Atop Technologies, Inc.

Rackmount 28-Gigabit Ports IEC61850-3 L2/L3 PoE Managed Switch

User Manual
V1.0

Apr. 8st, 2026

Series covered by this manual:
RHG9728/9828 Series

This PDF Document contains internal hyperlinks for ease of navigation.
For example, click on any item listed in the **Table of Contents** to go to that page.

Published by:

Atop Technologies, Inc.

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.

Tel: +886-3-550-8137
Fax: +886-3-550-8131
www.atoponline.com

Important Announcement

The information contained in this document is the property of Atop Technologies, Inc., and is supplied for the sole purpose of operation and maintenance of Atop Technologies, Inc., products.
No part of this publication is to be used for any other purposes, and it is not to be reproduced, copied, disclosed, transmitted, stored in a retrieval system, or translated into any human or computer language, in any form, by any means, in whole or in part, without the prior explicit written consent of Atop Technologies, Inc.,
Offenders will be held liable for damages and prosecution.
All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Disclaimer

We have checked the contents of this manual for agreement with the hardware and the software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections will be included in subsequent editions.
Suggestions for improvement are welcome. All other product's names referenced herein are registered trademarks of their respective companies.

Preface

This manual contains some advanced network management knowledge, instructions, examples, guidelines, and general theories. The contents are designed to help users manage the switch and use its software, a background in general theory is a must, when reading it. Please refer to the Glossary for technical terms and abbreviations.

Who Should Use This User Manual

This manual is to be used by qualified network personnel or support technicians who are familiar with network operations, and might be useful for system programmers or network planners as well. This manual also provides helpful and handy information for first time users. For any related problems, please contact your local distributor. If they are unable to assist you, please redirect your inquiries to www.atoponline.com .

Warranty Period

Atop technology provides a limited 5-year warranty for managed Ethernet switches.

Documentation Control

Author:	PC Hsu
Revision:	1.0
Revision History:	First version
Creation Date:	1 March 2026
Last Revision Date:	8 April 2026
Product Reference:	Rackmount L2/L3 PoE Managed Switch – RHG9728, RHG9828
Document Status:	Released

Table of Contents

1 Introduction 14
1.1 Introduction to Industrial Managed Switch 14
1.2 Software Features 16
1.3 Introduction to the Document 16
2 Configuring with a Web Browser 17
2.1 System 18
2.1.1 Information 18
2.1.2 IP 19
2.1.3 SNMP 23
2.1.4 NTP 31
2.1.5 Time 32
2.1.6 Log 34
2.1.7 Alert 35
2.1.8 SMTP Setting 36
2.1.9 AgentClient 38
2.2 Ports 38
2.3 ERPS 39
2.4 Media Redundancy Protocol 43
2.5 DHCPv4 43
2.5.1 Snooping 44
2.5.2 Relay 45
2.6 Security 46
2.6.1 Switch 47
2.6.2 Network 59
2.6.3 AAA 88
2.7 Aggregation 91
2.7.1 Common 91
2.7.2 Groups 92
2.7.3 LACP 93
2.8 Spanning Tree 94
2.8.1 Bridge Settings 94
2.8.2 MSTI Mapping 96
2.8.3 MSTI Priorities 98
2.8.4 CIST Ports 98
2.8.5 MSTI Ports 101
2.9 IPMC 102
2.9.1 IGMP Snooping 102
2.9.2 MLD Snooping 105
2.10 LLDP 108
2.10.1 LLDP 108
2.11 MAC Table 110
2.12 VLANs 111
2.12.1 Configuration 112
2.12.2 SVL 116
2.13 VCL 117
2.13.1 MAC-based VLAN 117
2.13.2 Protocol-based VLAN 117
2.13.3 IP Subnet-based VLAN 120
2.14 Voice VLAN 120
2.15 QoS 121
2.15.1 Port Classification 121

2.15.2 Port Policing 123
2.15.3 Queue Policing 124
2.15.4 Port Scheduler 125
2.15.5 Port Shaping 127
2.15.6 Port Tag Remarking 129
2.15.7 Port DSCP 130
2.15.8 DSCP-Based QoS 131
2.15.9 DSCP Translation 133
2.15.10 DSCP Classification 134
2.15.11 QoS Control List 134
2.15.12 Storm Policing 138
2.16 Mirroring 139
2.17 PTP 141
2.18 GVRP 144
2.18.1 Global config 144
2.18.2 Port config 145
2.19 sFlow 146
2.20 DDMI 147
2.21 UDLD 147
2.22 SD Backup 149
2.23 Modbus Setting 150
2.22 Modbus Memory Map 157
2.23 RedBox 163
3 Monitor 182
3.1 System 182
3.1.1 Information 182
3.1.2 CPU Load 183
3.1.3 IP Status 184
3.1.4 IPv4 Routing Info. Base 185
3.1.5 IPv6 Routing Info. Base 186
3.1.6 Log 186
3.1.7 Detailed Log 187
3.1.8 Power Status 188
3.1.9 Digital Input 188
3.2 Ports 189
3.2.1 State 189
3.2.2 Traffic Overview 189
3.2.3 QoS Statistics 190
3.2.4 QCL Status 191
3.2.5 Detailed Statistics 192
3.2.6 Name Map 193
3.3 ERPS 193
3.4 DHCPv4 196
3.4.1 Snooping Table 196
3.4.2 Relay Statistics 196
3.4.3 Detailed Statistics 197
3.5 Security 199
3.5.1 Network 199
3.5.2 AAA 206
3.5.3 Switch 211
3.6 Aggregation 214
3.6.1 Status 214
3.6.2 LACP 215
3.7 Spanning Tree 218
3.7.1 Bridge Status 218
3.7.2 Port Status 219
3.7.3 Port Statistics 219

