spanning Tree**.

The Switch Spanning Tree Settings page is displayed. See Figure 54 on page 149.

3. Change the following settings as needed:

- Active Protocol**— Specifies if the active spanning tree protocol is STP or RSTP. The default setting is RSTP.

Note

If you try to select MSTP from the menu, a message will appear indicating that MSTP can only be set via the Command Line Interface and will not allow the selection. To set the protocol to MSTP, and for more information on MSTP, see *Section VI: Spanning Tree Protocols* in the *AlliedWare Plus Management Software Command Line Interface User's Guide* and refer to the *STP, RSTP and MSTP Protocols*, and *MSTP Commands* chapters.

- Status**— Specifies if the spanning tree protocol is enabled or disabled on the switch.
- Current Priority**— By default, the current priority is set to 32,768. You cannot change this field.
- New Priority (0-15)**— Assigns the switch a priority number. The device that has the lowest priority number in the spanning tree domain becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.

The range is 0 to 61,440, in increments of 4,096. The range is divided into the sixteen increments listed in Table 1 on page 150. You specify the increment that represents the desired bridge priority value. The default value is 32,768 (increment 8).

Note

Set the hello time, forward delay, and max-age fields according to the following formulas, as specified in IEEE Standard 802.1d:

max-age \leq 2 x (forward time - 1.0 second)

max-age \geq 2 x (hello time + 1.0 second)

- ❑ **Hello Time**— Specifies the frequency that the switch sends spanning tree configuration information when it is the root bridge or is trying to become the root bridge.
- ❑ **Forward Delay**— Sets the forward time parameter on the switch and specifies how long the ports remain in the listening and learning states before they transition to the forwarding state.

This Forward Delay value is active only when the switch is acting as the root bridge of the spanning tree domain. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

- ❑ **Max Age**— Determines how long bridge protocol data units (BPDUs) are stored by the switch before they are deleted.
- ❑ **BPDU Guard**— Enables or disables the BPDU loop-guard feature on the switch. If a port that has this feature activated stops receiving BPDU packets, the switch automatically disables it. A port that has been disabled by the feature remains in that state until it begins to receive BPDU packets again or the switch is reset. The default setting for BPDU loop-guard on the ports is disabled.

4. Click **Apply**.
5. Click **SAVE**.

Chapter 14

Power Over Ethernet (PoE)

This chapter provides background information about Power over Ethernet (PoE) and includes procedures to configure the PoE feature globally on the switch and on each port. The sections in this chapter include:

- ❑ “Overview” on page 156
- ❑ “Displaying PoE Settings” on page 158
- ❑ “PoE Configuration” on page 160

For additional information about PoE, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ Power Over Ethernet
- ❑ Power Over Ethernet Commands

Overview

The AT-9000/12POE and AT-9000/28POE switches feature PoE on the 10/100/1000Base-Tx ports. PoE is used to supply power to network devices over the same twisted-pair cables that carry the network traffic.

The main advantage of PoE is that it can make installing a network easier. The selection of a location for a network device is often limited by whether there is a power source nearby. This constraint limits equipment placement or requires the added time and cost of having additional electrical sources installed. However, with PoE, you can install PoE compatible devices wherever they are needed without having to worry about whether there is a power source nearby.

Power Sourcing Equipment (PSE)

A device that provides PoE to other host devices is called *power sourcing equipment* (PSE). The AT-9000/12POE and AT-9000/28POE switches act as PSE units by adding DC power to the network cable, thus functioning as a central power source for other host devices.

Powered Device (PD)

A device that receives power from a PSE device is called a *powered device* (PD). Examples include wireless access points, IP phones, webcams, and even other Ethernet switches.

The switch automatically determines whether or not a device connected to a port is a powered device. Ports that are connected to network nodes that are not powered devices (that is, devices that receive their power from another power source) function as regular Ethernet ports, without PoE. The PoE feature remains activated on the ports, but no power is delivered to the devices.

PD Classes

PDs are grouped into five classes. The classes are based on the amount of power that PDs require. The AT-9000/12POE and AT-9000/28POE switches support all five classes listed in Table 2.

Table 2. IEEE Powered Device Classes

| Class | Maximum Power Output from a Switch Port | Power Ranges of the PDs |
|-------|---|-------------------------|
| 0 | 15.4W | 0.44W to 12.95W |
| 1 | 4.0W | 0.44W to 3.84W |
| 2 | 7.0W | 3.84W to 6.49W |
| 3 | 15.4W | 6.49W to 12.95W |
| 4 | 30.0W | 12.95W to 25.5W |

Power Budget

Power budget is the maximum amount of power that the PoE switch can provide at one time to the connected PDs. The AT-9000/12POE switch has a power budget of 125 watts. The AT-9000/28POE switch has a power budget of 370 watts.

Port Prioritization

If the power requirements of the powered devices exceed the switch's power budget, the switch denies power to some ports based on a system called port prioritization. You may use port prioritization to ensure that powered devices critical to the operations of your network are given preferential treatment by the switch in the distribution of power, should the demands of the devices exceed the available capacity.

There are three priority levels:

- Critical
- High
- Low

Ports set to the Critical level, the highest priority level, are guaranteed power before any of the ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all Critical ports are receiving power. Ports that are connected to the most critical powered devices should be assigned to this level. If there is not enough power to support all ports set to the Critical priority level, power is provided to the ports based on the port number, in ascending order.

The High level is the second highest level. Ports set to this level receive power only if all ports set to the Critical level are already receiving power. If there is not enough power to support all ports set to the High priority level, power is provided to the ports based on the port number, in ascending order.

The lowest priority level is Low. This is the default setting. Ports set to this level only receive power if all ports assigned to the other two levels are already receiving power. As with the other levels, if there is not enough power to support all ports set to the Low priority level, power is provided to the ports based on the port number, in ascending order.

Power allocation is dynamic. Ports supplying power to powered devices may cease power transmission if the switch's power budget is at maximum usage, and new powered devices, connected to ports with higher priorities, become active.

You can use port prioritization on dual power-supply PoE switches to protect your important networking devices from loss of power should one of the power supplies fail or lose power. By limiting the power requirements of the critical devices connected to a switch to less than 185 watts (the PoE power provided by a single power supply), a switch will have sufficient power to support the critical devices, even if it has only one functional power supply.

Displaying PoE Settings

To display the switch Spanning Tree Protocol settings do the following:

1. Hover the cursor over the **Switching** tab.

The Switching tab is displayed. See Figure 20 on page 59.

2. From the Switching tab drop-down menu, select **PoE**.

The PoE page is displayed. See Figure 55.

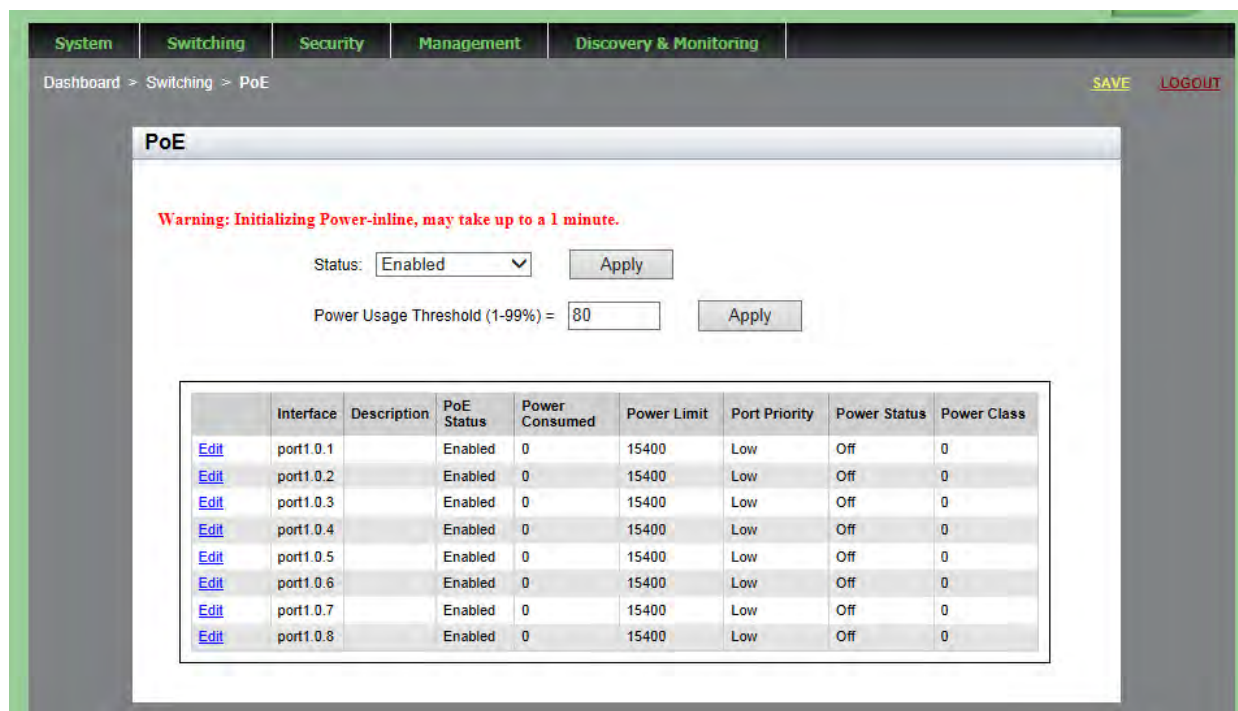


Figure 55. PoE Page

The following fields are displayed:

- ❑ **Status**— Indicates if PoE is enabled or disabled globally.
- ❑ **Power Usage Threshold**— Threshold of the switch's total available system and PoE power. An SNMP trap is transmitted if the requirements of the PDs exceed the threshold.
- ❑ **Interface**— Port ID.
- ❑ **Description**— Description of the PoE device connected to the port.
- ❑ **PoE Status**— Indicates if PoE is enabled or disabled on a specific port.

- ❑ **Power Consumed**— Power, in milliwatts (mW), that the port is supplying to the PD.
- ❑ **Power Limit**— Power limit, in mW, that the switch provides to the device connected to the port.
- ❑ **Port Priority**— Port priority: Low, High, or Critical. For more details, see “Port Prioritization” on page 157.
- ❑ **Power Status**— Whether or not the port is supplying PoE power: **On** indicates the port is supplying PoE power; **Off** indicates the port is not supplying PoE power.
- ❑ **Power Class**— Class of the PD. See Table 2 on page 156 for a definition of the PD PoE classes.

PoE Configuration

You can specify global PoE settings on all ports on the switch using the PoE page - refer to “Configuring Global PoE Settings”. You can also specify PoE settings on individual ports using the Modify Port PoE Settings page - refer to “Configuring Individual Port PoE Settings” on page 160.

Configuring Global PoE Settings

To configure global PoE settings on all ports on the switch, do the following:

1. Hover the cursor over the **Switching** tab.
The Switching tab is displayed. See Figure 20 on page 59.
2. From the Switching tab drop-down menu, select **PoE**.
The PoE page is displayed. See Figure 55 on page 158.
3. From the Status menu, select **Enabled** or **Disabled**:
 - Enabled** enables PoE on all ports on the switch.
 - Disabled** disables PoE on all ports on the switch.
4. Click **Apply**.
5. In the Power Usage Threshold field, enter the threshold of the switch’s total available system and PoE power. The range is 1 to 99%.
6. Click **Apply**.
7. Click **SAVE**.

Configuring Individual Port PoE Settings

To configure global PoE settings on individual ports on the switch, do the following:

1. Hover the cursor over the **Switching** tab.
The Switching tab is displayed. See Figure 20 on page 59.
2. From the Switching tab drop-down menu, select **PoE**.
The PoE page is displayed. See Figure 55 on page 158.
3. Select **Edit** next to the port you want to modify.
The Modify Port PoE Settings page is displayed. See Figure 56 on page 161.

The screenshot shows the 'Modify Port PoE Settings' page. The interface includes a navigation menu at the top with categories: System, Switching, Security, Management, and Discovery & Monitoring. Below the menu, the breadcrumb trail reads 'Home > PoE > Modify', and there are 'SAVE' and 'LOGOUT' links. The main content area is titled 'Modify Port PoE Settings' and contains the following fields:

- Interface:** port1.0.2
- PoE port status:** Enabled
- PoE device Description:** (empty text input)
- PoE port Power Limit (4000-30000):** 15400
- PoE legacy device:** No
- PoE port Priority:** Low

An 'Apply' button is located at the bottom of the form. A 'HELP' sidebar on the right provides the following instructions:

- Interface**— Indicates the port ID.
- PoE Port Status**— Select Enabled or Disabled. The default setting is Enabled.
- PoE Device Description**— Enter the description of the PoE device that is connected to the port. The description can contain up to 256 alphanumeric characters. Spaces and special characters are allowed. Note: The description will only show first 16 characters
- PoE Port Power Limit**— Enter the power limit in milliwatts (mW) that the switch provides to the device.

Figure 56. Modify Port PoE Settings Page

4. Change the following settings as needed:

- Interface**— Indicates the ID of the port you are modifying. You cannot change this parameter.
- PoE port status**— Select **Enabled** or **Disabled** to enable or disable PoE on this port.
- PoE device Description**— Enter the description of the PoE device that is connected to the port. The description can contain up to 256 alphanumeric characters. Spaces and special characters are allowed.

Note

Only the first 16 characters of the description will be displayed.

- PoE Port Power Limit**— Enter the power limit, in milliwatts (mW), that the switch provides to the device connected to the port. The range is 4000 to 30000 mW.

- **PoE Legacy Device**—Select whether the switch supplies power to a device that is connected to the port when the device is a legacy PD. Choose from the following:
 - **Yes**—Allows the switch to supply power to the device, even if the device is a legacy PD.
 - **No**—Does not allow the switch to supply power if the device is a legacy PD. This is the default setting.
- **PoE Port Priority**— Select the PoE port priority. Choose from the following:
 - **Critical**—The highest priority level. Ports set to the Critical level are guaranteed to receive power before any of the ports assigned to the other priority levels.
 - **High**—Ports set to the High level receive power only when all the ports assigned to the Critical level are already receiving power.
 - **Low**—The lowest priority level. Ports set to the Low level receive power only when all the ports assigned to the Critical and High levels are already receiving power. This level is the default setting.

5. Click **Apply**.

6. Click **SAVE**.

Chapter 15

Setting MAC Address-based Port Security

This chapter provides a brief description of MAC address-based port security and explains how to set this feature on the switch. See the following sections:

- ❑ “Overview” on page 164
- ❑ “Displaying MAC Address-based Port Security Settings” on page 166
- ❑ “Modifying MAC Address-based Port Security Settings” on page 168
- ❑ “Disabling MAC Address-based Port Security Settings” on page 170

For more information about MAC address-based security, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ MAC Address-based Port Security
- ❑ MAC Address-based Port Security Commands

Overview

This feature lets you control access to the ports on the switch based on the source MAC addresses of the network devices. You specify the maximum number of source MAC addresses that ports can learn. Ports that learn their maximum number of addresses discard packets that have new, unknown addresses, preventing access to the switch by any additional devices.

For example, if you configure port 3 on the switch to learn five source MAC addresses, the port learns up to five address and forwards the ingress packets of the devices that belong to those addresses. If the port receives ingress packets that have source MAC addresses other than the five it has already learned, it discards those packets to prevent the devices from passing traffic through the switch.

Static Versus Dynamic Addresses

The MAC addresses that the ports learn can be stored as either static or dynamic addresses in the MAC address table in the switch. Ports that store the addresses as static addresses do not learn new addresses after they have learned their maximum number. In contrast, ports that store the addresses as dynamic addresses can learn new addresses when addresses are timed out from the table by the switch. The addresses are aged out according to the aging time of the MAC address table.

Intrusion Actions

The intrusion actions define what the switch does when ports that have learned their maximum number of MAC addresses receive packets that have unknown source MAC addresses. Intrusion actions are also called violation actions. The possible settings are:

- ❑ Protect - Ports discard those frames that have unknown MAC addresses. No other action is taken. For example, if port 14 is configured to learn 18 addresses, it starts to discard packets with unknown source MAC addresses after learning 18 MAC addresses.
- ❑ Restrict - This is the same as the protect action, except that the switch sends SNMP traps when the ports discard frames. For example, if port 12 is configured to learn two addresses, the switch sends a trap every time the port, after learning two addresses, discards a packet that has an unknown MAC address.
- ❑ Shut Down - The switch disables the ports and sends SNMP traps. For example, if port 5 is configured to learn three MAC addresses, it is disabled by the switch to prevent it from forwarding any further traffic if it receives a packet with an unknown source MAC address, after learning three addresses. The switch also sends an SNMP trap.

Guidelines Here are the guidelines to MAC address-based port security:

- ❑ The filtering of a packet occurs on the ingress port, not on the egress port.
- ❑ You cannot use MAC address-based port security and 802.1x port-based access control on the same port. To configure a port as an Authenticator or Supplicant in 802.1x port-based access control, you must remove MAC address-based port security.
- ❑ MAC address-based port security is not supported on the optional GBIC, SFP, or XFP modules.
- ❑ You can manually add static addresses to ports that are configured for this security. The manually added addresses are not counted against the maximum number of addresses the ports can learn.

Displaying MAC Address-based Port Security Settings

To display the MAC address-based port security settings, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57.

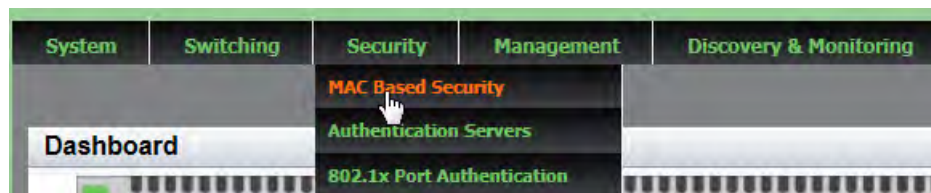


Figure 57. Security Tab

2. From the Security tab drop-down menu, select **MAC Based Security**.

The MAC Based Port Security page is displayed. See Figure 58.