3.8 IPMC 220
3.8.1 IGMP Snooping 220
3.8.2 MLD Snooping 223
3.9 LLDP 225
3.9.1 Neighbors 225
3.9.2 Port Statistics 226
3.10 PTP 227
3.10.1 PTP 227
3.10.2 802.1AS Statistics 228
3.11 PoE 229
3.12 MAC Table 230
3.13 VLANs 231
3.13.1 Membership 231
3.13.2 Ports 232
3.14 DDMI 233
3.14.1 Overview 233
3.14.2 Detailed 234
3.15 UDLD 235
4 Diagnostics 236
4.1 Ping (IPv4) 236
4.2 Ping (IPv6) 238
4.3 Traceroute (IPv4) 240
4.4 Traceroute (IPv6) 241
5 Maintenance 243
5.1 Restart Device 243
5.2 Factory Defaults 244
5.3 Software 245
5.3.1 Upload 245
5.4 Configuration 245
5.4.1 Save startup-config 246
5.4.2 Download 246
5.4.3 Upload 247
5.4.4 Activate 248
5.4.5 Delete 248
6 Diagnostics 250

Table of Figures

Figure 2.1 IP Address for Web-based Setting 17
Figure 2.2 Login page 17
Figure 2.3 Webpage of RHG9728 after a successful login 18
Figure 2.4 Submenus under Configuration→System Menu 18
Figure 2.5 System Information Configuration Webpage 19
Figure 2.6 Webpage to Configure System's IP Information. 20
Figure 2.7 Webpage to Configure System's IP Configuration 20
Figure 2.8 Webpage to Configure System's IP Interfaces 21
Figure 2.9 Webpage to Configure System's IP Routes 22
Figure 2.10 Webpage to Configure SNMP System 23
Figure 2.11 Webpage to Configure SNMP Trap Destinations 24
Figure 2.12 Adding New Entry to SNMP Trap Destination Table 24
Figure 2.13 Webpage to Configure SNMP Trap Sources 25
Figure 2.14 Adding New Entry to SNMP Trap Sources 25

Figure 2.15 Webpage to Configure SNMP Communities 26
Figure 2.16 Adding New Entry to SNMP Community Configuration 27
Figure 2.17 Webpage to Configure SNMP Users 27
Figure 2.18 Webpage to Configure SNMP Groups 29
Figure 2.19 Webpage to Configure SNMP Views 30
Figure 2.20 Webpage to Configure SNMP Access 31
Figure 2.21 Webpage to Configure System NTP 32
Figure 2.22 Webpage to Configure System Time 33
Figure 2.23 Webpage to Configure System Log 35
Figure 2.24 Webpage to Configure System Alert 36
Figure 2.25 Webpage to Configure System SMTP Setting 36
Figure 2.26 Example of SMTP Setting 37
Figure 2.27 Webpage to Configure Ports of RHG9728 38
Figure 2.28 An Example of Ring Topology (a) Major Ring, and (b) Sub-Ring 40
Figure 2.29 Webpage to Configure ERPS 41
Figure 2.30 After Clicking ⊕ to Configure ERPS 42
Figure 2.31 After Clicking ⊕ to Configure MRPs 43
Figure 2.32 Submenus under the DHCP Main Configuration Menu 44
Figure 2.33 Webpage to Configure DHCPv4 Snooping 44
Figure 2.34 Webpage to Configure DHCPv4 Relay 45
Figure 2.35 Configuration-> Security Menu 47
Figure 2.36 Configuration-> Security -> Switch Menu 48
Figure 2.37 Webpage to Configure Security Switch Users 48
Figure 2.38 Webpage to Configure Security Switch Users – After Clicked **Add New User** Button 49
Figure 2.39 Webpage to Edit User 49
Figure 2.40 Webpage to Configure Privilege Levels of the Switch 51
Figure 2.41 Webpage to Configure Switch Authentication Method 52
Figure 2.42 Webpage to Configure SSH 53
Figure 2.43 Webpage to HTTPS Configuration 54
Figure 2.44 Webpage to HTTPS Configuration with Certificate Uploading 54
Figure 2.45 Webpage to Configure RMON Statistics 55
Figure 2.46 Adding New Entry to RMON Statistics Configuration 55
Figure 2.47 Webpage to Configure RMON History 56
Figure 2.48 Adding New Entry to RMON History Table 56
Figure 2.49 Webpage to Configure RMON Alarm 57
Figure 2.50 Webpage to Configure RMON Event 58
Figure 2.51 Configuration-> Security -> Network Menu 59
Figure 2.52 Webpage to Configure Network Port Security 60
Figure 2.53 Webpage to Configure Network Port Security MAC Addresses 62
Figure 2.54 Webpage to Configure Network NAS 64
Figure 2.55 Access Control List's Submenus 70
Figure 2.56 Webpage to Configure Network ACL Ports 71
Figure 2.57 Webpage to Configure Network ACL Rate Limiters 72
Figure 2.58 Webpage to Configure Network ACL Access Control 73
Figure 2.59 Webpage to Configure Network ACL Access Control After Clicked + to add new entry 74
Figure 2.60 Webpage to IP Source Guard Configuration 82
Figure 2.61 Webpage to Configure Network IP Source Guard Static Table 83
Figure 2.62 ARP Inspection Menu 84
Figure 2.63 Webpage to Configure Network ARP Inspection Port 84
Figure 2.64 Webpage to Configure Network ARP Inspection VLAN 85
Figure 2.65 Webpage to Configure Network ARP Inspection Static Table 86
Figure 2.66 Webpage to Configure Network ARP Inspection Dynamic Table 87
Figure 2.67 Webpage to Configure AAA RADIUS 89
Figure 2.68 Webpage to Configure AAA TACACS+ 90
Figure 2.69 Aggregation Submenus 91
Figure 2.70 Webpage to Configure Common Aggregation 91
Figure 2.71 Webpage to Configure Group Aggregation 92
Figure 2.72 Webpage to Configure LACP Aggregation 93