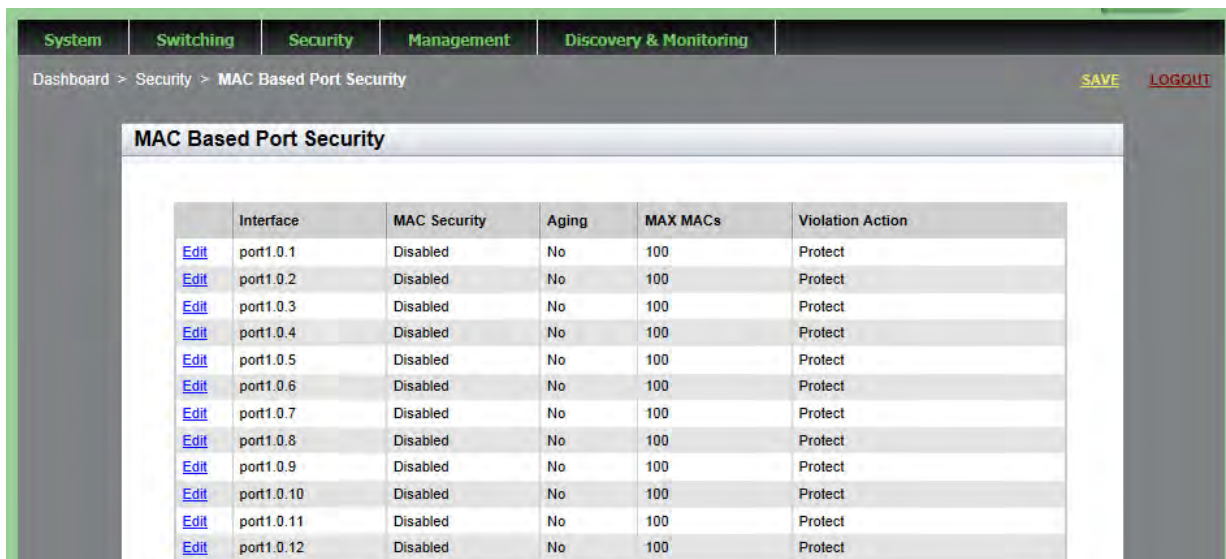


Figure 58. MAC Based Port Security Page

The following fields are displayed:

- Interface**— Port number.
- MAC Security**— Whether MAC address-based security is either “Enabled” or “Disabled” on a port. By default, this setting is disabled.
- Aging**— Indicates the ports that can or cannot add the source MAC addresses as dynamic MAC address in the MAC address

table. Ports that learn their maximum numbers of addresses can learn new addresses as inactive addresses are deleted from the table. A “Yes” value indicates a port that can add source MAC addresses as dynamic. A “No” value indicates a port that cannot add source MAC addresses as dynamic. By default, this field is set to “No.”

- ❑ **MAX MACs**— Maximum number of dynamic MAC addresses the port is permitted to learn. The range is 0 to 255. By default, this field is set to 0.
- ❑ **Violation Action**— Intrusion action of the port. Can be one of the followings actions:

| | |
|----------|---|
| Protect | Ports discard those frames that have unknown MAC addresses. |
| Restrict | Sends SNMP traps when the ports discard frames. |
| Disable | Disables the ports and sends SNMP traps. |

Modifying MAC Address-based Port Security Settings

To the modify the MAC address-based port security settings, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57 on page 166.

2. From the Security tab drop-down menu, select **MAC Based Security**.

The MAC Based Port Security page is displayed. See Figure 58 on page 166.

3. Click Edit next to the port that you want to modify.

The Modify MAC Based Port Security page is displayed. See Figure 59.

The screenshot shows a web-based network management interface. At the top, there is a navigation bar with tabs for System, Switching, Security, Management, and Discovery & Monitoring. Below the navigation bar, the breadcrumb path is "Home > MAC Based Port Security > Modify". On the right side of the breadcrumb path, there are links for "SAVE" and "LOGOUT". The main content area is titled "Modify MAC Based Port Security". It contains several configuration fields: "Interface" is set to "port1.0.2"; "MAC Security" is a dropdown menu set to "Disabled"; "Aging" is a dropdown menu set to "No"; "MAX MACs" is a text input field containing "100"; and "Violation Action" is a dropdown menu set to "Protect". Below these fields is an "Apply" button. To the right of the configuration fields is a "HELP" section with a scrollable area. The help text includes: "Interface— Indicates the port number.", "MAC Security— Activates or deactivates MAC address-based security on ports. Choose either 'Enabled' or 'Disabled.'", and "Aging— Indicates the ports that can or cannot add the source MAC addresses as dynamic MAC address in the MAC address table. Ports that learn their maximum numbers of addresses can learn new addresses as inactive addresses are deleted from the table. Choose from the following

Figure 59. Modify MAC Based Port Security Page

4. Change the following settings as needed:

- Interface**— Indicates the port number.
- MAC Security**— Activates or deactivates MAC address-based security on ports. Choose either “Enabled” or “Disabled.”
- Aging**— Selects if the ports that can or cannot add the source MAC addresses as dynamic MAC address in the MAC address table. Ports that learn their maximum numbers of addresses can learn new addresses as inactive addresses are deleted from the table. Choose from the following options:

| | |
|-----|---|
| Yes | Indicates a port that can add source MAC addresses as dynamic. |
| No | Indicates a port that cannot add source MAC addresses as dynamic. |
- MAX MACs**— Maximum number of dynamic MAC addresses the port is permitted to learn. The range is 0 to 255.
- Violation Action**— Selects the intrusion action of the port. Choose from the following:

- | | |
|-----------|---|
| Protect | Protects intrusion action. This is the default setting. Ports discard those frames that have unknown MAC addresses. |
| Restrict | Restricts intrusion action. Sends SNMP traps when the ports discard frames. |
| Shut Down | Shuts down intrusion action. Disables the ports and sends SNMP traps. |

5. Click **Apply**.6. Click **SAVE**.

Disabling MAC Address-based Port Security Settings

To deactivate MAC address-based port security settings, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57 on page 166.

2. From the Security tab drop-down menu, select **MAC Based Security**.

The MAC Based Port Security page is displayed. See Figure 58 on page 166.

3. Click Edit next to the port that you want to remove.

The Modify MAC Based Port Security page is displayed. See Figure 59 on page 168.

4. Use the pull-down menu next to the **MAC Security** field and select "Disabled."

5. Click **Apply**.

6. Click **SAVE**.

Chapter 16

Setting RADIUS and TACACS+ Clients

This chapter provides a brief description of both the RADIUS and TACACS+ clients and explains how to configure these clients on the switch.

See the following sections:

- ❑ “Overview” on page 172
- ❑ “Configuring RADIUS for Remote Manager Authentication” on page 175
- ❑ “Configuring TACACS+ for Remote Manager Authentication” on page 179
- ❑ “Deleting an Authentication Server” on page 184

For more information about the authentication server features, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ RADIUS and TACACS+ Clients
- ❑ RADIUS and TACACS+ Client Commands

Overview

The switch has RADIUS and TACACS+ clients for remote authentication. Here are the features that use remote authentication:

- ❑ 802.1x port-based network access control. This feature lets you increase network security by requiring that network users log on with a username and password before the switch will forward their packets. This feature is described in Chapter 17, “Setting 802.1x Port-based Network Access” on page 185.
- ❑ Remote manager accounts. This feature lets you add manager accounts to the switch by transferring the task of authenticating the accounts from the switch to an authentication server on your network. This feature is described in “Managing User Accounts” on page 44.

The RADIUS client supports both features, but the TACACS+ client supports only the remote manager accounts feature. Here are the guidelines:

- ❑ Only one client can be active on the switch at a time.
- ❑ If you want to use just the remote manager account feature, you can use either RADIUS or TACACS+ because both clients support that feature.
- ❑ If you want to use 802.1x port-based network access control, you have to use the RADIUS client because the TACACS+ client does not support that feature.

Remote Manager Accounts

The switch comes with one local manager account. The account is referred to as a local account because the switch authenticates the username and password when a manager uses the account to log on. If the username and password are valid, the switch allows the individual to access its management software. Otherwise, it cancels the login to prevent unauthorized access.

There are two ways to add more manager accounts. The first way is to create additional local accounts. For more information about local accounts, see “Managing User Accounts” on page 44.

The second way to add more accounts is with a RADIUS or TACACS+ authentication server on your network. With either authentication method, the authentication of the usernames and passwords of the manager accounts is performed by one or more authentication servers. The switch forwards the information to the servers when managers log on. The following steps illustrate the authentication process that occurs between the switch and an authentication server when a manager logs on:

1. The switch uses its RADIUS or TACACS+ client to transmit the username and password to an authentication server on the network.
2. The server checks to see if the username and password are valid.
3. If the combination is valid, the authentication server notifies the switch, which completes the login process, allowing the manager access to its management software.
4. If the username and password are invalid, the authentication protocol server notifies the switch, which cancels the login.

Accounting Information

RADIUS and TACACS+ also provide a way to monitor usage by login users. You can configure the switch to send a start accounting message at the beginning of a session and a stop accounting message at the end of the session to an authentication sever.

Configuring RADIUS and TACACS+

To authenticate using a RADIUS or TACACS+ server, you must configure remote manager authentication and add authentication servers that the switch can access.

You can configure up to three servers each for the RADIUS and TACACS+ features. However, only one authentication method, either RADIUS or TACACS+, can be configured at a time.

To configure remote manager authentication and add authentication servers, choose from the following procedures:

- “Configuring RADIUS for Remote Manager Authentication” on page 175
- “Configuring TACACS+ for Remote Manager Authentication” on page 179

Placing RADIUS and TACACS+ Servers in the Client's List

When a user logs on to the switch, the authentication client polls the servers for authentication information in the order in which they are listed in the client. The order that you add a server determines its order on the client. For instance, the first server that you add becomes Server 1, the second server that you add becomes Server 2, and the third server that you add becomes Server 3.

When you remove a server from the switch, the place holder is retained. For example, you make the following assignments:

- Server 1 has an IP address of 192.168.10.11
- Server 2 has an IP address of 192.168.10.12
- Server 3 has an IP address of 192.168.10.13

When you delete Server 1, the server with an IP address of 192.168.10.12 remains Server 2; the server with an IP address of 192.168.10.13 remains Server 3. As a result, the next server that you add to the switch becomes Server 1.

Configuring RADIUS for Remote Manager Authentication

To configure remote manager authentication using RADIUS and add RADIUS servers to the switch, perform the following:

- ❑ “Configuring Remote Manager Authentication Using RADIUS”
- ❑ “Adding a RADIUS Server” on page 177

Configuring Remote Manager Authentication Using RADIUS

To configure the RADIUS server, do the following:

1. Hover the cursor over the **Security** tab.
The Security tab is displayed. See Figure 57 on page 166.
2. From the Security tab drop-down menu, select **Authentication Servers**.

The Authentication Server Configuration page with the RADIUS tab selected is displayed. See Figure 60.

System Switching Security Management Discovery & Monitoring

Dashboard > Security > Authentication Servers SAVE LOGOUT

Authentication Server Configuration

Active Authentication Server: None

RADIUS TACACS+

Timeout Value(1-1000)

Key Value(Max length is 40)

RADIUS Authentication Login

AAA Authentication Login Local

AAA Accounting

HELP

Timeout Value— Enter the length of the time, in seconds, that the switch waits for a response from a RADIUS server to an authentication request, before querying the next server in the list. The range is 1 to 1,000 seconds. The default value is 5.

Key Value— Enter the value of the global encryption key of the RADIUS servers. You can define a global encryption key if you have one RADIUS server or if there is more than one server and they all use the same encryption key. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

Configured RADIUS Servers

| Add | IP Address | Authentication Port | Accounting Port | Key |
|-----|------------|---------------------|-----------------|-----|
| | | | | |

Figure 60. Authentication Server Configuration Page with RADIUS Tab

3. Change the following fields as needed:
 - ❑ **Timeout Value**— Enter the length of the time, in seconds, that the

switch waits for a response from a RADIUS server to an authentication request, before querying the next server in the list. The range is 1 to 1,000 seconds. The default value is 5 seconds.

- ❑ **Key Value**— Enter the value of the global encryption key of the RADIUS servers. You can define a global encryption key if you have one RADIUS server or if there is more than one server and they all use the same encryption key. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.



Caution

To define two or three servers that use different encryption keys, do not enter a global encryption key value on this web page. Instead, define the individual keys when you add the IP addresses of the servers to the client on the RADIUS Server Configuration Page. See “Adding a RADIUS Server” on page 177.

- ❑ **RADIUS Authentication Login**— Enable or disable RADIUS to authenticate user login. Choose from the following:
 - Enabled:** The RADIUS servers authenticate user login.
 - Disabled:** The RADIUS servers do not authenticate user login. Authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.
- ❑ **AAA Authentication Login Local**— Enable or disable RADIUS to authenticate user login in combination with local manager accounts. Choose from the following:
 - Enabled:** The RADIUS servers authenticate the user login. When any RADIUS server is not available, authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.
 - Disabled:** The RADIUS servers do not authenticate user login. Authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

Note

For additional information about the User Management page, see “Managing User Accounts” on page 44. For more information about the USERNAME command, see “Local Manager Accounts” in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*.

- ❑ **AAA Accounting**— Select a RADIUS accounting setting. Choose from the following:

Start-Stop: A start accounting message is sent at the beginning of a session, and a stop accounting message is sent at the end of the session.

Stop-Only: A stop accounting message is sent at the end of the session.

None: Sending accounting messages is disabled.

4. Click **Apply**.

The Active Authentication Server field shown on the upper middle of the page indicates “RADIUS.”

5. Click **SAVE**.

Adding a RADIUS Server

To add a RADIUS server, do the following:

1. Click **Add** near the RADIUS server list.

The RADIUS Server Add page is displayed. See Figure 61.

System Switching Security Management Discovery & Monitoring

Dashboard > Security > Authentication Servers > Add SAVE LOGOUT

RADIUS Server Add

IP Address

Authentication Port

Accounting Port

Key

HELP ^

IP Address— Specifies the IP address of a RADIUS server on the network. The IP address must be in the following IPv4 format: xxx.xxx.xxx.xxx.

Authentication Port— Specifies the UDP destination port for RADIUS authentication requests. If you select 0, the server is not used for authentication. The default UDP port for authentication is 1812.

Accounting Port— Select the accounting port for the RADIUS server. This is the UDP destination port for RADIUS accounting requests. If you select 0, the server is not used for accounting. v

Figure 61. Radius Server Add Page

2. Enter the following fields as needed:
 - IP Address**— IP address of a RADIUS server on the network. The IP address must be in the following IPv4 format: xxx.xxx.xxx.xxx.
 - Authentication Port**— UDP destination port for RADIUS authentication requests. If you select 0, the server is not used for authentication. The default UDP port for authentication is 1812.
 - Accounting Port**— UDP destination port for RADIUS accounting requests. If you select 0, the server is not used for accounting. The default UDP port for accounting is 1813.
 - Key**— Encryption key for RADIUS communications between the switch and RADIUS server. The key must match the encryption key used by the RADIUS server. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.
3. Click **Apply**.
4. Click **SAVE**.

Configuring TACACS+ for Remote Manager Authentication

To configure remote manager authentication using TACACS+ and add TACACS+ servers to the switch, perform the following:

- “Configuring Remote Manager Authentication Using TACACS+” on page 179
- “Adding a TACACS+ Server” on page 182

Configuring Remote Manager Authentication Using TACACS+

To configure a TACACS+ server, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57 on page 166.

2. From the Security tab drop-down menu, select **Authentication Servers**.

The Authentication Server Configuration page is displayed. See Figure 60 on page 175.

3. Click the **TACACS+** tab.

The Authentication Server Configuration Page with the TACACS+ tab is displayed. See Figure 62 on page 180.

System Switching Security Management Discovery & Monitoring

Dashboard > Security > Authentication Servers SAVE LOGOUT

Authentication Server Configuration

Active Authentication Server: None

RADIUS | **TACACS+**

| | |
|---------------------------------|--------------------------------|
| Timeout Value(1-1000) | <input type="text" value="5"/> |
| Key Value(Max length is 40) | <input type="text"/> |
| TACACS+ Authentication Login | Disabled |
| AAA Authentication Login Local | Disabled |
| AAA Authentication Enable | Disabled |
| AAA Authentication Enable Local | Disabled |
| AAA Accounting | None |

HELP

Timeout Value— Enter the length of the time, in seconds, that the switch waits for a response from a TACACS+ server to an authentication request, before querying the next server in the list. The range is 1 to 1,000 seconds. The default value is 5.

Key Value— Enter the value of the global encryption key of the TACACS+ servers. You can define a global encryption key if you have one TACACS+ server or if there is more than one server and they all use the same encryption key. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

Configured TACACS+ Servers

| Add | IP Address | Key |
|---------------------|------------|-----|
| | | |

Figure 62. Authentication Server Configuration Page with TACACS+ Tab

4. Change the following fields as needed:

- ❑ **Timeout Value**— Enter the length of the time, in seconds, that the switch waits for a response from a TACACS+ server to an authentication request, before querying the next server in the list. The range is 1 to 1,000 seconds. The default value is 5.
- ❑ **Key Value**— Enter the value of the global encryption key of the TACACS+ servers. You can define a global encryption key if you have one TACACS+ server or if there is more than one server and they all use the same encryption key. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

**Caution**

To define two or three servers that use different encryption keys, do not enter a global encryption key value on this web page. Instead, define the individual keys when you add the IP addresses of the servers to the switch on the TACACS+ Add page. See “Adding a RADIUS Server” on page 177.

- ❑ **TACACS+ Authentication Login**— Enable or disable TACACS+ to authenticate user login. Choose from the following:

Enabled: The TACACS+ servers authenticate user login.

Disabled: The TACACS+ servers do not authenticate user login. Authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

- ❑ **AAA Authentication Login Local**— Enable or disable TACACS+ to authenticate user login in combination with local manager accounts. Choose from the following:

Enabled: The TACACS+ servers authenticate user login. When any TACACS+ server is not available, authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

Disabled: The TACACS+ servers do not authenticate user login. Authentication is attempted using the username and password combinations specified on the User Management page and using the USERNAME command in the CLI.

Note

For additional information about the User Management page, see “Managing User Accounts” on page 44. For more information about the USERNAME command, see “Local Manager Accounts” in the *AlliedWare Plus Management Software Command Line Interface User's Guide*.

- ❑ **AAA Authentication Enable**— Enable or disable TACACS+ to authenticate users requesting the Privileged Exec mode. Choose from the following:

Enabled: The TACACS+ determines whether users can access the Privileged EXEC level using the TACACS+ enable password.

Disabled: The TACACS+ servers do not use its enable password. Authentication is attempted using the password specified using the ENABLE PASSWORD command in the CLI.

- ❑ **AAA Authentication Enable Local**— Enable or disable TACACS+ to authenticate users requesting the Privileged Exec mode. Choose from the following:
 - Enabled:** The TACACS+ determines whether users can access the Privileged EXEC level using the TACACS+ enable password. When any TACACS+ server is not available, authentication is attempted using the password specified using the ENABLE PASSWORD command in the CLI.
 - Disabled:** The TACACS+ servers do not use its enable password. Authentication is attempted using the password specified using the ENABLE PASSWORD command in the CLI.
- ❑ **AAA Accounting**— Select a TACACS+ accounting setting. Choose from the following:
 - Start-Stop:** A start accounting message is sent at the beginning of a session, and a stop accounting message is sent at the end of the session.
 - Stop-Only:** A stop accounting message is sent at the end of the session.
 - None:** Sending accounting messages is disabled.

5. Click **Apply**.

The Active Authentication Server field shown on the upper middle of the page indicates “TACACS+.”

6. Click **SAVE**.

Adding a TACACS+ Server

To add a TACACS+ server, do the following:

1. Click **Add** at the bottom of the page.

The TACACS+ Add page is displayed. See Figure 63 on page 183.

Figure 63. TACACS+ Server Add Page

2. Enter the following settings:
 - ❑ **IP Address**— Enter the IP address of the TACACS+ server. The IP address must be in the following IPv4 format: xxx.xxx.xxx.xxx.
 - ❑ **Key**— Enter the encryption key for TACACS+ communications between the switch and TACACS+ server. The key must match the encryption key used by the TACACS+ server. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.
3. Click **Apply**.
4. Click **SAVE**.

Deleting an Authentication Server

To delete either an TACACS+ or RADIUS authentication server, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57 on page 166.