Figure 2.73 Webpage to Configure Bridge Settings of Spanning Tree 95
Figure 2.74 Webpage to Configure MSTI Mapping of Spanning Tree 97
Figure 2.75 Webpage to Configure Bridge Priorities of Spanning Tree 98
Figure 2.76 Webpage to Configure CIST Ports of Spanning Tree 99
Figure 2.77 Webpage to Configure MSTI of Spanning Tree 101
Figure 2.78 Example of MST1 MSTI Port Configuration 101
Figure 2.79 Configuration->IPMC Menu 102
Figure 2.80 Basic Configuration Webpage to IGMP Snooping of an IPMC Profile 103
Figure 2.81 Webpage to Configure IGMP Snooping's VLAN for an IPMC Profile 104
Figure 2.82 Basic Configuration Webpage to MLD Snooping of an IPMC Profile 105
Figure 2.83 Webpage to Configure MLD Snooping's VLAN for an IPMC Profile 107
Figure 2.84 Webpage to Configure LLDP 108
Figure 2.85 Webpage to Configure MAC Table 110
Figure 2.86 Example of VLAN Configuration 112
Figure 2.87 Webpage for Basic Configuration of VLANs 112
Figure 2.88 Webpage to SVL Configuration 116
Figure 2.89 Webpage to Configure MAC-based VLAN of VCL 117
Figure 2.90 Webpage to Configure Protocol to Group Mapping Table 118
Figure 2.91 Webpage to Configure Group name to VLAN Mapping Table 119
Figure 2.92 Webpage to Configure IP Subnet-based VLAN of VCL 120
Figure 2.93 Webpage to Configure Port Classification of QoS 122
Figure 2.94 Webpage to Configure Port Policing of QoS 123
Figure 2.95 Webpage to Configure Queue Policing of QoS 124
Figure 2.96 Webpage to Configure Port Scheduler of QoS 125
Figure 2.97 Webpage to Configure QoS Egress Port Scheduler and Shapers Port 126
Figure 2.98 Webpage to Configure Port Shaping of QoS 127
Figure 2.99 Webpage to Detailed Configure QoS Egress Port Scheduler and Shapers Port 128
Figure 2.100 Webpage to Configure Port Tag Remarking of QoS 129
Figure 2.101 Webpage to Configure Each Port Tag Remarking of QoS 130
Figure 2.102 Webpage to Configure Port DSCP of QoS 130
Figure 2.103 Webpage to Configure DSCP-Based of QoS 132
Figure 2.104 Webpage to Configure DSCP Translation of QoS 133
Figure 2.105 Webpage to Configure DSCP Classification of QoS 134
Figure 2.106 Webpage to Configure QoS Control List 135
Figure 2.107 Adding New QCE Configuration 136
Figure 2.108 Webpage to Configure Storm Policing of QoS 138
Figure 2.109 Traffic Mirroring Operation 139
Figure 2.110 Webpage to Configure Mirroring 140
Figure 2.111 Webpage to Detailed Configure Mirroring for Session ID 141
Figure 2.112 Webpage to Configure PTP 142
Figure 2.113 Webpage to Add New PTP Clock 143
Figure 2.114 Webpage to Configure GVRP Globally 145
Figure 2.115 Webpage to Configure Port for GVRP 145
Figure 2.116 Webpage to Configure DDMI 147
Figure 2.117 Webpage to Configure UDLD 149
Figure 2.118 Webpage to Configure SD Backup 150
Figure 2.119 Webpage to Configure Modbus Setting 151
Figure 2.120 Mapping Table of Modbus Address for Switch's IP Address 151
Figure 2.121 Entering Connection Setup Menu of the Modbus Poll 152
Figure 2.122 Modbus Poll Connection Setup 152
Figure 2.123 Multiple Cell Section in Modbus Poll 153
Figure 2.124 Set Display Mode to Hex in Modbus Poll 153
Figure 2.125 Modbus Poll Setup Read/Write Definition 154
Figure 2.126 Slave ID in the Modbus Poll Function is set to 1 154
Figure 2.127 Set Code 03 in the Modbus Poll Function 155
Figure 2.128 Setup Starting Address and Quantity in Modbus Poll 155
Figure 2.129 Mapping Table of Modbus Address for Clearing Port Statistics 156