2. From the Security tab drop-down menu, select **Authentication Servers**.

The Authentication Server Configuration page is displayed. See Figure 60 on page 175.

3. Click either the TACACS+ or the RADIUS tab, depending on the type of server you want to delete.
4. Click **Delete** next to the server that you want to delete.
5. Click **SAVE**.

Chapter 17

Setting 802.1x Port-based Network Access

This chapter provides a brief description of the 802.1x Port-based Authentication feature, and explains how to enable this feature on the switch and configure authentication on a port.

See the following sections:

- ❑ “Overview” on page 186
- ❑ “Enabling 802.1x Port-based Authentication on the Switch” on page 187
- ❑ “Configuring 802.1x Port-based Authentication” on page 188
- ❑ “Displaying the 802.1x Authentication Port Settings” on page 194
- ❑ “Disabling 802.1x Port-based Authentication on the Switch” on page 195
- ❑ “Disabling 802.1x Port-based Authentication on a Port” on page 196

For more information about the 802.1x features, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ 802.1x Port-based Network Access Control
- ❑ 802.1x Port-based Network Access Control Commands

Overview

The 802.1x port-based network access control feature lets you control who can send traffic through, and receive traffic from, the individual switch ports. The switch does not allow an end node to send or receive traffic through a port until the user of the node has been authenticated by a RADIUS server.

This port-security feature is used to prevent unauthorized individuals from connecting a computer to a switch port or using an unattended workstation to access your network resources. Only those users designated as valid network users on a RADIUS server are permitted to use the switch to access the network.

This port security method uses the RADIUS authentication protocol. The management software of the switch includes RADIUS client software. As mentioned in Chapter 16, “Setting RADIUS and TACACS+ Clients” on page 171, you can use the RADIUS client software on the switch, along with a RADIUS server on your network, to create new remote manager accounts.

Note

RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication protocol for 802.1x port-based network access control. This feature is not supported with the TACACS+ authentication protocol.

Here are several terms to keep in mind when using this feature:

- ❑ **Supplicant**— A supplicant is an end user or end node that wants to access the network through a switch port. A supplicant is also referred to as a client.
- ❑ **Authenticator**— The authenticator is a port that prohibits network access until a supplicant has logged on and been validated by the RADIUS server.
- ❑ **Authentication server**— The authentication server is the network device that has the RADIUS server software. This is the device that does the actual authenticating of the supplicants.

The switch does not authenticate any supplicants connected to its ports. Its function is to act as an intermediary between the supplicants and the authentication server during the authentication process.

Enabling 802.1x Port-based Authentication on the Switch

To enable the 802.1x port-based Authentication feature on a switch, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57 on page 166.

2. From the Security tab drop-down menu, select **802.1x Port Authentication**.

The 802.1x Authentication page is displayed. See Figure 64.

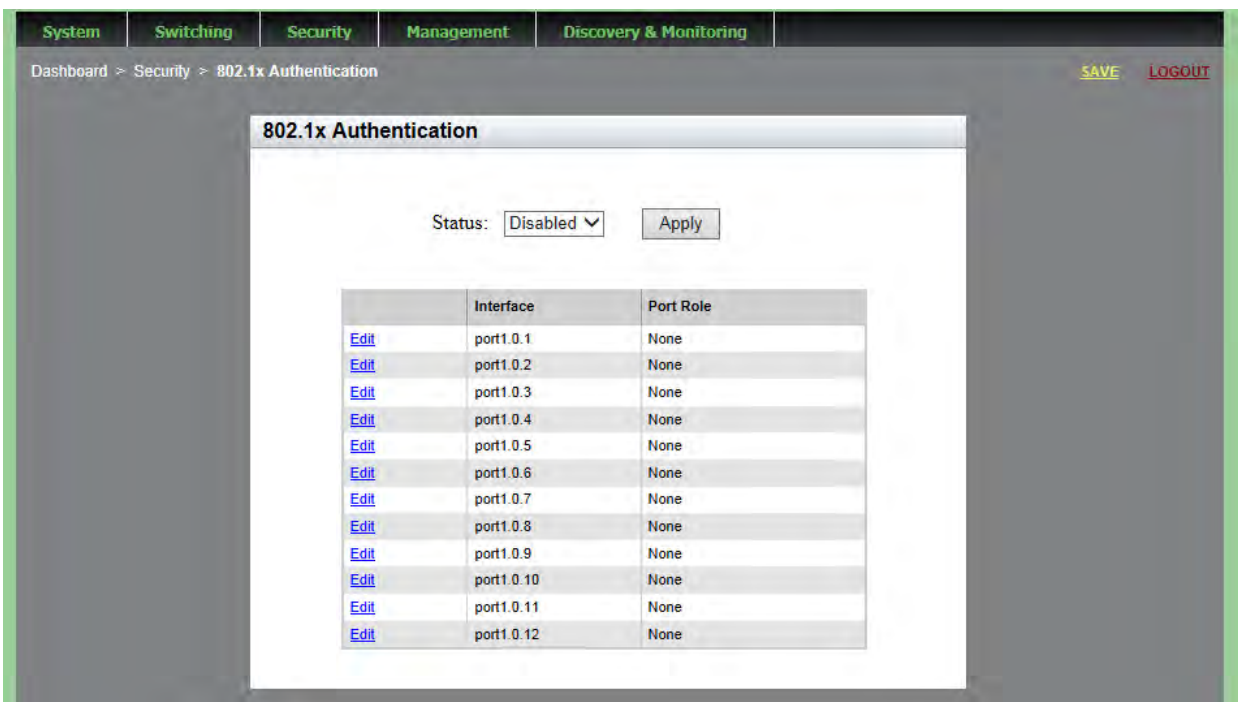


Figure 64. 802.1x Authentication Page

3. Use the pull-down menu next to the Status field to select **Enabled**.
4. Click **Apply**.

Configuring 802.1x Port-based Authentication

To configure 802.1x port authentication on a port, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57 on page 166.

2. From the Security tab drop-down menu, select **802.1x Port Authentication**.

The 802.1x Authentication page is displayed. See Figure 64 on page 187.

3. Click Edit next to the port that you want to modify.

The Modify 802.1x Authentication page is displayed. See Figure 65.

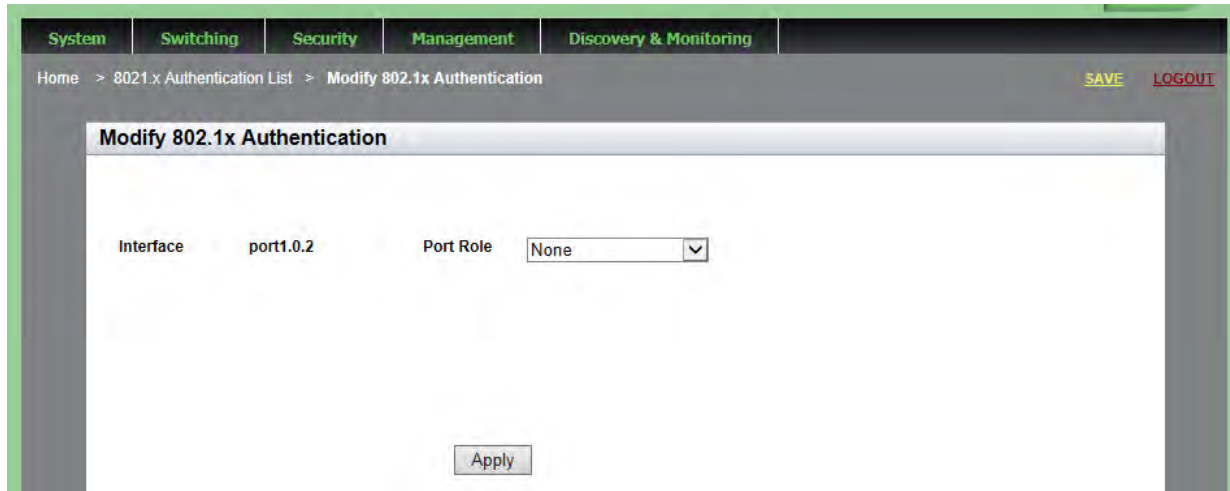


Figure 65. Modify 802.1x Authentication Page

4. Use the pull-down menu next to the **Port Role** field to select **Authenticator**.

The Modify 802.1x Authentication page expands to display the Authenticator parameters. See Figure 66 on page 189.

System Switching Security Management Discovery & Monitoring

Home > 802.1x Authentication List > Modify 802.1x Authentication SAVE LOGOUT

Modify 802.1x Authentication

| | | | |
|--|--------------|-----------|---------------|
| Interface | port1.0.2 | Port Role | Authenticator |
| Authentication Mode | Unauthorized | | |
| Timeouts | | | |
| Quiet-period | 60 | | |
| Tx-period | 30 | | |
| Reauth-period | 3600 | | |
| Supplicant-timeout | 30 | | |
| Server-timeout | 30 | | |
| <input type="checkbox"/> Re-authentication | | | |
| Number of Re-auth Requests | 2 | | |
| Port Control Direction | Both | | |
| <input type="checkbox"/> Dynamic VLAN Creation | | | |
| Type | Multi | | |
| Guest VLAN | | | |
| Host Mode | Single-Host | | |
| <input type="checkbox"/> Mac Authentication | | | |
| <input type="checkbox"/> Re-auth Learning | | | |
| <input type="button" value="Apply"/> | | | |

HELP

Port Id— Indicates the port number.

Port Role— Indicates that you've selected the port as an Authenticator.

Authentication Mode— Indicates the authentication mode. Choose from the following:

- **Unauthorized:** Sets the port to the 802.1x authenticator role, in the unauthorized state. Although the port is in the authenticator role, the switch blocks all authentication on the port. If you set all the ports on the switch to this setting, then no clients can log on and forward packets through them.
- **Force-authorized:** Sets port to the 802.1x authenticator role, in the force-authorized state. A port in the force-authorized state transitions to the authorized state without any authentication exchanges required. The port transmits and receives traffic normally without 802.1X-based authentication of the clients.
- **Auto:** Sets the port to the 802.1X port-based authenticator role. A port in this state begins in the unauthorized state, forwarding only EAPOL frames, until a client has logged on successfully.

Quiet Period— Sets the number of seconds that an authenticator port remains in the quiet state following a failed authentication exchange with a client. The

Figure 66. Modify 802.1x Authentication Page Expanded

5. Modify the following fields as needed:

- Interface**— Indicates the port number.
- Port Role**— Indicates that you have selected the port as an Authenticator.
- Authentication Mode**— Sets the authentication mode. Choose from the following:

| | |
|--------------|---|
| Unauthorized | Sets the port to the 802.1x authenticator role, in the unauthorized state. Although the port is in the authenticator role, the switch blocks all authentication on the port. If you set all the ports on the switch to this setting, then no clients can log on and forward packets through them. |
|--------------|---|

| | |
|------------------|---|
| Force-authorized | Sets port to the 802.1x authenticator role, in the force-authorized state. A port in the force-authorized state transitions to the authorized state without any authentication exchanges required. The port transmits and receives traffic normally without 802.1X-based authentication of the clients. |
|------------------|---|

| | |
|------|--|
| Auto | Sets the port to the 802.1X port-based authenticator role. A port in this state begins in the unauthorized state, forwarding only EAPOL frames, until a client has logged on successfully. |
|------|--|

| | |
|------------|---|
| Supplicant | Sets the port to the 802.1X port-based supplicant role. A port in this state acts as a client. It has to log on by providing a valid username and password to the device it is connected to, typically another switch port, before forwarding traffic. A port set to the supplicant role and connected to another port that is not set to the authenticator role will begin to forward traffic after a timeout period and without logging on. |
|------------|---|

- Timeouts**— The following fields set the timers for this feature:

| | |
|--------------|--|
| Quiet Period | Sets the number of seconds that an authenticator port remains in the quiet state following a failed authentication |
|--------------|--|

exchange with a client. The range is 1 to 65,535 seconds. The default value is 60 seconds.

| | |
|--------------------|--|
| Tx-period | Sets the number of seconds an authenticator port waits for a response to an EAP-request/identity frame from a client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds. |
| Reauth-period | Specifies the time interval that an authenticator port requires a client to reauthenticate. The range is 1 to 65,535 seconds. The default value is 3600 seconds. |
| Supplicant-timeout | Sets the timer used by the switch to determine authentication server timeout conditions. The range is 1 to 65,535 seconds. The default value is 30 seconds. |
| Server-timeout | Sets the timer used by the switch to determine authentication server timeout conditions. The range is 1 to 65,535 seconds. The default value is 30 seconds. |

- Re-authentication**— Activates reauthentication on the authenticator port. The client must periodically reauthenticate according to the time interval set with the Reauth-period timer. Click the box to activate this field.
- Number of Re-auth Requests**— Specifies the maximum number of times the switch retransmits EAP Request packets to a client before it times out an authentication session. The range is 1 to 10 retransmissions. The default value is 2.
- Port Control Direction**— Specifies whether authenticator ports that are in the unauthorized state should forward egress broadcast and multicast traffic. Choose from the following:

In Specifies that authenticator ports in the unauthorized state should forward egress broadcast and multicast traffic, and discard the ingress broadcast and multicast traffic. This is the default setting.

Both Specifies that authenticator ports in the unauthorized state should discard both ingress and egress broadcast and multicast traffic.

- Dynamic VLAN Creation**— Activates dynamic VLAN assignments of authenticator ports. Click the box to activate this field.
- Type**— Activates dynamic VLAN assignments of authenticator ports. Choose from the following:

Single Specifies that an authenticator port forwards packets of only those supplicants that have the same VID as the supplicant who initially logged on.

Multi Specifies that an authenticator port forwards packets of all supplicants, regardless of the VIDs in their client accounts on the RADIUS server.

- Guest VLAN**— Specifies the ID number of a VLAN that is the guest VLAN of an authenticator port. You can enter only one VID.
- Host Mode**— Sets the operating modes on authenticator ports. Choose from the following:

Single-host Specifies the single-host operating mode. An authenticator port set to this mode forwards only those packets from the one client who initially logs on. This is the default setting.

Multi-host Specifies the multiple-host operating mode. An authenticator port set to this mode forwards all packets after one client logs on. This is referred to as piggy-backing.

Multi-suppliant Specifies the multiple-suppliant operating mode. An authenticator port set to this mode requires that all clients log on.

- Mac Authentication**— Activates MAC address-based authentication on authenticator ports. An authenticator port that uses this type of authentication extracts the source MAC address from the initial frames from a supplicant and automatically sends it as the supplicant's username and password to the authentication server. This authentication method does not require 802.1x client software on supplicant nodes. Click the box to activate this field.

- Re-Auth Learning**— Forces ports that are using MAC address authentication into the unauthorized state. You may use this setting to reauthenticate the nodes on authenticator ports. Click the box to activate this field.

6. Click **Apply**.

7. Click **SAVE**.

Displaying the 802.1x Authentication Port Settings

To display the 802.1x Authentication port settings, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57 on page 166.

2. From the Security tab drop-down menu, select **802.1x Port Authentication**.

The 802.1x Authentication page is displayed. See Figure 64 on page 187.

3. Click View next to the port that you want to display.

The 802.1x Authentication View page is displayed. See Figure 67.

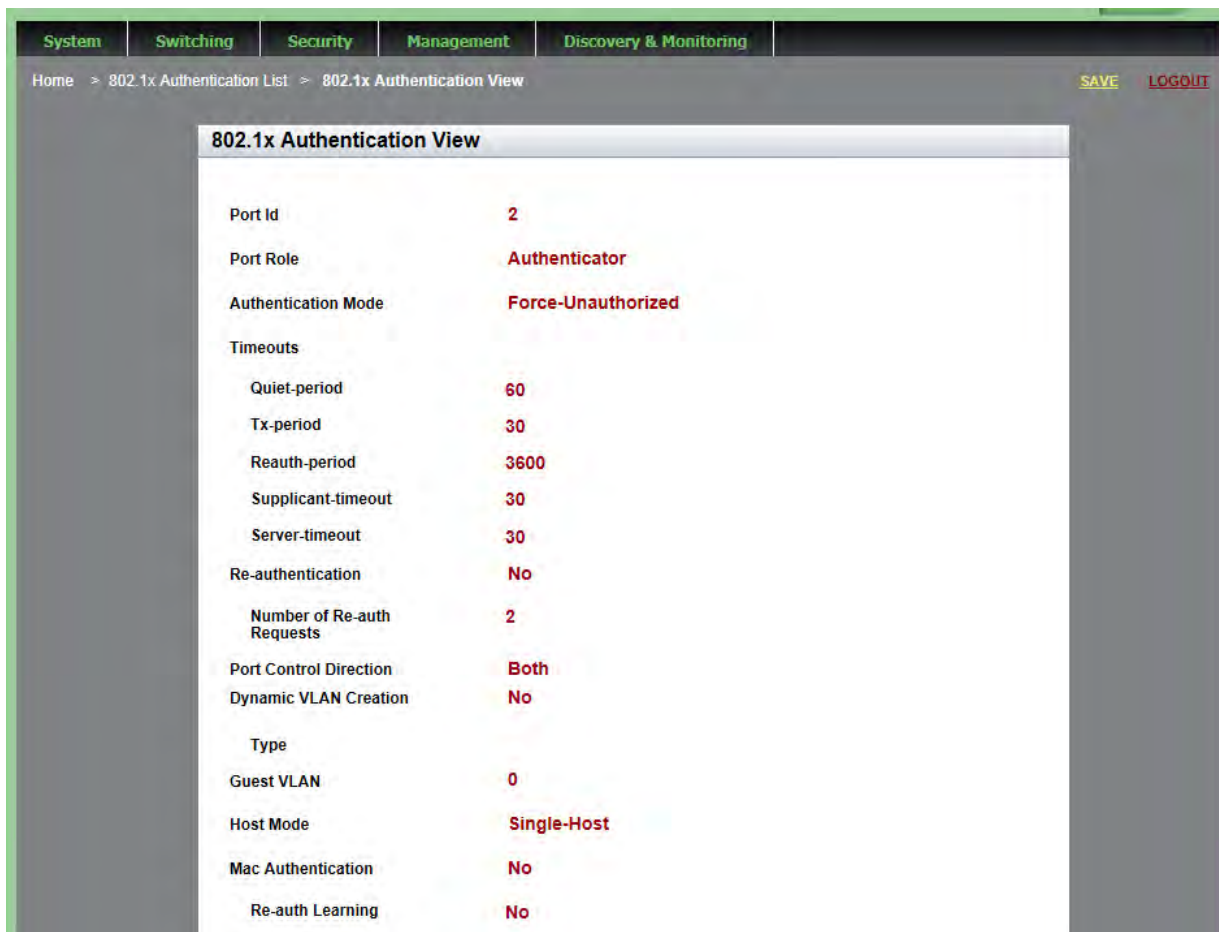


Figure 67. 802.1x Authentication View Page

Disabling 802.1x Port-based Authentication on the Switch

To disable the 802.1x port-based Authentication feature on a switch, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57 on page 166.

2. From the Security tab drop-down menu, select **802.1x Port Authentication**.

The 802.1x Authentication page with the Status field set to **Enabled** is displayed. See Figure 68.

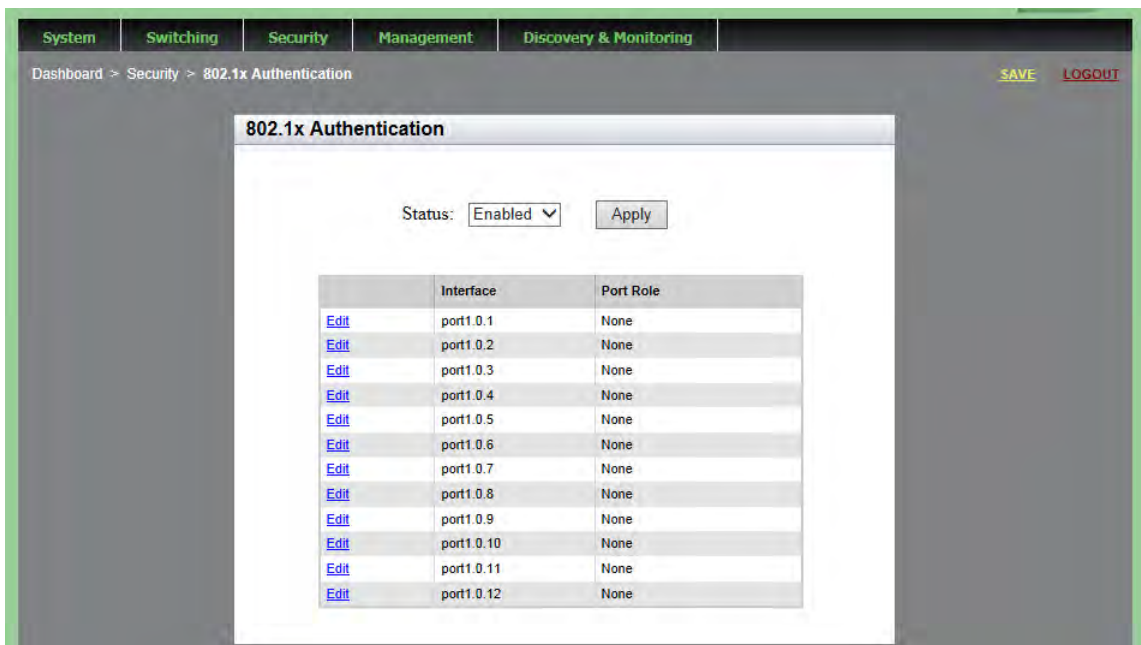


Figure 68. 802.1x Authentication Page with Status Enabled

3. Use the pull-down menu next to the **Status** field to select **Disabled**.
4. Click **Apply**.
5. Click **SAVE**.

Disabling 802.1x Port-based Authentication on a Port

To disable 802.1x port authentication on a port, do the following:

1. Hover the cursor over the **Security** tab.

The Security tab is displayed. See Figure 57 on page 166.

2. From the Security tab drop-down menu, select **802.1x Port Authentication**.

The 802.1x Authentication page is displayed. See Figure 64 on page 187.

3. Click E**dit** next to the port that you want to modify.

The Modify 802.1x Authentication page is displayed. See Figure 65 on page 188.

4. Use the pull-down menu next to the **Port Role** field to select **None**.

5. Click **Apply**.

6. Click **SAVE**.

Chapter 18

Setting IPv4 and IPv6 Management

This chapter provides brief descriptions of IPv4 and IPv6 Management, and explains how to configure both types of IP addresses on the switch.

See the following sections:

- ❑ “Overview” on page 198
- ❑ “Assigning an IPv4 Address” on page 200
- ❑ “Assigning an IPv6 Address” on page 204
- ❑ “Displaying IP Addresses” on page 206
- ❑ “Modifying IP Addresses” on page 207

For more information about the IP management, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ IPv4 and IPv6 Management Addresses
- ❑ IPv4 and IPv6 Management Address Commands

Overview

If you use the AlliedWare Plus web interface to change the IP address of the switch, the web connection to the switch is lost. In order to maintain a connection with the switch, it is necessary to also have a local connection if you are going to change the IP address with the web interface. For information about a local connection to the switch, see the *AlliedWare Plus Management Software Command Line Interface User's Guide*.

The features listed in Table 3 require that the switch is assigned a management IP address in the web interface. The switch uses the address to identify itself to other network devices, such as TFTP servers and Telnet clients.

You can assign the switch an IPv4 address and an IPv6 address, but only one of each type. However, as shown in the table, a management IPv6 address only supports the TACACS+ client. To use features that are not supported by an IPv6 address, you must assign the switch an IPv4 address instead of or, in addition to, an IPv6 address.

Note

In the Command Line Interface, there are additional features that require either an IPv4 or IPv6 address.

Table 3. Web Interface Features that Require an IP Management Address

| Feature | Description | Supported by IPv4 Address | Supported by IPv6 Address |
|--|---|---------------------------|---------------------------|
| 802.1x port-based network access control | Used for port security. | yes | no |
| RADIUS client | Used for remote management authentication and for 802.1x port-based network access control. | yes | no |
| sFlow agent | Used to transmit packet statistics and port counters to an sFlow collector on your network. | yes | no |
| TACACS+ client | Used for remote management authentication using a TACACS+ server on your network. | yes | yes |

IP Management Guidelines

See the following list for guidelines about assigning the switch a management IPv4 or IPv6 address:

- ❑ You can assign the switch one IPv4 address and one IPv6 address.
- ❑ A management address must be assigned to a VLAN on the switch. It can be assigned to any VLAN, including the default VLAN, which has a VID of 1. For background information on VLANs, see Chapter 11, “Setting Port-based and Tagged VLANs” on page 125.
- ❑ If you assign both IPv4 and IPv6 addresses to the switch, you must assign them to the *same* VLAN.
- ❑ An IPv4 management address can be assigned manually or from a DHCP server on your network. (To learn the switch's MAC address, go to the Dashboard page. See Figure 4 on page 23.)
- ❑ An IPv6 address must be assigned manually. The switch does not support the assignment of an IPv6 management address from a DHCP server.
- ❑ You must assign the switch a default gateway if the network devices, such as syslog servers and Telnet workstations, are not members of the same subnet as the management address. This IP address designates an interface on a router or other Layer 3 device that represents the first hop to the remote subnets or networks where the network devices are located.
- ❑ The default gateway address, if needed, must be a member of the same subnet as the management address.

Assigning an IPv4 Address

Use one of the following procedures to assign a static or DHCP IPv4 address to the switch.

- ❑ “Assigning a Static IPv4 Address”
- ❑ “Assigning a DHCP IPv4 Address” on page 201

Assigning a Static IPv4 Address

To assign a static IPv4 address, do the following:

1. Hover the cursor over the **Management** tab.

The Management tab is displayed. See Figure 69.



Figure 69. Management Tab

2. From the **Management** tab drop-down menu, select **IP**.

The IP Management Configuration page with the Static IP Address field selected is displayed. See Figure 70.

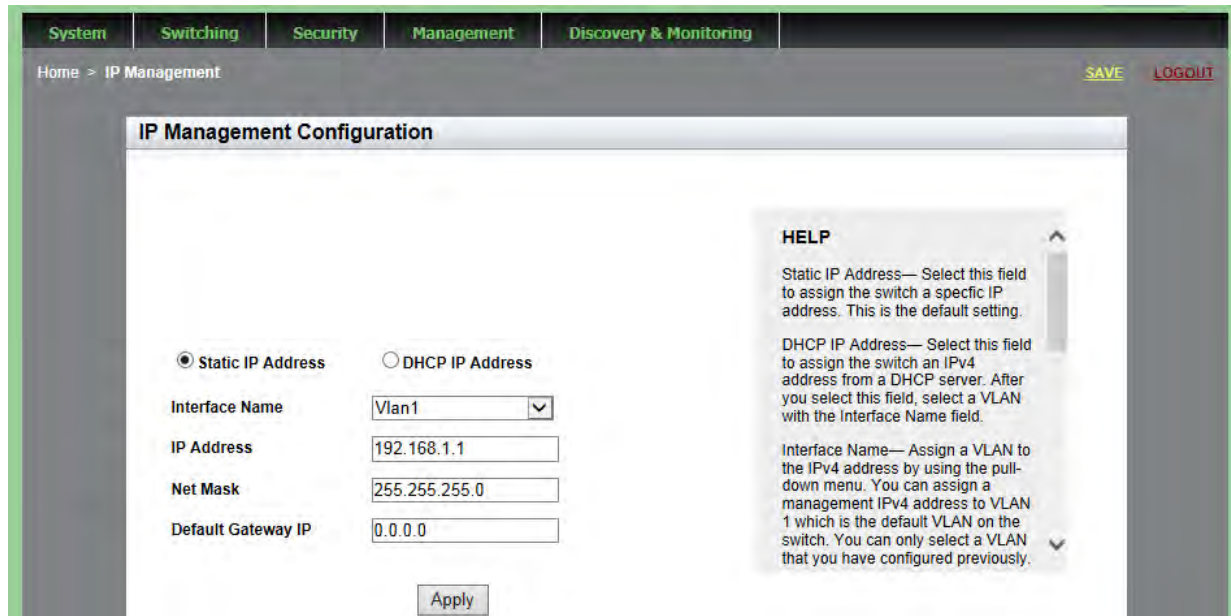


Figure 70. IP Management Configuration Page with Static IP Address

3. Click the box next to the **Static IP Address** field. This is the default setting.
4. Assign a VLAN to the IPv4 address by using the pull-down menu next to the **Interface Name** field.

You can only select a VLAN that you have configured previously. For information about how to assign a VLAN, see Chapter 11, "Setting Port-based and Tagged VLANs" on page 125.

5. Enter an IPv4 address in the **IP Address** field in the following format:

xxx.xxx.xxx.xxx

where xxx is a number from 0 to 255. There are four groups of numbers that are separated by periods.

6. Enter a value in the **Net Mask** field to assign a subnet mask to the switch.

The Net Mask is a decimal number that represents the number of bits, from left to right, that constitute the network portion of the address. For example:

- The decimal mask 16 is equivalent to the mask 255.255.0.0.
- The decimal mask 24 is equivalent to the mask 255.255.255.0.

7. To assign a default gateway to the switch, enter an IPv4 address in the **Default IP Gateway** field.

The IPv4 address is specified in the following format:

xxx.xxx.xxx.xxx

where xxx is a number from 0 to 255. There are four groups of numbers that are separated by periods.

For more information about the default gateway, see "IP Management Guidelines" on page 199.

8. Click **Apply**.
9. Click **SAVE**.

Assigning a DHCP IPv4 Address

Use this procedure to assign the switch an IPv4 management address from a DHCP server. This procedure activates the DHCP client, which automatically queries the network for a DHCP server. The client also queries for a DHCP server whenever you reset or power-cycle the switch.



Caution

When you use the web interface to assign an IPv4 address to the switch using DHCP, you lose connection with the switch. To maintain your connection with the switch, make sure you have a local connection to the switch when you assign a DHCP IP address.

To assign a DHCP IPv4 address, do the following:

1. Hover the cursor over the **Management** tab.

The Management tab is displayed. See Figure 69 on page 200.

2. From the **Management** tab drop-down menu, select **IP**.
3. Click the box next to the **DHCP Address** field.

The IP Management Configuration page with the DHCP IP Address selected is displayed. See Figure 71.

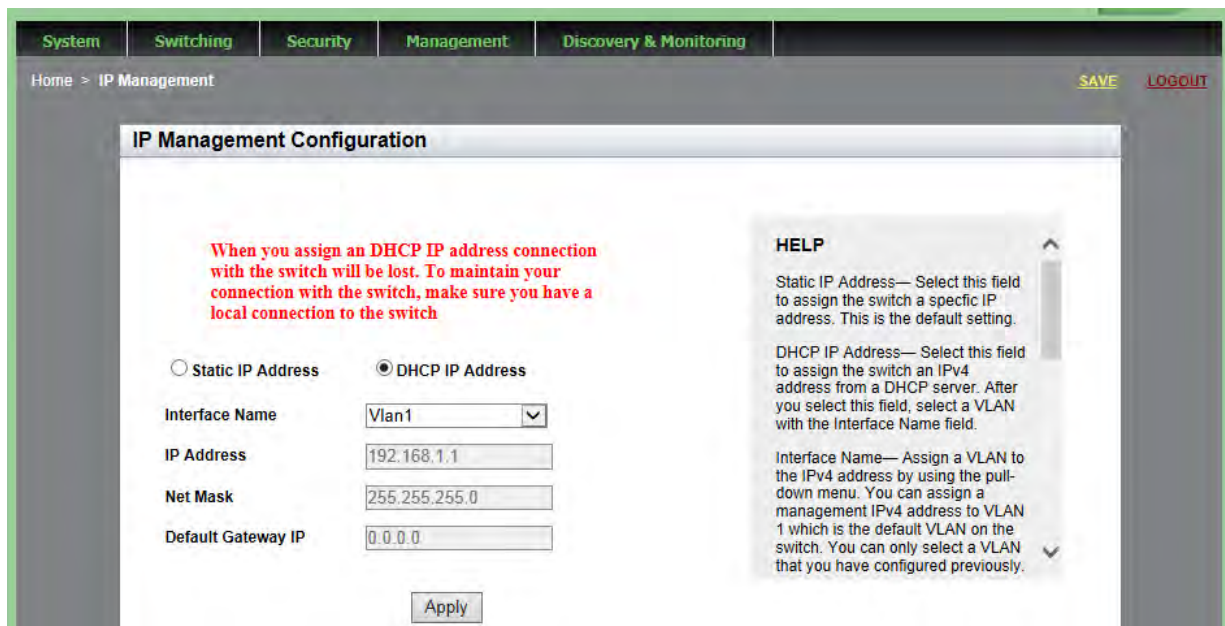


Figure 71. IP Management Configuration Page with DHCP

4. To select a VLAN, use the pull-down menu next to the **Interface Name** field.

You can only select a VLAN that you have configured previously. For information about how to assign a VLAN, see Chapter 11, “Setting Port-based and Tagged VLANs” on page 125.

Note

You cannot select the **IP address**, **Net Mask**, and **Default Gateway** IP fields from this page.

5. Click **Apply**.
6. Click **SAVE**.

Assigning an IPv6 Address

To assign an IPv6 address to the switch, do the following:

1. Hover the cursor over the **Management** tab.

The Management tab is displayed. See Figure 69 on page 200.

2. From the **Management** tab drop-down menu, select **IPv6**.

The IPv6 Management Configuration page is displayed. See Figure 72.

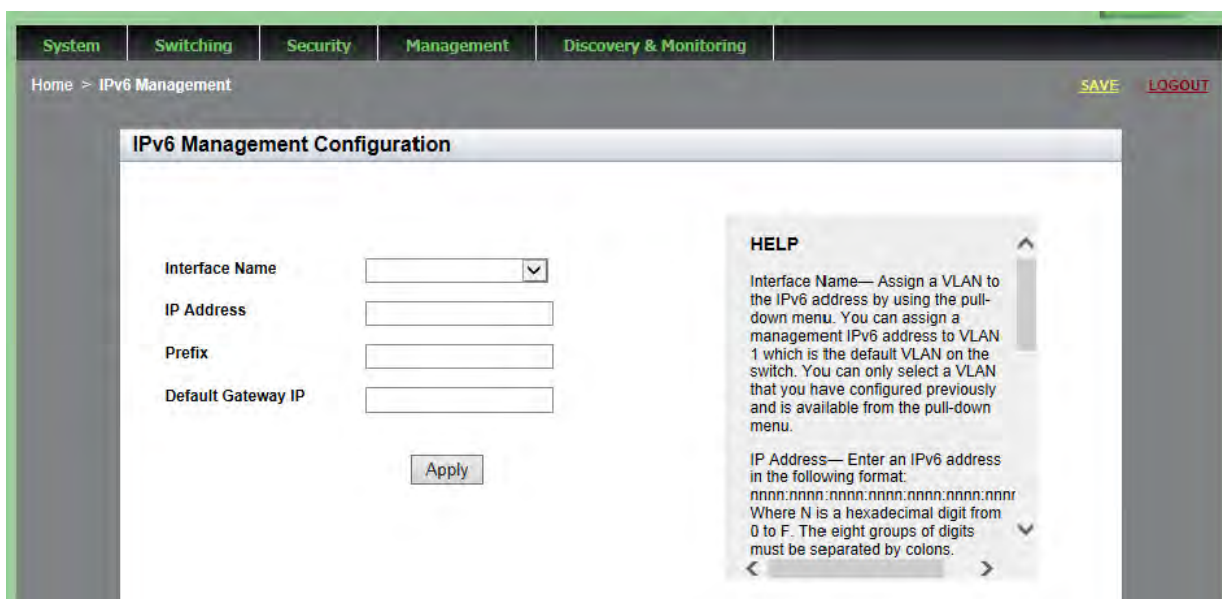


Figure 72. IPv6 Management Configuration Page

3. Assign a VLAN to the IPv6 address by using the pull-down menu next to the **Interface Name** field.

You can only select a VLAN that you have configured previously. For information about how to assign a VLAN, see Chapter 11, “Setting Port-based and Tagged VLANs” on page 125.

4. Enter an IPv6 address in the **IP Address** field in the following format:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

Where n is a hexadecimal number from 0 to F. The eight groups of numbers must be separated by colons. Groups where all four digits are "0" can be omitted. Leading "0's" in groups can also be omitted. For example, the following IPv6 addresses are equivalent:

```
12c4:421e:09a8:0000:0000:0000:00a4:1c50
```

```
12c4:421e:9a8::a4:1c50
```

5. To assign a prefix to the IPv6 address, enter a value in the **Prefix** field.

The prefix is a decimal number that represents the number of bits, from left to right, that constitute the network portion of the address. (In an IPv4 address, the prefix is called the subnet mask.) For example:

- The decimal mask 16 is equivalent to the prefix 255.255.0.0.
- The decimal mask 24 is equivalent to the prefix 255.255.255.0.

6. To assign an IPv6 default gateway to the switch, enter an IPv6 address in the **Default IP Gateway** field.

A default gateway is an address of an interface on a router or other Layer 3 device. It defines the first hop to reaching the remote subnets or networks where the network devices are located. You must assign the switch a default gateway address if the following are true:

- The remote management devices, such as Telnet workstations and TFTP servers, are not members of the same subnet as the IPv6 management address.
- The switch can have only one IPv6 default gateway.
- The IPv6 management address and the default gateway address must be members of the same subnet.

For more information about the default gateway, see "IP Management Guidelines" on page 199.

7. Click **Apply**.
8. Click **SAVE**.

Displaying IP Addresses

To display the IPv4 and IPv6 addresses, as well as the IPv4 and IPv6 gateway addresses assigned to the switch, go to the Dashboard page. For an example, see Figure 4 on page 23.

Modifying IP Addresses

To modify an IP address on the switch, choose one of the following procedures:

- ❑ “Modifying an IPv4 Static Address”
- ❑ “Changing a DHCP IPv4 Address to Static” on page 207
- ❑ “Modifying an IPv6 Address” on page 208



Caution

Modifying the IP address assigned to the switch may cause you to end the current login session and lose the connection to the web interface. To re-gain access to the web interface, enter the new IP address in your web browser.

Modifying an IPv4 Static Address

To modify an IPv4 address, do the following:

1. Hover the cursor over the **Management** tab.

The Management tab is displayed. See Figure 69 on page 200.