Figure 2.130 Port Count in Port Statistics Webpage 156
Figure 2.131 Click on Function 06 in the Modbus Poll 157
Figure 2.132 Use Modbus Poll to Clear Switch's Port Count 157
Figure 2.133 Cleared Port Statistics 157
Figure 2.134 A PRP-SAN RedBox connected to a PRP network 164
Figure 2.135 An HSR-SAN Redbox connected to an HSR ring 165
Figure 2.136 Two HSR-PRP RedBoxes interconnect a PRP network and an HSR ring 166
Figure 2.137 Multiple PRP networks connected to a single HSR ring 168
Figure 2.138 Single PRP network connected to multiple HSR rings 169
Figure 2.139 Connection of two HSR rings with two QuadBoxes 170
Figure 2.140 Demonstration of HSR-SAN 180
Figure 2.141 Enable RedBox in HSR-SAN mode (Step 1) 180
Figure 2.142 Enable RedBox in HSR-SAN mode (Step 2) 180
Figure 2.143 Enable RedBox in HSR-SAN mode (Step 3) 180
Figure 2.144 Enable RedBox in HSR-SAN mode (Step 4) 181
Figure 3.1 Webpage to Monitor System Information 182
Figure 3.2 Summary of Software License 183
Figure 3.3 Webpage to Monitor System's CPU Load 183
Figure 3.4 Webpage to Monitor System's IP Status 184
Figure 3.5 Webpage to Monitor System's IPv4 Routing Information Base 185
Figure 3.6 Webpage to Monitor System's IPv6 Routing Information Base 186
Figure 3.7 Webpage to Monitor System Log 187
Figure 3.8 Webpage to Monitor System Detailed Log 188
Figure 3.9 Webpage to Monitor System's Power Status 188
Figure 3.10 Webpage to Monitor System's Digital Input 189
Figure 3.11 Webpage of RHG9728 to Monitor Port State 189
Figure 3.12 Webpage to Monitor Traffic Overview of Ports 190
Figure 3.13 Webpage to Monitor Queuing Counters 190
Figure 3.14 Webpage to Monitor QoS Control List Status 191
Figure 3.15 Webpage to Monitor Detailed Port Statistics 192
Figure 3.16 Webpage to Name Map 193
Figure 3.17 Webpage to ERPS Status 194
Figure 3.18 Webpage to ERPS Detailed Status 195
Figure 3.19 Webpage to Monitor Dynamic DHCP Snooping Table 196
Figure 3.20 Webpage to Monitor DHCP Relay Statistics 197
Figure 3.21 Webpage to Monitor DHCP Server Statistics 198
Figure 3.22 Webpage to Monitor DHCP Server Statistics 199
Figure 3.23 Webpage to Monitor Port Security Port Status All Ports 200
Figure 3.24 Webpage to Monitor Network Access Server Switch Status 202
Figure 3.25 Webpage to Monitor NAS Statistics Port 1 203
Figure 3.26 Webpage to Monitor ACL Status 204
Figure 3.27 Webpage to Monitor Dynamic ARP Inspection Table 205
Figure 3.28 Webpage to Monitor Dynamic IP Source Guard Table 206
Figure 3.29 Webpage to Monitor RADIUS Server Status Overview 206
Figure 3.30 Webpage to Monitor Each Port's RADIUS Server Status 207
Figure 3.31 Webpage to Monitor RADIUS Authentication and Accounting Statistics 209
Figure 3.32 Webpage to Monitor RMON Statistics Status Overview 211
Figure 3.33 Webpage to Monitor RMON History Overview 212
Figure 3.34 Webpage to Monitor RMON Alarm Overview 213
Figure 3.35 Webpage to Monitor RMON Event 214
Figure 3.36 Webpage to Monitor Aggregation Status 215
Figure 3.37 Webpage to Monitor LACP System Status 215
Figure 3.38 Webpage to Monitor LACP Internal Port Status 216
Figure 3.39 Webpage to Monitor LACP Neighbour Port Status 217
Figure 3.40 Webpage to Monitor LACP Statistics 218
Figure 3.41 Webpage to Monitor STP Bridges 218
Figure 3.42 Webpage to Monitor STP Port Status 219
Figure 3.43 Webpage to Monitor STP Statistics 219