2. From the **Management** tab drop-down menu, select **IP**.

The IP Management Configuration page with the Static IP Address field selected is displayed. See Figure 70 on page 200.

3. Modify the IP address in the **IP Address** field.
4. Click **Apply**.
5. Click **SAVE**.

Changing a DHCP IPv4 Address to Static

To change a DHCP IPv4 address to a static address, do the following:

1. Hover the cursor over the **Management** tab.

The Management tab is displayed. See Figure 69 on page 200.

2. From the **Management** tab drop-down menu, select **IP**.

The IP Management Configuration page with DHCP IP Address field selected is displayed. See Figure 71 on page 202.

3. Select **Static IP Address**.
4. Click **Apply**.
5. Click **SAVE**.

Modifying an IPv6 Address

To modify an IPv6 address, do the following:

1. Hover the cursor over the **Management** tab.

The Management tab is displayed. See Figure 69.

2. From the **Management** tab drop-down menu, select **IPv6**.

The IPv6 Management Configuration page is displayed. See Figure 72 on page 204.

3. Modify the IPv6 address in the **IP Address** field.

4. Click **Apply**.

5. Click **SAVE**.

Chapter 19

Setting LLDP and LLDP-MED

This chapter provides a brief description of the Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) features, and explains how to enable these features on the switch. See the following sections:

- ❑ “Overview” on page 210
- ❑ “Setting LLDP Locations” on page 211
- ❑ “Configuring LLDP and LLDP-MED” on page 219
- ❑ “Displaying LLDP Neighbor Information” on page 231
- ❑ “Displaying LLDP Statistics” on page 236
- ❑ “Displaying LLDP Locations” on page 238
- ❑ “Displaying LLDP and LLDP-MED Settings” on page 241
- ❑ “Disabling LLDP on the Switch” on page 247

For more information about the LLDP and LLDP-MED features, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User’s Guide*:

- ❑ 802.1x Port-based Network Access Control
- ❑ 802.1x Port-based Network Access Control Commands

Overview

Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) allow Ethernet network devices, such as switches and routers, to receive and/or transmit device-related information to directly connected devices on the network that are also using the protocols, and to store the information that is learned about other devices. The data sent and received by LLDP and LLDP-MED are useful for many reasons. The switch can discover other devices directly connected to it. Neighboring devices can use LLDP to advertise some parts of their Layer 2 configuration to each other, enabling some types of misconfiguration to be more easily detected and corrected.

LLDP is a “one-hop” protocol. LLDP information can only be sent to and received by devices that are directly connected to each other, or connected via a hub or repeater. Devices that are directly connected to each other are called *neighbors*. Advertised information is not forwarded on to other devices on the network. In addition, LLDP is a one-way protocol. That is, the information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors, and the communication ends there. Transmitted advertisements do not solicit responses, and received advertisements do not solicit acknowledgements. LLDP cannot solicit any information from other devices. LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static port trunks or LACP trunks, but not on the trunks themselves, and on switch ports that belong to VLANs, but not on the VLANs themselves.

Each port can be configured to transmit local information, receive neighbor information, or both. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value (TLV) elements, each of which contains a particular type of information about the device or port transmitting it.

A single LLDPDU contains multiple TLVs. TLVs are short information elements that communicate complex data, such as variable length strings, in a standardized format. Each TLV advertises a single type of information, such as its device ID, type, or management addresses.

Setting LLDP Locations

Creating LLDP locations lets you create IDs that are then used in following procedures. The procedures in this section allow you to create LLDP Civic, Coordinate, and Emergency Location Identifier Number (ELIN) locations. See the following:

- ❑ “Creating a Civic Location”
- ❑ “Creating a Coordinate Location” on page 215
- ❑ “Creating an ELIN Location” on page 217

Creating a Civic Location

To create an LLDP Civic Location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73.



Figure 73. Discovery & Monitoring Tab

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, move the cursor to the right and hover over **Locations**.

The Locations tab is displayed. See Figure 74 on page 212.

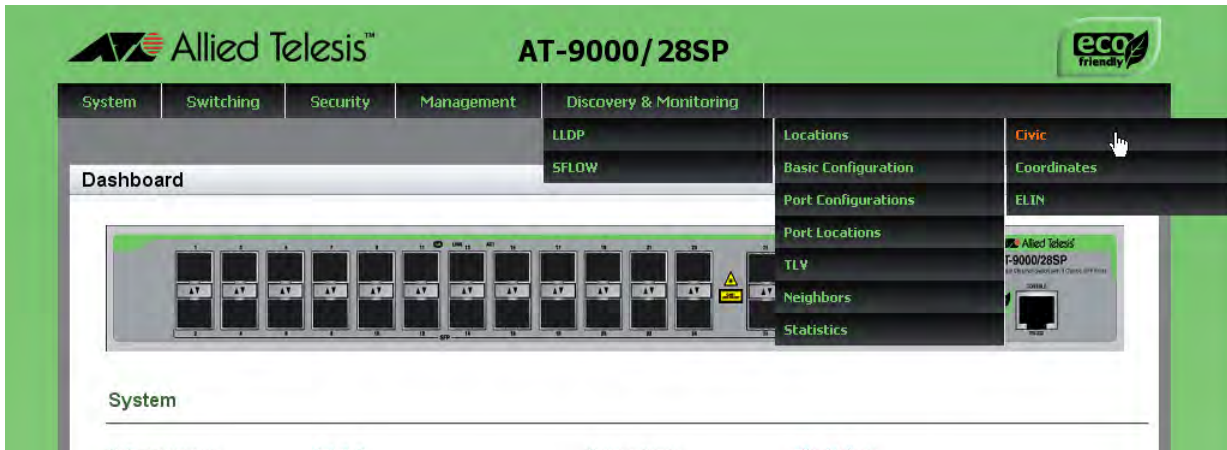


Figure 74. Locations Tab

4. From the Locations tab drop-down menu, move the cursor to the right and select **Civic**.

The LLDP Civic Location page is displayed. See Figure 75.

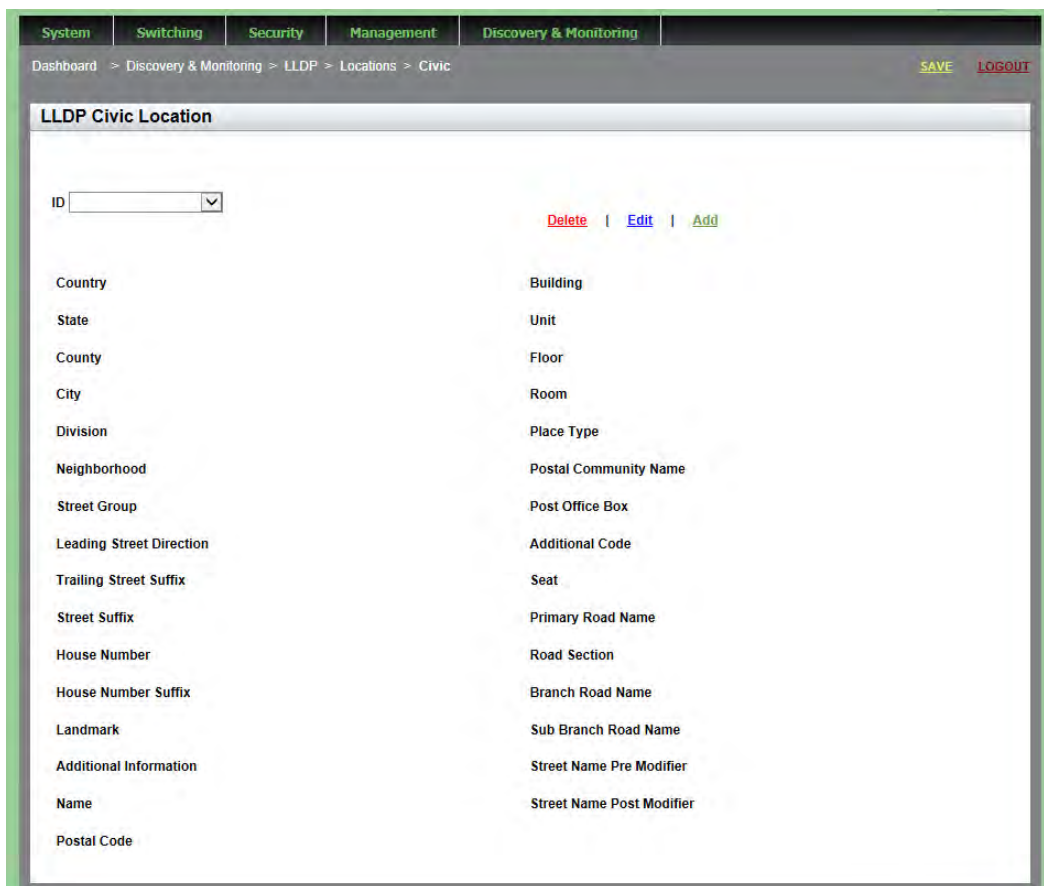


Figure 75. LLDP Civic Location Page

The following fields are displayed:

- ID**
- Country**
- State**
- County**
- City**
- Division**
- Neighborhood**
- Street Group**
- Leading Street Direction**
- Trailing Street Suffix**
- Street Suffix**
- House Number**
- House Number Suffix**
- Landmark**
- Additional Information**
- Name**
- Postal Code**
- Building**
- Unit**
- Floor**
- Room**
- Place Type**
- Postal Community Name**
- Post Office Box**
- Additional Code**
- Seat**
- Primary Road Name**
- Road Selection**
- Branch Road Name**
- Sub Branch Road Name**
- Street Name Pre Modifier**
- Street Name Post Modifier**

5. Click **Add**.

The Add LLDP Civic Location Page is displayed. See Figure 76.

Figure 76. Add LLDP Civic Location Page

6. Define or edit the fields as needed.

You must define the **ID** and **Country** fields. The remaining fields are optional.

The fields are listed in Step 4. Each field can contain up to 255 characters.

Note

The ID number indicates the civic location. The Country field must contain two uppercase characters, for example, "US."

7. Click **Apply**.
8. Click **SAVE**.

Creating a Coordinate Location

To create an LLDP Coordinate Location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, move the cursor to the right and hover over **Locations**.

The Locations tab is displayed. See Figure 74 on page 212.

4. From the Locations tab drop-down menu, move the cursor to the right and select **Coordinates**.

The LLDP Coordinate Location page is displayed. See Figure 77.

| | ID | Latitude | Latitude Resolution | Longitude | Longitude Resolution | Altitude | Altitude Resolution | Datum |
|---|----|-----------|---------------------|-----------|----------------------|------------------|---------------------|-------|
| Delete Edit | 5 | 10.000000 | 7 | 40.000000 | 7 | 20.000000 Meters | 3 | WGS84 |

Figure 77. LLDP Coordinate Location Page

5. From the LLDP Coordinate Location page, click **Add**.

The Add LLDP Coordinate Location page is displayed. See Figure 78.

Figure 78. Add LLDP Coordinate Location Page

6. Define or edit the following fields as needed:
 - ❑ **ID**— LLDP Coordinate Location ID.
 - ❑ **Latitude**— Latitude value in decimal degrees. The range is -90.0° to 90.0°. The field accepts up to two digits to the right of the decimal point.
 - ❑ **Latitude Resolution**— Latitude resolution as the number of valid bits. The range is 0 to 34.
 - ❑ **Longitude**— Longitude value in decimal degrees. The range is -180.0° to 180.0°. The field accepts up to two digits to the right of the decimal point.
 - ❑ **Longitude Resolution**— Longitude resolution as the number of valid bits. The range is 0 to 34.
 - ❑ **Altitude**— Altitude in meters or floors. For the altitude in meters, the range is -2097151.0 to 2097151.0 meters. The parameter accepts up to eight digits to the right of the decimal point. For altitude in the number of floors, the range is -2097151.0 to 2097151.0. Use the **Altitude Type** field to specify meters or floors.
 - ❑ **Altitude Type**— Choose between meters and floors.
 - ❑ **Altitude Resolution**— Altitude resolution as the number of valid bits. The range is 0 to 30.

- ❑ **Datum**— Geodetic system (or datum) of the coordinates. Choose one of the following:

nad83-mlw Mean lower low water datum 1983

nad83-navd North American vertical datum 1983

wgs84 World Geodetic System 1984

7. Click **Apply**.

8. Click **SAVE**.

Creating an ELIN Location

The Emergency Location Identifier Number (ELIN) TLV specifies the location of a network device by its ELIN.

To create an LLDP ELIN location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, move the cursor to the right and hover over **Locations**.

The Locations tab is displayed. See Figure 74 on page 212.

4. From the Locations tab drop-down menu, move the cursor to the right and select **ELIN**.

The LLDP ELIN Location List page is displayed. See Figure 79.

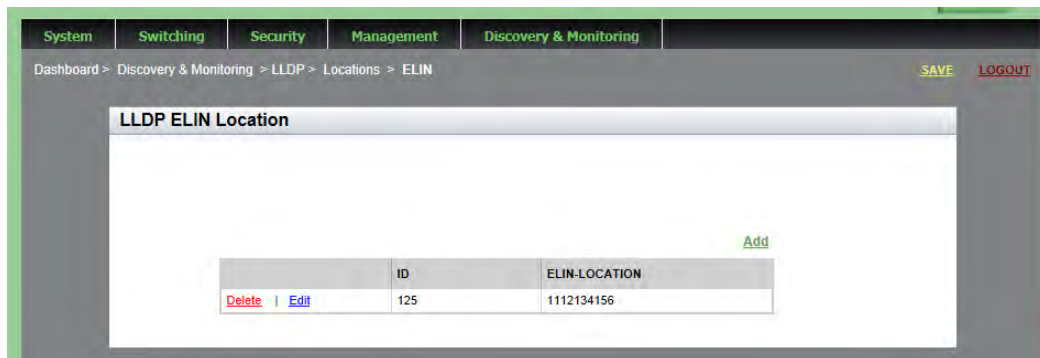


Figure 79. LLDP ELIN Location List Page

5. From the LLDP ELIN Location page, click **Add**.

The LLDP ELIN Location page is displayed. See Figure 80.

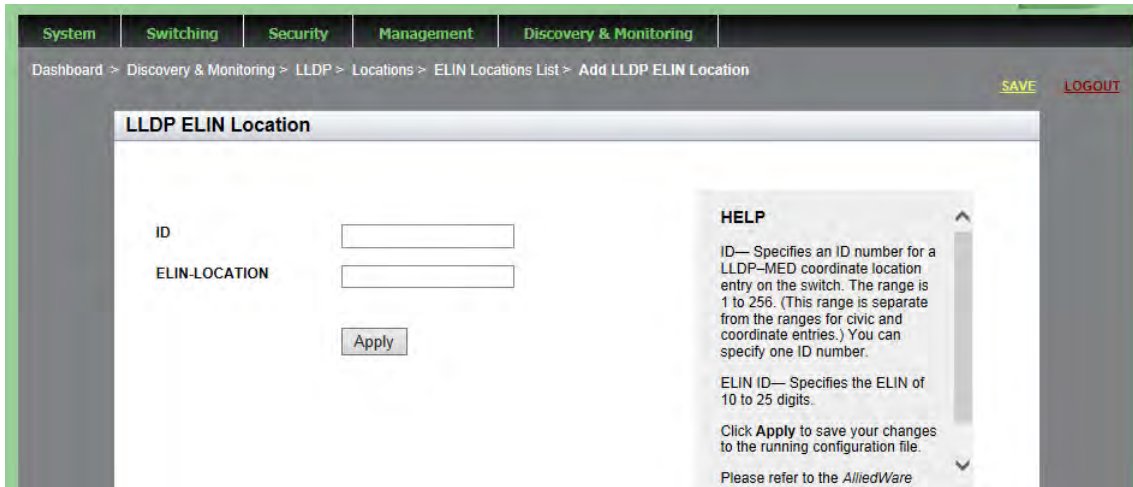


Figure 80. LLDP ELIN Location Page

6. Define or edit the following fields as needed:
 - ❑ **ID**— ID number for an LLDP-MED coordinate location entry on the switch. The range is 1 to 256. (This range is separate from the ranges for civic and coordinate entries.) You can specify one ID number.
 - ❑ **ELIN LOCATION**— ELIN of 10 to 25 digits.
7. Click **Apply**.
8. Click **SAVE**.

Configuring LLDP and LLDP-MED

To configure LLDP and LLDP-MED, perform the following procedures:

- ❑ “Setting the Basic LLDP Configuration”
- ❑ “Setting LLDP Port Assignments” on page 220
- ❑ “Assigning Port Locations” on page 222
- ❑ “Enabling LLDP TLV” on page 224
- ❑ “Enabling LLDP- MED TLV” on page 228

Setting the Basic LLDP Configuration

To set the basic LLDP configuration, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears to the right.

3. From the LLDP tab, move the cursor to the right and select **Basic Configuration**.

The LLDP Configuration page is displayed. See Figure 81.

The screenshot shows the LLDP Configuration page with the following fields and values:

| Field | Value |
|--------------------------------|--------------------------|
| Status | Disabled |
| Timer | 30 |
| Fast start Count | 3 |
| Holdtime Multiplier | 4 |
| Non Strict Med TLV Order Check | <input type="checkbox"/> |
| Notification Interval | 5 |
| Reinit | 2 |
| Tx Delay | 2 |
| Total Neighbors | 0 |
| Neighbors Last Update | 4h:59m:45s |

The HELP section on the right contains the following text:

HELP

Status— Indicates whether LLDP is enabled or disabled on the switch. By default, LLDP is disabled on the switch.

Timer— Specifies the transmit interval. The range is 5 to 32,768 seconds.

Fast Start Count— Indicates the fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from a port when it begins sending LLDP-MED advertisements from a port, for instance when it detects

Figure 81. LLDP Configuration Page

4. Define or edit the following fields as needed:
 - Status**— Choose whether LLDP is enabled or disabled on the switch. By default, LLDP is disabled on the switch.
 - Timer**— Transmit interval. The range is 5 to 32,768 seconds. The default value is 30 seconds.
 - Fast Start Count**— Fast-start count for LLDP-MED. The fast-start count determines how many fast-start advertisements LLDP sends from a port when it begins sending LLDP-MED advertisements from a port, for instance when it detects a new LLDP-MED capable device. The range is 1 to 10. The default value is 3.
 - Holdtime Multiplier**— Holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) the switch advertises to the neighbors. The range is 2 to 10. The default value is 4.
 - Non Strict Med TLV Order Check**— Sets the switch to accept LLDP-MED advertisements, even if the TLVs are not in the standard order, as specified in ANSI/TIA-1057. This configuration is useful if the switch is connected to devices that send LLDP-MED advertisements in which the TLVs are not in the standard order. Click in the box next to this field to select the nonstrict Med TLV Order Check.
 - Notification Interval**— Notification interval. This is the minimum interval between LLDP SNMP notifications (traps). The range is 5 to 3,600 seconds. The default value is 5.
 - Reinit**— Reinitialization delay. This is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized. The range is 1 to 10 seconds. The default value is 2.
 - Tx Delay**— Transmission delay. This is the minimum time interval between transmissions of advertisements due to changes in LLDP local information. The range is 1 to 8192 seconds. The default value is 2.
 - Total Neighbors**— Indicates the number of LLDP neighbors the switch has discovered on all its ports. You cannot modify this field.
 - Neighbors Last Update**— Indicates the time since the LLDP neighbor table was last updated. You cannot modify this field.
5. Click **Apply**.
6. Click **SAVE**.

Setting LLDP Port Assignments

To assign LLDP to a port, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

- From the **Discovery & Monitoring** tab, hover over **LLDP** and then select **Port Configurations** on the right.

The LLDP Port Config page is displayed. See Figure 82.

| | Interface | Notification | Adv. Transmit | Adv. Received | MED Notifications |
|----------------------|------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|
| Edit | port1.0.1 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.2 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.3 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.4 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.5 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.6 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.7 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.8 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.9 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.10 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.11 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Edit | port1.0.12 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Figure 82. LLDP Port Config Page

The following fields are displayed:

- Interface**— Port number.
- Notification**— The switch sends LLDP-MED topology change notifications when devices are connected to, or disconnected from, the specified ports. By default, this field is not selected.
- Adv. Transmit**— The port sends LLDP advertisements. Ports configured to transmit LLDP advertisements send the mandatory TLVs and any optional LLDP TLVs they have been configured to send. By default, this field is selected.
- Adv. Receive**— The port accepts LLDP advertisements. Ports configured to receive LLDP advertisements accept all advertisements from their neighbors. By default, this field is selected.
- Med Notifications**— The switch sends LLDP-MED topology change notifications when devices are connected to, or disconnected from, the specified ports. By default, this field is not selected.

- Select **Edit** next to the port that you want to modify.

The Modify LLDP Port Configuration page is displayed. See Figure 83.

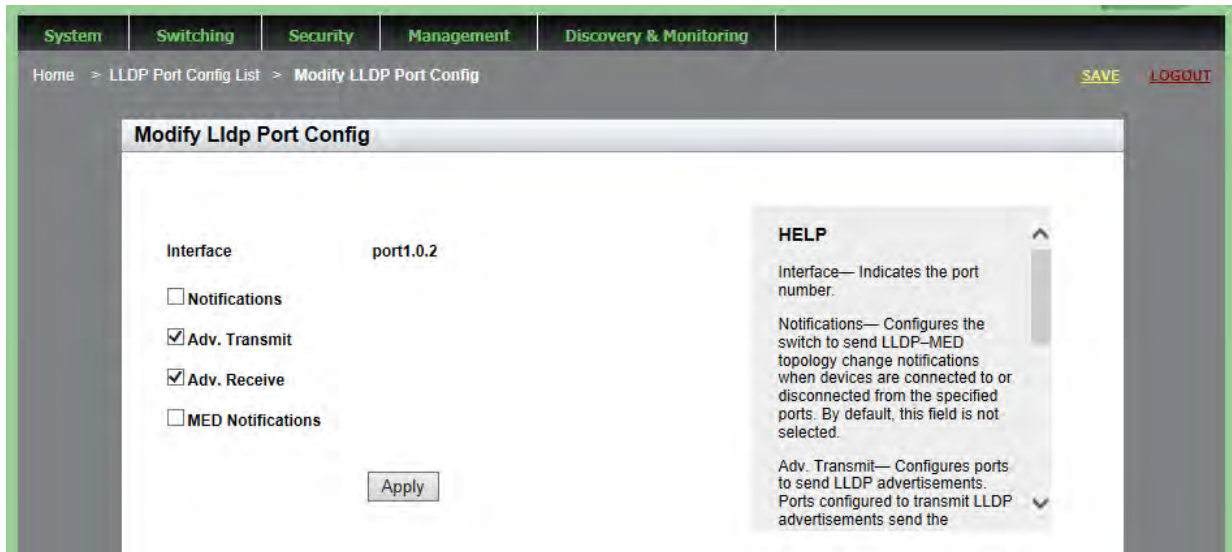


Figure 83. Modify LLDP Port Configuration Page

4. Change the settings as needed.

The definitions are listed in Step 2. Click on the box next to the field to select it.

Note

You cannot modify the port ID from this page. To change this field, go to the previous page (Figure 82, “LLDP Port Config Page” on page 221) and select **Edit** next to the port you want to modify.

5. Click **Apply**.
6. Click **SAVE**.

Assigning Port Locations

A port location is assigned to a Civic, Coordinate, or ELIN location ID. You must create these IDs *before* you assign a port location. For instructions, see “Setting LLDP Locations” on page 211.

To assign an LLDP port location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

- From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears on the right.

- From the LLDP tab, select **Port Locations** on the right.

The LLDP Port Location page is displayed. See Figure 84.

The screenshot shows the 'LLDP Port Location' page. At the top, there are navigation tabs: System, Switching, Security, Management, and Discovery & Monitoring. Below the tabs is a breadcrumb trail: Dashboard > Discovery & Monitoring > LLDP > Port Location. On the right side, there are 'SAVE' and 'LOGOUT' buttons. The main content area is titled 'LLDP Port Location' and contains a table with the following data:

| | Interface | Civic Location ID | Coordinate Location ID | ELIN Location ID |
|----------------------|------------|-------------------|------------------------|------------------|
| Edit | port1.0.1 | | | |
| Edit | port1.0.2 | | | |
| Edit | port1.0.3 | | | |
| Edit | port1.0.4 | | | |
| Edit | port1.0.5 | | | |
| Edit | port1.0.6 | | | |
| Edit | port1.0.7 | | | |
| Edit | port1.0.8 | | | |
| Edit | port1.0.9 | | | |
| Edit | port1.0.10 | | | |
| Edit | port1.0.11 | | | |
| Edit | port1.0.12 | | | |

Figure 84. LLDP Port Location Page

The fields displayed are described in Step 5.

- Click **Edit** next to the port (listed under **Interface**) that you want to modify.

The Modify LLDP Port Location page is displayed. See Figure 85 on page 224.

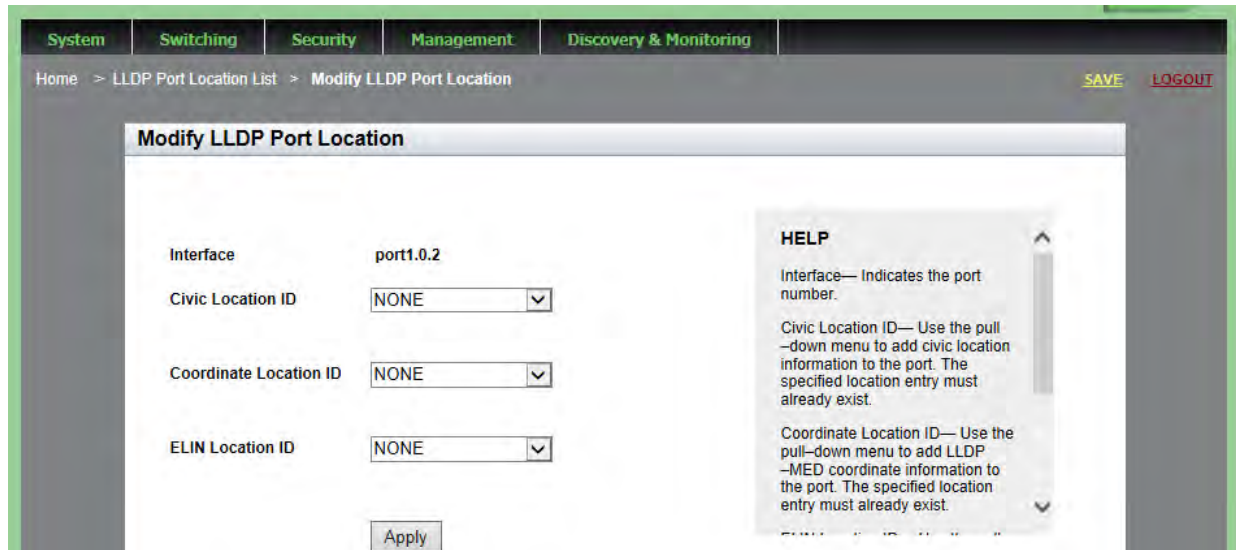


Figure 85. Modify LLDP Port Location Page

5. Change the parameters as needed. Use the drop-down menu next to a field to select.
 - Interface**— Indicates the port number. You cannot modify this parameter on this page.
 - Civic Location ID**— Use the pull-down menu to add civic location information to the port. The specified location entry must already exist.
 - Coordinate Location ID**— Use the pull-down menu to add LLDP-MED coordinate information to the port. The specified location entry must already exist.
 - ELIN Location ID**— Use the pull-down menu to add ELIN location information to the port. The specified location entry must already exist.
6. Click **Apply**.
7. Click **SAVE**.

Enabling LLDP TLV

To enable LLDP TLV, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab is displayed.

- From the LLDP tab, hover over **TLV**.

The LLDP TLV tab is displayed in Figure 86.

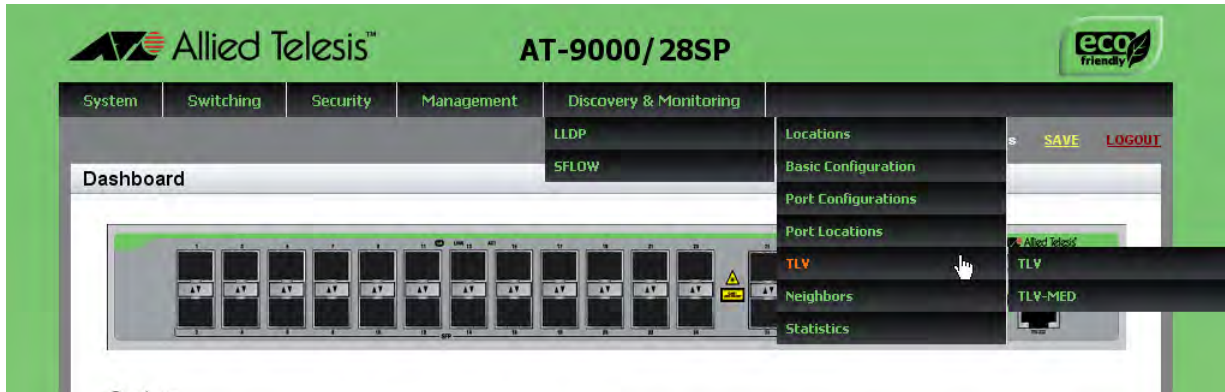


Figure 86. LLDP TLV Tab

- Move your cursor to the right and select **TLV** again.

The LLDP TLV page is displayed. See Figure 87.

The screenshot displays the LLDP TLV configuration page. The breadcrumb trail at the top reads: Dashboard > Discovery & Monitoring > LLDP > TLV > TLV. The page title is "LLDP TLV". Below the title is a table with 13 columns: Interface, Port Description, System Name, System Description, System Capabilities, Management Address, Port Vlan, Port And Protocol Vlans, Vlan Names, Protocol Ids, MAC Phy Config, Link Aggregation, and Max Frame Size. The first row (port1.0.1) has an "Edit" link in the first column. The second row (port1.0.2) has green checkmarks in all columns. The remaining rows (port1.0.3 to port1.0.12) have "Edit" links in the first column and are otherwise empty.

| | Interface | Port Description | System Name | System Description | System Capabilities | Management Address | Port Vlan | Port And Protocol Vlans | Vlan Names | Protocol Ids | MAC Phy Config | Link Aggregation | Max Frame Size |
|----------------------|------------|------------------|-------------|--------------------|---------------------|--------------------|-----------|-------------------------|------------|--------------|----------------|------------------|----------------|
| Edit | port1.0.1 | | | | | | | | | | | | |
| Edit | port1.0.2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Edit | port1.0.3 | | | | | | | | | | | | |
| Edit | port1.0.4 | | | | | | | | | | | | |
| Edit | port1.0.5 | | | | | | | | | | | | |
| Edit | port1.0.6 | | | | | | | | | | | | |
| Edit | port1.0.7 | | | | | | | | | | | | |
| Edit | port1.0.8 | | | | | | | | | | | | |
| Edit | port1.0.9 | | | | | | | | | | | | |
| Edit | port1.0.10 | | | | | | | | | | | | |
| Edit | port1.0.11 | | | | | | | | | | | | |
| Edit | port1.0.12 | | | | | | | | | | | | |

Figure 87. LLDP TLV Page

- Click **Edit** next to the port that you want to modify.

The Modify LLDP TLV page is displayed. See Figure 88 on page 226.

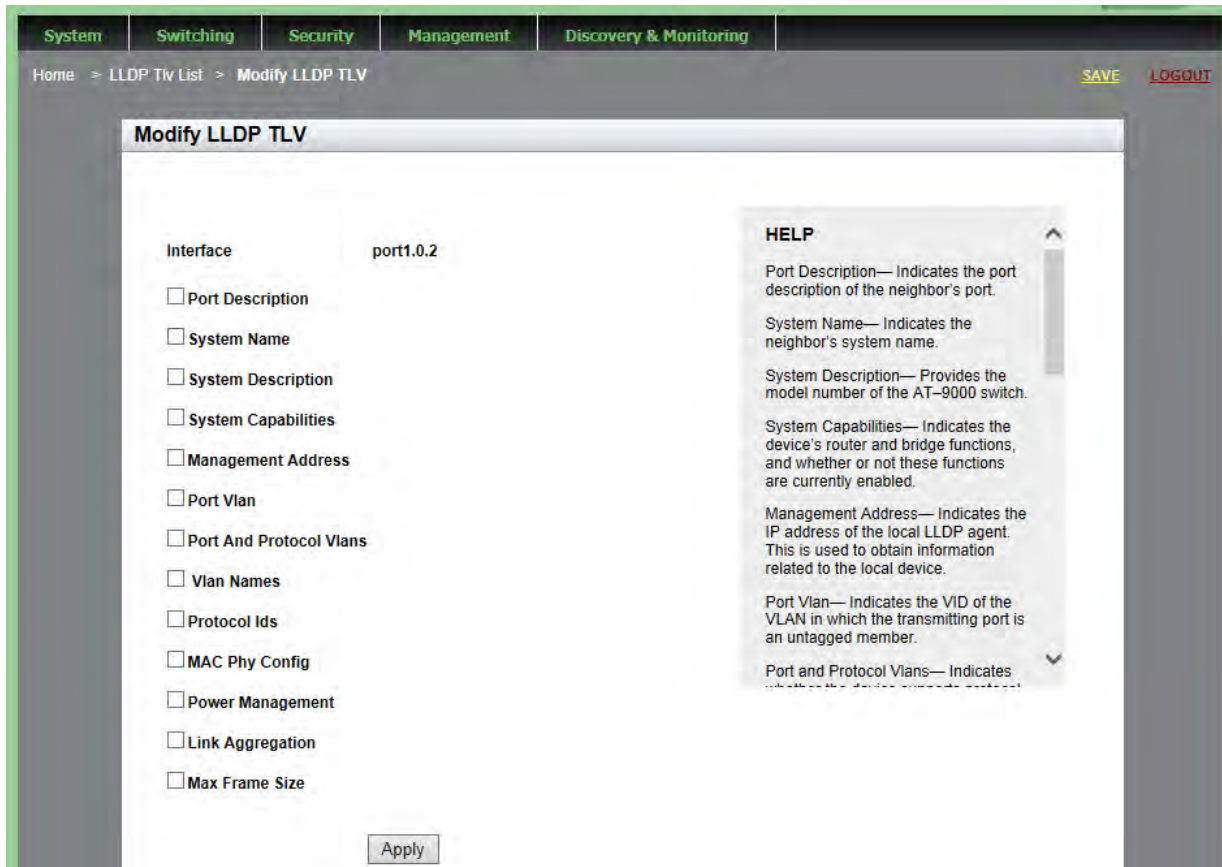


Figure 88. Modify LLDP TLV Page

6. Change the following fields as needed by clicking the box next to the field:
 - Port Description**— Port description of the neighbor's port.
 - System Name**— Neighbor's system name.
 - System Description**— Model number of the AT-9000 switch.
 - System Capabilities**— Device's router and bridge functions, and whether or not these functions are currently enabled.
 - Management Address**— IP address of the local LLDP agent. This is used to obtain information related to the local device.
 - Port Vlan**— VID of the VLAN in which the transmitting port is an untagged member.
 - Port and Protocol Vlans**— Whether the device supports protocol VLANs, and if it does, the protocol VLAN identifiers. This field is not supported on the AT-9000 switches.
 - Vlan Names**— Lists the names of the VLANs in which the transmitting port is either an untagged or tagged member.

- ❑ **Protocol Ids**— List of protocols that are accessible through the port, for instance:
 - 9000 (Loopback)
 - 0026424203000000 (STP, RSTP, or MSTP)
 - 888e01 (802.1x)
 - AAAA03 (EPSR)
 - 88090101 (LACP)
 - 00540000e302 (Loop protection)
 - 0800 (IPv4)
 - 0806 (ARP)
 - 86dd (IPv6)
 - ❑ **MAC Phy Config**— Speed and duplex mode of the port and whether the port was configured with Auto-Negotiation.
 - ❑ **Link Aggregation**— Whether the port is capable of link aggregation and, if so, whether it is currently a member of an aggregator.
 - ❑ **Max Frame Size**— Sends the maximum supported frame size of the port. This field is not adjustable on the switch.
7. Click **Apply**.
 8. Click **SAVE**.

Enabling LLDP-MED TLV

To enable LLDP-MED TLV, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP** and then hover over **TLV**.

The LLDP TLV tab is displayed. See Figure 86 on page 225.

3. From the LLDP TLV tab, select **TLV-MED** on the right

The LLDP MED TLV page is displayed. See Figure 89.

| | Interface | Capabilities | Network-policy | Location | Inventory-management |
|----------------------|------------|--------------|----------------|----------|----------------------|
| Edit | port1.0.1 | | | | |
| Edit | port1.0.2 | ✓ | ✓ | ✓ | ✓ |
| Edit | port1.0.3 | | | | |
| Edit | port1.0.4 | | | | |
| Edit | port1.0.5 | | | | |
| Edit | port1.0.6 | | | | |
| Edit | port1.0.7 | | | | |
| Edit | port1.0.8 | | | | |
| Edit | port1.0.9 | | | | |
| Edit | port1.0.10 | | | | |
| Edit | port1.0.11 | | | | |
| Edit | port1.0.12 | | | | |

Figure 89. LLDP MED TLV Page

The following fields are displayed:

- Interface**— Port number.
- Capabilities**— Device's router and bridge functions, and whether or not these functions are currently enabled.
- Network-policy**— Network policy information configured on the port for connected media endpoint devices. The switch supports Application Type 1: Voice, including the following network policy for connected voice devices to use for voice data:
 - Voice VLAN ID
 - Voice VLAN Class of Service (CoS) priority

- Voice VLAN Diffserv Code Point (DSCP)
 - Location**— Location information configured for the port, in one or more of the following formats:
 - Civic location
 - Coordinate location
 - Emergency Location Identification Number (ELIN)
 - Inventory-management**— Current hardware platform and the software version, identical on every port on the switch:
 - Hardware Revision
 - Firmware Revision
 - Software Revision
 - Serial Number
 - Manufacturer Name
 - Model Name
 - Asset ID
4. Click **Edit** next to the port that you want to modify.

The Modify LLDP Med TLV page is displayed. See Figure 90.