Figure 3.44 IGMP Snooping Submenu under Configuration->IPMC Main Menu 220
Figure 3.45 Webpage to Monitor DHCP Server Statistics 221
Figure 3.46 Webpage to Monitor IGMP Snooping Group Information 222
Figure 3.47 Webpage to Monitor IGMP SFM Information 222
Figure 3.48 Webpage to Monitor MLD Snooping Status 223
Figure 3.49 Webpage to Monitor MLD Snooping Group Information 224
Figure 3.50 Webpage to Monitor....225
Figure 3.51 Webpage to Monitor LLDP Neighbour Information....225
Figure 3.52 Webpage to Monitor LLDP Global and Statistics Local Counters 226
Figure 3.53 Webpage to Monitor PTP External Clock Mode and Clock Configuration 228
Figure 3.54 Webpage to Monitor 802.1AS Statistics 228
Figure 3.55 Webpage to PoE Status....230
Figure 3.56 Webpage to Monitor MAC Address Table 231
Figure 3.57 Webpage to Monitor VLAN Membership Status for Combined Users....231
Figure 3.58 Webpage to Monitor VLAN Port Status for Combined Users 232
Figure 3.59 Webpage to Monitor DDMI Overview 233
Figure 3.60 Webpage to Monitor DDMI Detailed 234
Figure 3.61 Webpage to Monitor Detailed UDLD Status for Port 1 and Neighbour Status 235
Figure 4.1 Diagnostics Menu 236
Figure 4.2 Diagnostics Webpage using IPv4 Ping....236
Figure 4.3 Result of successful IPv4 ping 238
Figure 4.4 Result of failure IPv4 ping 238
Figure 4.5 Diagnostics Webpage using IPv6 Ping....238
Figure 4.6 Result of successful IPv6 ping 239
Figure 4.7 Result of failure IPv6 ping 239
Figure 4.8 Diagnostics Webpage using IPv4 Traceroute....240
Figure 4.9 Example of traceroute (IPv4) output 241
Figure 4.10 Diagnostics Webpage using IPv6 Traceroute....241
Figure 5.1 Maintenance Menu 243
Figure 5.2 Webpage to Restart the Device 243
Figure 5.3 System restart in progress webpage 244
Figure 5.4 Webpage to Reset Configuration to Factory Defaults 244
Figure 5.5 Message after the configuration factory reset is done. 244
Figure 5.6 Webpage to Upload Software 245
Figure 5.7 Submenus under Maintenance→Configuration menu....246
Figure 5.8 Webpage to Save the Start-up Configuration 246
Figure 5.9 Message indicates the saving of startup-configuration file successfully 246
Figure 5.10 Webpage to Download the Current Configuration File 247
Figure 5.11 Webpage to Upload a Configuration File....247
Figure 5.12 Webpage to Activate a Configuration File 248
Figure 5.13 Activating New Configuration Webpage 248
Figure 5.14 Webpage to Delete a Configuration File....249
Figure 5.15 Confirmation for deleting a configuration file 249

Table of Tables

Table 2.1 Description of the System Information Configuration 19
Table 2.2 Description of Basic Settings 20
Table 2.3 Description of IP Interfaces' Options....21
Table 2.4 Description of IP Routes' Options 22
Table 2.5 Descriptions of SNMP Trap Destination Configurations 24
Table 2.6 Description of SNMP Trap Source Configurations....26
Table 2.7 Descriptions of SNMP Community Configurations 27
Table 2.8 Descriptions of SNMP Users....27
Table 2.9 Descriptions of SNMP Groups 29
Table 2.10 Descriptions of SNMP Views 30
Table 2.11 Descriptions of SNMP Access Configuration....31
Table 2.12 Descriptions of the NTP Settings 32

Table 2.13 Description of System Time Configuration....33
Table 2.14 Description of Time Zone Configuration....34
Table 2.15 Description of Daylight-Saving Time Configuration....34
Table 2.16 Descriptions of the System Zone Configuration....35
Table 2.17 Descriptions of Power Status Alarm Event Selection....36
Table 2.18 Descriptions of SMTP Setting....37
Table 2.19 Descriptions of Port Configuration....38
Table 2.20 Description of EPRS Configuration Table....41
Table 2.21 Descriptions of ERPS Configuration Webpage....42
Table 2.22 Description of DHCP Snooping Configuration....45
Table 2.23 Description of DHCP Relay Configuration....45
Table 2.24 Description of Users Configuration....48
Table 2.25 Descriptions of Users Configuration – After Clicked **Add New User** Button....49
Table 2.26 Examples of Group Name....50
Table 2.27 Descriptions of Switch Authentication Method....52
Table 2.28 Description of HTTPS Configuration Webpage....54
Table 2.29 Descriptions of RMON Statistics....55
Table 2.30 Descriptions of RMON History....56
Table 2.31 Descriptions of RMON Alarm....57
Table 2.32 Descriptions of RMON Event....58
Table 2.33 Descriptions of Port Security Configuration....60
Table 2.34 Descriptions of RMON Event....62
Table 2.35 Descriptions of Network NAS....64
Table 2.36 Descriptions of Network ACL Ports....71
Table 2.37 Descriptions of Network ACL Rate Limiters....72
Table 2.38 Summary of Label, Description, and Factory Default for ACL (Access Control List)....73
Table 2.39 Description of ACL Configuration....75
Table 2.40 Description of ACL Configuration with MAC Parameters....76
Table 2.41 Description of ACL Configuration with VLAN Parameters....76
Table 2.42 Description of ACL Configuration with ARP Parameters....77
Table 2.43 Description of ACL Configuration with IPv4 Parameters....78
Table 2.44 Description of ACL Configuration with IPv6 Parameters....79
Table 2.45 Description of ACL Configuration with ICMP Parameters....80
Table 2.46 Description of ACL Configuration with TCP/UDP Parameters....80
Table 2.47 Description of ACL Configuration with Ethernet Type Parameters....82
Table 2.48 Descriptions of Network IP Source Guard Configuration....83
Table 2.49 Descriptions of Network IP Source Guard Static....83
Table 2.50 Descriptions of ARP Inspection Port Configuration....84
Table 2.51 Descriptions of ARP Inspection VLAN Table....86
Table 2.52 Descriptions of Static ARP Inspection Table....86
Table 2.53 Descriptions of ARP Inspection Dynamic Table....87
Table 2.54 Descriptions of AAA RADIUS....89
Table 2.55 Comparison of Authentication Server Settings between RADIUS and TACACS+....90
Table 2.56 Descriptions of AAA RADIUS....90
Table 2.57 Descriptions of Common Aggregation Configuration....91
Table 2.58 Descriptions of Aggregation Group Configuration....92
Table 2.59 Descriptions of LACP Aggregation Configuration....93
Table 2.60 Descriptions of Bridge Settings Configuration of Spanning Tree....95
Table 2.61 Descriptions of Bridge Priorities Configuration of Spanning Tree....97
Table 2.62 Descriptions of Bridge MSTI Priorities Configuration of Spanning Tree....98
Table 2.63 Descriptions of CIST Ports Configuration of Spanning Tree....99
Table 2.64 Descriptions of MSTI Configuration of Spanning Tree....102
Table 2.65 Descriptions of IGMP Snooping of an IPMC Profile....103
Table 2.66 Descriptions of IGMP Snooping's VLAN Configuration for an IPMC Profile....104
Table 2.67 Descriptions of MLD Snooping Configuration for an IPMC Profile....106
Table 2.68 Descriptions of MLD Snooping's VLAN Configuration for an IPMC Profile....107
Table 2.69 Descriptions of LLDP Configuration....108
Table 2.70 Description of MAC Address Table Configuration....110
Table 2.71 Description of Global VLAN Configuration....113
Table 2.72 Description of Port VLAN Configuration....113