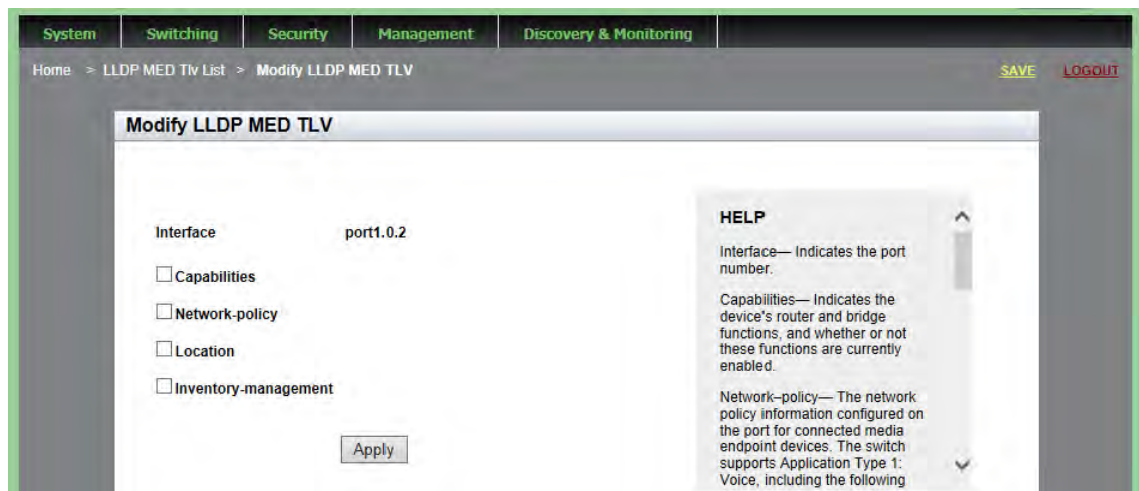


Figure 90. Modify LLDP Med TLV Page

5. Change the following fields, as needed, by clicking the box next to the field. The fields are described in detail in Step 3.
- Capabilities**— Capabilities TLV.

- Network-policy**— Network policy TLV.
 - Location**— Location identification TLV.
 - Inventory-management**— Inventory management TLV.
6. Click **Apply**.
 7. Click **SAVE**.

- ❑ **System Capabilities**— Capabilities that are supported and enabled on the neighbor. The System Capabilities codes are:
 - O = Other
 - P = Repeater
 - B = Bridge
 - W = Wireless Access Point
 - R = Router
 - T = Telephone
 - C= Cable Device
 - S = Station only

- ❑ **Med Device class and Power Source code**— The MED device Classes I through III are supported. Power Source code indicates the current power source which is either the Primary Power Source or the Backup Power Source. The codes are:
 - C1 = Class I
 - C2 = Class II
 - C3 = Class III
 - N = Network
 - L = Local
 - PSE = PoE
 - prim = Primary
 - UN = Unknown
 - Ba = Backup

Displaying LLDP Neighbor Detail

To display LLDP Neighbor detailed information, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**, move the cursor to the right, and then select **Neighbors**.

The LLDP Neighbors Information page is displayed. See Figure 91 on page 231.

- From the LLDP Neighbors Information page, click **Details** next to the port whose LLDP Neighbor detailed information you want to view.

The LLDP Neighbor Detail page is displayed. See Figure 92.

| LLDP Neighbor Detail | | | |
|--|------------------|---------------------------------|---------------------|
| Port Id | 7 | Neighbor Power Via MDI | Supported / Enabled |
| Neighbor Chassis Id | eccd.6d9e.33f5 | Neighbor Link Aggregation | [not advertised] |
| Neighbor Port Id Type | Interface alias | Neighbor Max Frame Size | 0 |
| Neighbor Port Id | port1.0.3 | Neighbor LLDP Med Device Type | [not advertised] |
| Neighbor TTL | 120 | Neighbor LLDP Med Capabilities | [not advertised] |
| Neighbor System Name | | Neighbor Network Policies | [not advertised] |
| Neighbor System Description | | Neighbor Location Identifier | |
| Neighbor System Capabilities Supported | [not advertised] | Neighbor Extended Power Via MDI | [not advertised] |
| Neighbor System Capabilities Enabled | [not advertised] | Neighbor Power Source | Unknown |
| Neighbor Management Address | [not advertised] | Neighbor Power Priority | Unknown |
| Neighbor PVID | [not advertised] | Neighbor Power Value | 0(0.0 Watts) |
| Neighbor Port Vlan Supported | [not advertised] | Neighbor Hardware Revision | [not advertised] |
| Neighbor Port Vlan Enabled | [not advertised] | Neighbor Firmware Revision | [not advertised] |
| Neighbor VIDs | [not advertised] | Neighbor Software Revision | [not advertised] |
| Neighbor VNames | [not advertised] | Neighbor Serial Number | [not advertised] |
| Neighbor Protocol Ids | | Neighbor Mfg Name | [not advertised] |
| Neighbor MAC Phy Auto Neg | | Neighbor Model Name | [not advertised] |
| Neighbor Advertised Capability | | Neighbor Asset Id | [not advertised] |
| Neighbor Operational Mau Type | Unknown | | |

Figure 92. LLDP Neighbor Detail Page

The following fields are displayed:

- Port Id**— Local port ID.
- Neighbor Chassis Id**— Chassis ID that uniquely identifies the neighbor.
- Neighbor Port Id Type**— Port ID type of the neighbor.
- Neighbor Port Id**— Port ID of the neighbor.

- ❑ **Neighbor TTL**— Number of seconds that the information advertised by the neighbor remains valid.
- ❑ **Neighbor System Name**— Neighbor's system name.
- ❑ **Neighbor System Description**— Description of the neighbor switch, such as the product name.
- ❑ **Neighbor System Capabilities Supported**— Neighbor device's functions supported by the switch.
- ❑ **Neighbor System Capabilities Enabled**— Neighbor device's functions and whether or not these functions are currently enabled.
- ❑ **Neighbor Management Address**— IP address of the neighbor.
- ❑ **Neighbor PVID**— VLAN ID of the neighbor port.
- ❑ **Neighbor Port Vlan Supported**— Protocol VLANs supported by the neighbor switch.
- ❑ **Neighbor Port Vlan Enabled**— Protocol VLANs enabled on the neighbor switch.
- ❑ **Neighbor VIDs**— VLAN IDs of the protocol VLANs supported on the neighbor switch.
- ❑ **Neighbor VNames**— Names of the port-based and tagged VLANs in which the neighbor port is a member.
- ❑ **Neighbor Protocol Ids**— List of protocols that are accessible through the neighbor's port.
- ❑ **Neighbor MAC Phy Auto**— Speed and duplex mode of the neighbor port and whether the port was configured with Auto-Negotiation.
- ❑ **Neighbor Advertised Capability**— Auto-negotiation neighbor port capabilities, including 1000BaseTDF, 100BaseTXFD, 100BaseTX, 10BaseTFD, 10BaseT.
- ❑ **Neighbor Operational Mau Type**— Operational Medium Attachment Unit (MAU) type is the attached device's medium speed, such as twisted pair, fiber, or link speed.
- ❑ **Neighbor Power Via MDI**— Power via MDI capabilities of the neighbor port.
- ❑ **Neighbor Link Aggregation**— Neighbor link aggregation status.
- ❑ **Neighbor Max Frame Size**— Maximum frame size the neighbor port can forward.
- ❑ **Neighbor LLDP Med Device Type**— LLDP-MED device types are Class I, Class II, Class III, Network Connectivity, Local, and Unknown.
- ❑ **Neighbor LLDP Med Capabilities**— LLDP-MED TLVs that are supported and enabled on the neighbor switch, and the device type.
- ❑ **Neighbor Network Policies**— Network policy information

configured on the port for connected media endpoint devices. The switch supports Application Type 1: Voice, including the following network policy for connected voice devices to use for voice data:

- Voice VLAN ID
 - Voice VLAN Class of Service (CoS) priority
 - Voice VLAN Diffserv Code Point (DSCP)
- Neighbor Location Identifier**— ID number for an LLDP-MED civic location entry on the neighbor switch.
 - Neighbor Extended Power Via MDI**— Extended power via MDI capabilities of the neighbor port.
 - Neighbor Power Source**— Current neighbor power source, either Primary Power Source or Backup Power Source.
 - Neighbor Power Priority**— Power priority configured on the neighbor port.
 - Neighbor Power Value**— In TLVs transmitted by a Power Sourcing Equipment (PSE), such as this switch, this advertises the power that the port can supply over a maximum length cable based on its current configuration (that is, it takes into account power losses over the cable). In TLVs received from Powered Device (PD) neighbors, the power value is the power the neighbor requests.
 - Neighbor Hardware Revision**— Hardware revision number of the neighbor chassis.
 - Neighbor Firmware Revision**— Revision number of the bootloader on the neighbor chassis.
 - Neighbor Software Revision**— Revision number of the management software on the neighbor chassis.
 - Neighbor Serial Number**— Serial number of the neighbor device.
 - Neighbor Mfg Name**— Name of the company that manufactured the neighbor device.
 - Neighbor Model Name**— Model name of the neighbor.
 - Neighbor Asset Id**— Asset ID of the neighbor.

Displaying LLDP Statistics

To display LLDP Statistical information, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

3. From the LLDP tab, move the cursor to the right and select **Statistics**.

The LLDP Statistics page is displayed with the Port Statistics tab selected automatically. See Figure 93.

| Interface | Out Frames | In Frames | In Frames Errored | In Frames Dropped | Unrecognized TLVs | Discarded | New Entries | Deleted Entries | Dropped Entries | Ageout Entries |
|------------|------------|-----------|-------------------|-------------------|-------------------|-----------|-------------|-----------------|-----------------|----------------|
| port1.0.1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| port1.0.12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Figure 93. LLDP Statistics Page with Port Statistics Tab

The following fields are displayed:

- Interface**— Port number.
- Out Frames**— Number of LLDPDU frames transmitted.
- In Frames**— Number of LLDPDU frames received.
- In Frames Errored**— Number of invalid LLDPDU frames received.
- In Frames Dropped**— Number of LLDPDU frames received and discarded.
- Unrecognized TLVs**— Number of LLDP TLVs received that were unrecognized, but the TLV types were in the range of reserved TLV types.
- Discarded**— Number of discarded TLVs.

- ❑ **New Entries**— Number of times the information advertised by neighbors has been inserted into the neighbor table.
- ❑ **Deleted Entries**— Number of times the information advertised by neighbors has been removed from the neighbor table.
- ❑ **Dropped Entries**— Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.
- ❑ **Ageout Entries**— Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.

4. Select the **Summary** tab.

The LLDP Statistics Summary page is displayed. See Figure 94.

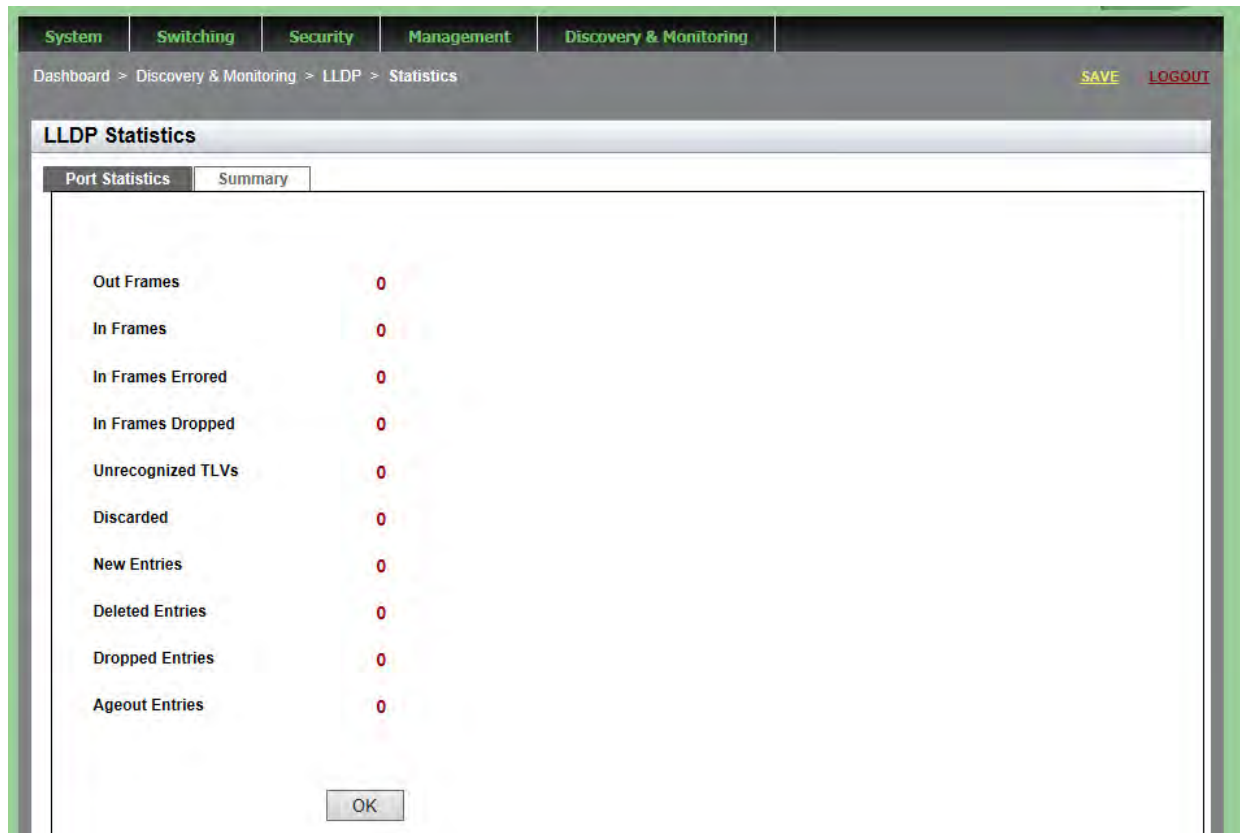


Figure 94. LLDP Statistics Page with Summary Tab

The fields are described in Step 2. These fields list the statistics for all of the ports.

5. Click **OK** to return to the LLDP Statistics Page with the Port Statistics Tab selected.

Displaying LLDP Locations

To display the LLDP Civic, Coordinate, and ELIN locations, use the following procedures:

- ❑ “Displaying Civic Locations”
- ❑ “Displaying Coordinate Locations” on page 239
- ❑ “Displaying ELIN Locations” on page 240

For information about creating LLDP locations, see “Setting LLDP Locations” on page 211.

Displaying Civic Locations

To display a Civic Location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, hover over **Locations**.

The Locations tab is displayed. See Figure 74 on page 212.

4. From the Locations tab, move the cursor to the right and select **Civic**.

The LLDP Civic Location page is displayed. See Figure 75 on page 212.

The following fields are displayed:

- ❑ **ID**
- ❑ **Country**
- ❑ **State**
- ❑ **County**
- ❑ **City**
- ❑ **Division**
- ❑ **Neighborhood**
- ❑ **Street Group**
- ❑ **Leading Street Direction**
- ❑ **Trailing Street Suffix**
- ❑ **Street Suffix**

- House Number**
- House Number Suffix**
- Landmark**
- Additional Information**
- Name**
- Postal Code**
- Building**
- Unit**
- Floor**
- Room**
- Place Type**
- Postal Community Name**
- Post Office Box**
- Additional Code**
- Seat**
- Primary Road Name**
- Road Selection**
- Branch Road Name**
- Sub Branch Road Name**
- Street Name Pre Modifier**
- Street Name Post Modifier**

Displaying Coordinate Locations

To display a Coordinate Location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, hover over **Locations**.

The Locations tab is displayed. See Figure 74 on page 212.

4. From the Locations tab, move the cursor to the right and select **Coordinates**.

The LLDP Coordinate Location page is displayed. See Figure 77 on page 215.

The following fields are displayed:

- ❑ **ID**— LLDP Coordinate Location ID.
- ❑ **Latitude**— Latitude value in decimal degrees.
- ❑ **Latitude Resolution**— Latitude resolution as the number of valid bits.
- ❑ **Longitude**— Longitude value in decimal degrees.
- ❑ **Longitude Resolution**— Longitude resolution as the number of valid bits.
- ❑ **Altitude**— Altitude in meters or floors.
- ❑ **Altitude Resolution**— Altitude resolution as the number of valid bits.
- ❑ **Datum**— Geodetic system (or datum) of the coordinates:
 - nad83-mllw Mean lower low water datum 1983
 - nad83-navd North American vertical datum 1983
 - wgs84 World Geodetic System 1984

Displaying ELIN Locations

To display an LLDP ELIN location, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, hover over **Locations**.

The Locations tab is displayed. See Figure 74 on page 212.

4. From the Locations tab, move the cursor to the right and select **ELIN**.

The LLDP ELIN Location page is displayed. See Figure 79 on page 217.

The following fields are displayed:

- ❑ **ID**— ID number for an LLDP-MED coordinate location entry on the switch.
- ❑ **ELIN LOCATION**— ELIN of 10 to 25 digits.

Displaying LLDP and LLDP-MED Settings

To display the LLDP and LLDP-MED settings, use the following procedures:

- ❑ “Displaying the Basic LLDP Configuration”
- ❑ “Displaying LLDP Port Assignments” on page 242
- ❑ “Displaying Port Locations” on page 243
- ❑ “Displaying LLDP TLV” on page 243
- ❑ “Displaying LLDP-MED TLV” on page 245

For information about configuring LLDP and LLDP-MED, see “Configuring LLDP and LLDP-MED” on page 219

Displaying the Basic LLDP Configuration

To display the basic LLDP configuration, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears to the right.

3. From the LLDP tab, select **Basic Configuration**.

The LLDP Configuration page is displayed. See Figure 81 on page 219.

The following fields are displayed:

- ❑ **Status**— Whether LLDP is enabled or disabled on the switch.
- ❑ **Timer**— Transmit interval.
- ❑ **Fast Start Count**— Fast-start count for LLDP-MED. The fast-start count determines how many fast start advertisements LLDP sends from a port when it begins sending LLDP-MED advertisements from a port, for instance when it detects a new LLDP-MED capable device.
- ❑ **Holdtime Multiplier**— Holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) the switch advertises to the neighbors.
- ❑ **Non Strict Med TLV Order Check**— Indicates whether the switch accepts LLDP-MED advertisements when the TLVs are not in the standard order, as specified in ANSI/TIA-1057.
- ❑ **Notification Interval**— Notification interval. This is the minimum

interval between LLDP SNMP notifications (traps).

- ❑ **Reinit**— Reinitialization delay. This is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized.
- ❑ **Tx Delay**— Transmission delay. This is the minimum time interval between transmissions of advertisements due to changes in LLDP local information.
- ❑ **Total Neighbors**— Number of LLDP neighbors the switch has discovered on all its ports.
- ❑ **Neighbors Last Update**— Time since the LLDP neighbor table was last updated.

Displaying LLDP Port Assignments

To display LLDP port assignments, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**, move the cursor to the right, and then select **Port Configurations**.

The LLDP Port Config page is displayed. See Figure 82 on page 221.

The following fields are displayed:

- ❑ **Interface**— Port ID.
- ❑ **Notification**— Indicates whether the switch sends LLDP-MED topology change notifications when devices are connected to, or disconnected from, the specified ports.
- ❑ **Adv. Transmit**— Indicates whether the ports send LLDP advertisements. Ports configured to transmit LLDP advertisements send the mandatory TLVs and any optional LLDP TLVs they have been configured to send.
- ❑ **Adv. Receive**— Indicates whether the ports accept LLDP advertisements. Ports configured to receive LLDP advertisements accept all advertisements from their neighbors.