Table 2.73 Description of Shared VLAN Learning Configuration 116
Table 2.74 Descriptions of MAC-based VLAN Configuration of VCL 117
Table 2.75 Descriptions of Protocol to Group Mapping Table Configuration....118
Table 2.76 Descriptions of Group name to VLAN Mapping Table Configuration 119
Table 2.77 Descriptions of IP Subnet-based VLAN Configuration....120
Table 2.78 Descriptions of Voice VLAN Configuration 121
Table 2.79 Descriptions of Port Classification Configuration of QoS....122
Table 2.80 Descriptions of Port Policing Configuration of QoS 124
Table 2.81 Descriptions of Queue Policing Configuration of QoS 124
Table 2.82 Descriptions of Port Scheduler Configuration of QoS....125
Table 2.83 Descriptions of QoS Egress Port Scheduler and Shapers Port Configuration 126
Table 2.84 Descriptions of Port Shaping Configuration of QoS....127
Table 2.85 Descriptions of Detaled QoS Egress Port Scheduler and Shapers Port Configuration....128
Table 2.86 Descriptions of Port Tag Remarking Configuration of QoS 129
Table 2.87 Descriptions for Port Tag Remarking Configuration of Mode 130
Table 2.88 Descriptions of Port DSCP Configuration of QoS 130
Table 2.89 Descriptions of DSCP-Based Configuration of QoS 132
Table 2.90 Descriptions of DSCP Translation Configuration of QoS....133
Table 2.91 Descriptions of DSCP Classification Configuration of QoS 134
Table 2.92 Descriptions of QoS Control List Configuration 135
Table 2.93 Descriptions of QoS Control Entry's Parameters....136
Table 2.94 Description of Frame Type....137
Table 2.95 Descriptions of Storm Policing Configuration of QoS 138
Table 2.96 Descriptions of Mirroring Webpage....140
Table 2.97 Descriptions of PTP Clock Configuration....143
Table 2.98 Descriptions of New PTP Clock Configuration....143
Table 2.99 Descriptions of GVRP Globally Configuration....145
Table 2.100 Descriptions of GVRP PortConfiguration 146
Table 2.101 Descriptions of sFlow PortConfiguration 146
Table 2.102 Descriptions of DDMI Configuration....147
Table 2.103 Descriptions of UDLD Port Configuration 149
Table 2.104 Descriptions of SD Backup Configuration....150
Table 2.105 Descriptions of Modbus Setting PortConfiguration 151
Table 2.106 Descriptions of RedBox Configuration 173
Table 3.1 Monitoring Descriptions of System Information 182
Table 3.2 Monitor Descriptions of System's IP Status 184
Table 3.3 Monitoring Descriptions of System's IPv4 Routing Information Base....185
Table 3.4 Monitoring Descriptions of System's IPv6 Routing Information Base....186
Table 3.5 Monitoring Descriptions of System Log....187
Table 3.6 Monitoring Descriptions of System Detailed Log 188
Table 3.7 Monitoring Descriptions of Traffic Overview of Ports 190
Table 3.8 Monitoring Descriptions of Queuing Counters 190
Table 3.9 Monitoring Descriptions of QoS Control List Status....191
Table 3.10 Monitoring Descriptions of Detailed Port Statistics 192
Table 3.11 Description of ERPS Status 194
Table 3.12 Description of ERPS Detailed Status....195
Table 3.13 Monitoring Descriptions of Dynamic DHCP Snooping Table....196
Table 3.14 Monitoring Descriptions of DHCP Relay Statistics....197
Table 3.15 Monitoring Descriptions of DHCP Detailed Statistics Port 1 198
Table 3.16 Monitoring Descriptions of Port Security Switch Status 199
Table 3.17 Monitoring Descriptions of Port Security Port Status All Ports 201
Table 3.18 Monitoring Descriptions of Network Access Server Switch Status 202
able 3.19 Monitoring Descriptions of NAS Statistics Port 1 203
Table 3.20 Monitoring Descriptions of ACL Status 204
Table 3.21 Monitoring Descriptions of Dynamic ARP Inspection Table 205
Table 3.22 Monitoring Descriptions of Dynamic IP Source Guard Table 206
Table 3.23 Monitoring Descriptions of RADIUS Server Status Overview....206
Table 3.24 Monitoring Descriptions of Each Port's RADIUS Server Status 207
Table 3.25 Monitoring Descriptions of RADIUS Authentication and Accounting Statistics 209
Table 3.26 Monitoring Descriptions of RMON Statistics Status Overview....211

Table 3.27 Monitoring Descriptions of RMON History Overview 212
Table 3.28 Monitoring Descriptions of RMON Alarm Overview 213
Table 3.29 Monitoring Descriptions of RMON Event 214
Table 3.30 Monitoring Descriptions of Aggregation Status 215
Table 3.31 Monitoring Descriptions of LACP System Status 215
Table 3.32 Monitoring Descriptions of LACP Internal Port Status 216
Table 3.33 Monitoring Descriptions of LACP Neighbour Port Status 217
Table 3.34 Monitoring Descriptions of LACP Statistics 218
Table 3.35 Monitoring Descriptions of STP Bridges 218
Table 3.36 Monitoring Descriptions of STP Port Status 219
Table 3.37 Monitoring Descriptions of STP Statistics 219
Table 3.38 Descriptions of DHCP Server Statistics Monitoring 221
Table 3.39 Monitoring Descriptions of IGMP Snooping Group Information 222
Table 3.40 Monitoring Descriptions IGMP SFM Information 223
Table 3.41 Monitoring Descriptions of MLD Snooping Status 223
Table 3.42 Monitoring Descriptions of MLD Snooping Group Information 224
Table 3.43 Monitoring Descriptions of MLD SFM Information 225
Table 3.44 Monitoring Descriptions of LLDP Neighbour Information 225
Table 3.45 Monitoring Descriptions of LLDP Global and Statistics Local Counters 226
Table 3.46 Monitoring Descriptions of PTP External Clock Mode and Clock Configuration 228
Table 3.47 Monitoring Descriptions of 802.1AS Statistics 229
Table 3.48 Monitoring Descriptions of QoS Control List Status 230
Table 3.49 Monitoring Descriptions of MAC Address Table 231
Table 3.50 Monitoring Descriptions of VLAN Membership Status for Combined Users 232
Table 3.51 Monitoring Descriptions of VLAN Port Status for Combined Users 232
Table 3.52 Monitoring Descriptions of DDMI Overview 233
Table 3.53 Monitoring Descriptions of DDMI Detailed 234
Table 3.54 Monitoring Descriptions of Detailed UDLD Status for Port 1 and Neighbour Status 235
Table 4.1 Descriptions of Options for Ping (IPv4) Diagnostic Tool 236
Table 4.2 Descriptions of Options for Ping (IPv6) Diagnostic Tool 239
Table 4.3 Description of each parameter for Traceroute (IPv4) 240
Table 4.4 Description of each parameter for Traceroute (IPv6) 241

1 Introduction

1.1 Introduction to Industrial Managed Switch

The ATOP RHG9728 series is a product line of powerful industrial managed switches designed as Open Systems Interconnection (OSI) Layer 2 bridging devices.