- Med Notification**— Indicates whether the switch sends LLDP-MED topology change notifications when devices are connected to, or disconnected from, the specified ports.

Displaying Port Locations

To display the LLDP port locations, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, move the cursor to the right and select **Port Locations**.

The LLDP Port Location page is displayed. See Figure 84 on page 223.

The following fields are displayed.

- Interface**— Port number.
- Civic Location ID**— Civic location information for the port.
- Coordinate Location ID**— LLDP-MED coordinate information for the port.
- ELIN Location ID**— ELIN location information for the port.

Displaying LLDP TLV

To display the LLDP TLV settings, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab is displayed.

3. From the LLDP tab, hover over **TLV**.

The LLDP TLV tab is displayed in Figure 86 on page 225.

4. From the LLDP TLV tab, select **TLV** again.

The LLDP TLV page is displayed. See Figure 87 on page 225.

The following fields are displayed:

- Interface**— Port number.
- Port Description**— Port description of the neighbor's port.
- System Name**— Neighbor's system name.
- System Description**— Model number of the AT-9000 switch.
- System Capabilities**— Device's router and bridge functions, and whether or not these functions are currently enabled.
- Management Address**— IP address of the local LLDP agent. This is used to obtain information related to the local device.
- Port Vlan**— VID of the VLAN in which the transmitting port is an untagged member.
- Port and Protocol Vlans**— Whether the device supports protocol VLANs and, if it does, the protocol VLAN identifiers. This field is not supported on the AT-9000 switches.
- Vlan Names**— Names of the VLANs in which the transmitting port is either an untagged or tagged member.
- Protocol Ids**— Protocols that are accessible through the port, for instance:
 - 9000 (Loopback)
 - 0026424203000000 (STP, RSTP, or MSTP)
 - 888e01 (802.1x)
 - AAAA03 (EPSR)
 - 88090101 (LACP)
 - 00540000e302 (Loop protection)
 - 0800 (IPv4)
 - 0806 (ARP)
 - 86dd (IPv6)
- MAC Phy Config**— Speed and duplex mode of the port and whether the port was configured with Auto-Negotiation.
- Link Aggregation**— Whether the port is capable of link aggregation, and if so, whether it is currently a member of an aggregator.
- Max Frame Size**— Sends the maximum supported frame size of the port. This field is not adjustable on the switch.

Displaying LLDP-MED TLV

To display LLDP-MED TLV settings, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP** and then hover over **TLV**.

The LLDP TLV tab is displayed. See Figure 86 on page 225.

3. From the LLDP TLV tab, move the cursor to the right and select **TLV-MED**.

The LLDP Med TLV page is displayed. See Figure 89 on page 228.

The following fields are displayed:

- Interface**— Port number.
- Capabilities**— Device's router and bridge functions, and whether or not these functions are currently enabled.
- Network-policy**— Network policy information configured on the port for connected media endpoint devices. The switch supports Application Type 1: Voice, including the following network policy for connected voice devices to use for voice data:
 - Voice VLAN ID
 - Voice VLAN Class of Service (CoS) priority
 - Voice VLAN Diffserv Code Point (DSCP)
- Location**— Location information configured for the port, in one or more of the following formats:
 - Civic location
 - Coordinate location
 - Emergency Location Identification Number (ELIN)

- ❑ **Inventory-management**— Current hardware platform and the software version, identical on every port on the switch:
 - Hardware Revision
 - Firmware Revision
 - Software Revision
 - Serial Number
 - Manufacturer Name
 - Model Name
 - Asset ID

Disabling LLDP on the Switch

To disable the LLDP feature on a switch, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab, hover over **LLDP**.

The LLDP tab appears to the right.

3. From the LLDP tab, select **Basic Configuration**.

The LLDP Configuration page is displayed. See Figure 81 on page 219.

4. Use the pull-down menu next to the **Status** field to select **Disabled**.

5. Click **Apply**.

6. Click **SAVE**.

Chapter 20

Setting sFlow

This chapter provides a brief description of the sFlow feature and explains how to enable this feature on the switch and on a port.

See the following sections:

- ❑ “Overview” on page 250
- ❑ “Configuring sFlow on a Port” on page 252
- ❑ “Specifying an sFlow Collector” on page 254
- ❑ “Enabling sFlow on the Switch” on page 256
- ❑ “Displaying the sFlow Settings” on page 257

For more information about the sFlow feature, see the following chapters in the *AlliedWare Plus Management Software Command Line Interface User's Guide*:

- ❑ sFlow Agent
- ❑ sFlow Agent Commands

Overview

The sFlow agent allows the switch to gather data about the traffic on the ports and to send the data to sFlow collectors on your network for analysis. You can use the information to monitor the performance of your network or identify traffic bottlenecks.

The sFlow agent can gather two types of information about the traffic on the ports of the switch:

- Ingress packet samples
- Packet counters

Ingress Packet Samples

The sFlow agent can capture ingress packets on ports and send copies of the packets to sFlow collectors on your network for analysis. Depending on the capabilities of the collectors, packets can be scrutinized for source and destination MAC or IP addresses, protocol type, length, and so forth.

Packet sampling is activated by specifying sampling rates on the ports. This value defines the number of ingress packets from which the agent samples one packet. For example, a sampling rate of 1000 on a port prompts the agent to send one packet from every 1000 ingress packets to the designated sFlow collector. Different ports can have different rates.

Packet Counters

The agent can also gather and send data to a collector about overall information regarding the status and performance of the ports, such as speeds and status, and the statistics from the packet counters. The counters contain the number and types of ingress and egress packets handled by the ports since the switch or the counters were last reset. The agent can gather and send the following port status and counter information to a collector on your network:

- Port number
- Port type
- Speed
- Direction
- Status
- Number of ingress and egress octets
- Number of ingress and egress unicast packets
- Number of ingress and egress multicast packets
- Number of ingress and egress broadcast packets
- Number of ingress and egress discarded packets
- Number of ingress and egress packets with errors
- Number of ingress packets with unknown protocols

To configure the agent to forward these port statistics to the collectors, you have to specify polling rates, which define the maximum amount of time permitted between successive queries of the counters of a port by the agent.

Different ports can have different polling rates. Ports to which critical network devices are connected can be assigned low polling rates, so that the information on the collector is kept up-to-date. Ports connected to less critical devices can be assigned higher polling rates.

To increase its efficiency, the agent can send port status and counter information before the polling interval of a port times out. For example, if you define a polling interval of five minutes for a port, the agent, depending on its internal dynamics, may send the information to the collector before five minutes have actually elapsed.

sFlow Collectors

The sFlow agent on the switch can send port performance data to up to an sFlow collector on your network. The performance data from each port can be sent to one collector.

Guidelines

Here are the guidelines for the sFlow agent:

- ❑ The sFlow agent can send port performance data to up to four sFlow collectors on your network.
- ❑ The switch must have a management IP address. For instructions, refer to Chapter 18, "Setting IPv4 and IPv6 Management" on page 197.
- ❑ The sFlow collectors must be members of the same subnet as the management IP address of the switch, or must have access to it through routers or other Layer 3 devices.
- ❑ If the sFlow collectors are not a member of the same subnet as the management IP address of the switch, the switch must have a default gateway that specifies the first hop to reaching the collectors' subnet. For instructions, refer to Chapter 18, "Setting IPv4 and IPv6 Management" on page 197.
- ❑ The sFlow feature is not dependent on SNMP. You do not have to enable or configure SNMP on the switch to use the sFlow feature. In addition, you cannot use sFlow collectors to configure or manage SNMP.

Configuring sFlow on a Port

To configure the sFlow feature on a port, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab drop-down menu, select **sFlow**.

The sFlow page is displayed with the Port Configurations tab selected. See Figure 98 on page 256.

3. Click Edit next to the port that you want to modify.

The sFlow Port Modify page is displayed. See Figure 95.

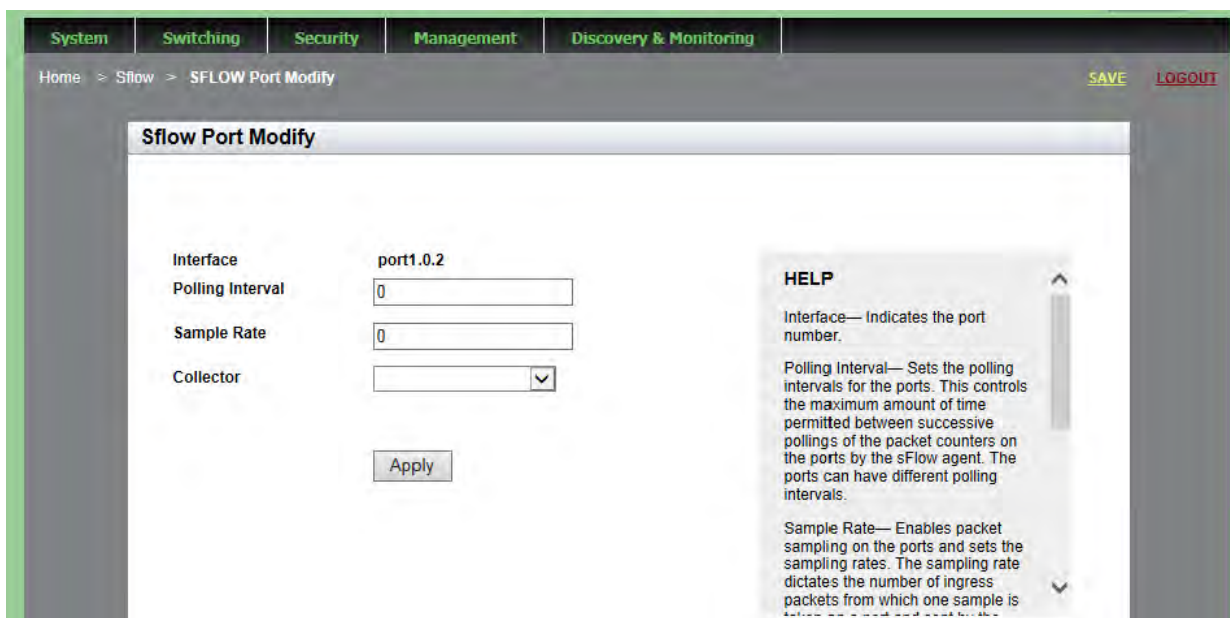


Figure 95. sFlow Port Modify Page

4. Change the following fields as needed:
 - Interface**— Indicates the port number.
 - Polling Interval**— Sets the polling intervals for the ports. This controls the maximum amount of time permitted between successive pollings of the packet counters on the ports by the sFlow agent. The ports can have different polling intervals.
 - Sample Rate**— Enables packet sampling on the ports and sets the sampling rates. The sampling rate dictates the number of ingress packets from which one sample is taken on a port and sent by the agent to the sFlow collector. For example, a sample rate of 700 on a port means that one sample packet is taken for every 700 ingress packets. The ports can have different sampling rates.
 - Collector**— Select the Collector, which is the number of sFlow collectors that have been defined on the switch by entering their IP addresses in the agent. The agent can contain up to four IP addresses of sFlow collectors. Enter the IP addresses in the “Specifying an sFlow Collector” on page 254.
5. Click **Apply**.
6. Click **SAVE**.

Specifying an sFlow Collector

Use this procedure to specify the IP addresses and the UDP ports of the sFlow collectors on your network. The packet sampling data and the packet counters are sent by the switch to the collectors specified. You can specify up to four collectors, but you can add only one address at a time with this procedure.

To select the Collectors tab from the sFlow page, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab drop-down menu, select **sFlow**.

The sFlow page is displayed with the Port Configurations tab selected. See Figure 98 on page 256.

3. From the sFlow page, select the **Collectors** tab.

The sFlow page is displayed with the Collectors Tab selected. See Figure 96.

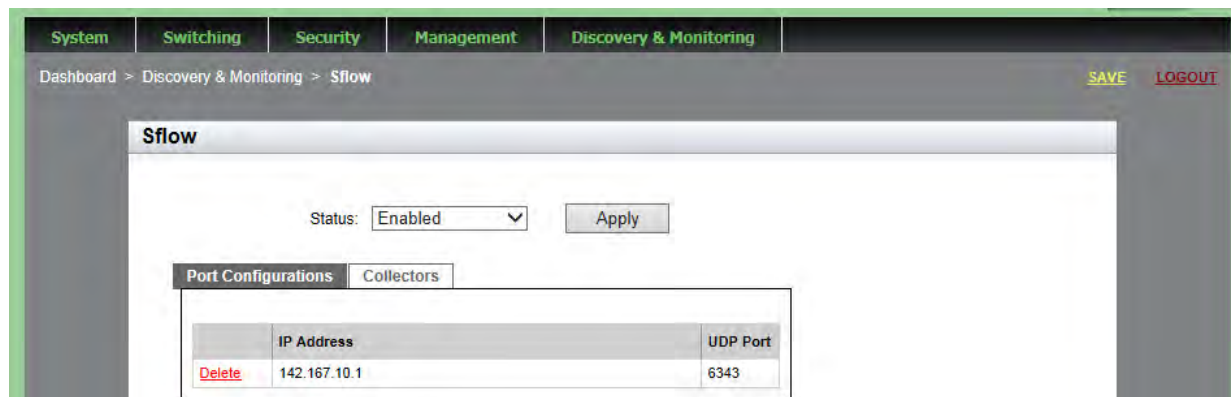


Figure 96. sFlow Page with Collectors Tab

4. Click **Add**.

The sFlow Collector page is displayed. See Figure 97 on page 255.

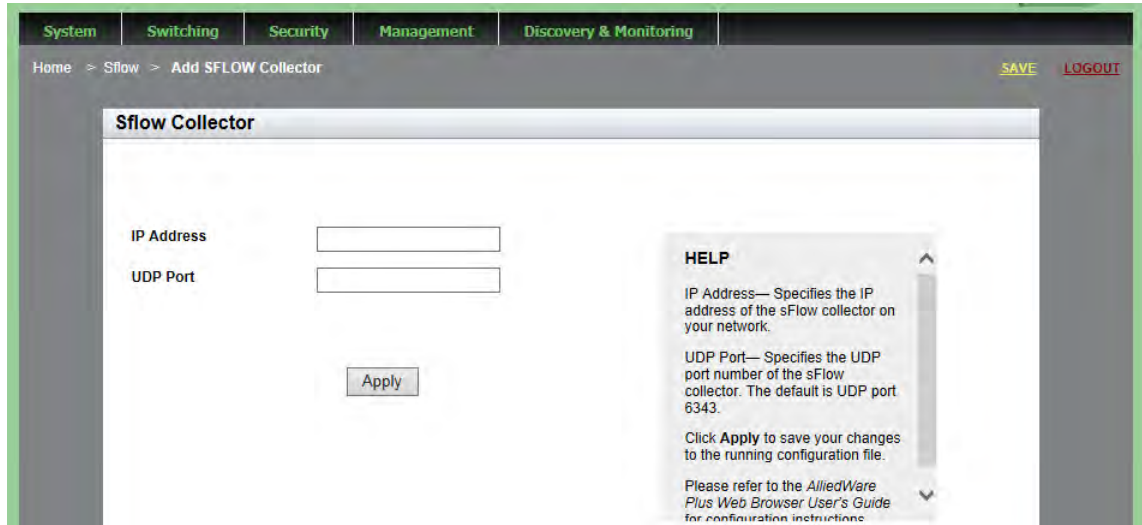


Figure 97. sFlow Collector Page

5. Define or change the following fields as needed:
 - ❑ **IP Address**— IPv4 address of the sFlow collector on your network. Enter the IPv4 address in the following format:
 xxx.xxx.xxx.xxx
 where xxx is a number from 0 to 255. There are four groups of numbers that are separated by periods.
 - ❑ **UDP Port**— UDP port number of the sFlow collector. The default is UDP port 6343.
6. Click **Apply**.
7. Click **SAVE**.

Enabling sFlow on the Switch

To enable the sFlow feature on a switch, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 73 on page 211.

2. From the **Discovery & Monitoring** tab drop-down menu, select **sFlow**.

The sFlow page is displayed with the Port Configurations tab selected. See Figure 98.

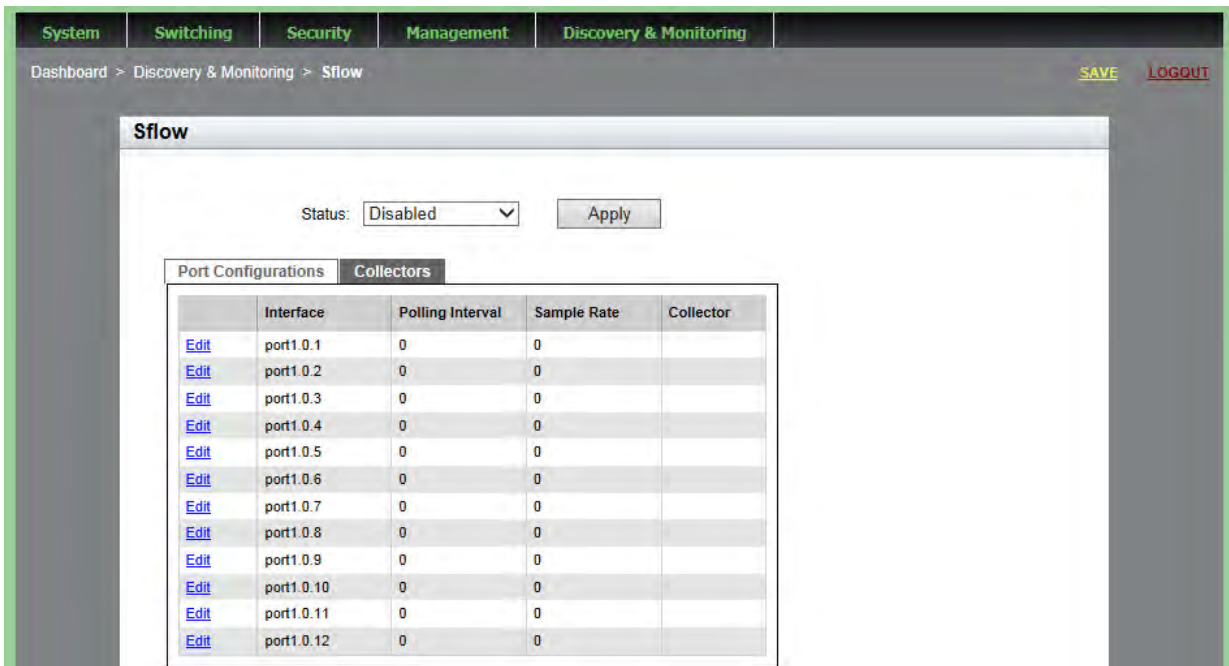


Figure 98. sFlow Page with Port Configurations Tab

3. Use the pull-down menu next to the **Status** field to select **Enabled**.
4. Click **Apply**.
5. Click **SAVE**.

Displaying the sFlow Settings

To display the sFlow settings, do the following:

1. Hover the cursor over the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 98 on page 256.

2. From the **Discovery & Monitoring** tab drop-down menu, select **sFlow**.

The sFlow page is displayed with the Port Configurations tab selected. See Figure 98 on page 256.