Unlike an unmanaged switch, typically found in homes or Small Office/Home Office (SOHO) environments and operating in automatic “plug-and-play” mode, each port of a managed switch can be precisely configured for bandwidth, priority, security, and duplex settings. The RHG9728 series can be managed via Simple Network Management Protocol (SNMP), web browsers, Telnet, or serial console. With per-port configuration, network administrators can exercise full control of the network and optimize overall functionality.

Industrial-Grade Design

ATOP’s managed switches are designed specifically for harsh industrial environments—not just comfortable office conditions. They continue operating reliably under:

- Extreme temperature variations
- High humidity
- Dusty or polluted air
- Mechanical impact or vibration
- High levels of electrostatic discharge

This rugged design ensures stable and reliable performance even under demanding conditions.

Secure and Reliable Networking

The RHG9728 series delivers a faster, more secure, and stable network. Key advantages include:

- Security features: IP Source Guard, DHCP Snooping, ARP Inspection, and Access Control Lists (ACLs).
- Redundancy protocols: Ethernet Ring Protection Switching (ERPS), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP). These protocols enhance network reliability and minimize recovery time during link failures.
- Standards Compliance

ATOP’s managed switches support a broad range of IEEE standard protocols. They are reliable in preventing system downtime or data loss, easy to configure for users at all levels, and optimized to deliver an enhanced network management experience.

Additional Redundancy Protocols: HSR and PRP

To meet the requirements of critical applications where zero recovery time is essential, the RHG9728 series also supports IEC 62439-3 redundancy protocols:

High-availability Seamless Redundancy (HSR)

HSR creates a ring topology where each frame is duplicated and sent in both directions. End devices receive two copies of each frame and use the first valid one, discarding duplicates. This ensures seamless communication with zero packet loss even if a link or node fails. HSR is particularly suited for time-sensitive industrial networks, such as those found in power substations and process automation.

Parallel Redundancy Protocol (PRP)

PRP operates by connecting each end device to two independent LANs. Every transmitted frame is duplicated and sent over both networks simultaneously. The receiving device processes the first arriving frame and ignores the

duplicate. Since both LANs are fully independent, PRP guarantees uninterrupted operation with zero switchover delay, even if one entire network fails.

Both HSR and PRP are designed for mission-critical industrial applications requiring high availability, such as utilities, transportation, and manufacturing automation. By supporting these protocols in addition to ERPS, RSTP, and MSTP, the RHG9728 series provides flexible redundancy options to ensure network resilience and continuous operation.

Please note that the HSR/PRP function will be available in the first quarter of 2027.

Note:
Throughout the manual, the symbol * indicates that more detailed information of the subject will be provided at the end of this book or as a footnote.

1.2 Software Features

Atop's industrial Layer-2 Managed switches come with a wide range of network protocols and software features. These protocols and software features allow the network administrator to implement security and reliability into their network. These features enable Atop's switches to be used in safety applications, and factory and process automation. The followings are the list of protocols and software features.

- User Interfaces
  - Web browser
  - Telnet Console
  - Serial Console
- Dynamic Host Configuration Protocol (DHCP) Snooping/Relay/Client
- Time Synchronization
  - Network Time Protocol (NTP) Client
  - Simplified Network Time Protocol (SNTP)
  - IEEE 1588 Precision Clock Synchronization Protocol (PTP) v2 hw-E2E TC and hw-sw-Boundary -> hw-Boundary Clock
  - TSN
- Port Mirroring
- Quality of Service (QoS) Traffic Regulation
- Link Aggregation Control Protocol (LACP)
- Medium Access Control (MAC) Filter
- GARP VLAN Registration Protocol (GVRP)
- Internet Group Management Protocol (IGMP)/ Multicast Listener Discovery (MLD)
- Simple Network Management Protocol (SNMP) v1/v2/v3
- SNMP Inform
- Spanning Tree Protocol (STP)/ Rapid Spanning Tree Protocol (RSTP)/ Multiple Spanning Tree Protocol (MSTP)
- Virtual Local Area Network (VLAN)
- IEEE 802.1x/ Extensible Authentication Protocol (EAP) / Remote Authentication Dial-In User Service (RADIUS) / Terminal Access Controller Access-Control System (TACACS+)
- Security feature including Port Security/ IP Source Guard/ ARP Inspection/ Access Control List (ACL)
- Ring
  - Ethernet Ring Protection Switching (ERPS)
  - High-availability Seamless Redundancy (HSR)
  - Media Redundancy Protocol (MRP)
- Link Layer Discovery Protocol (LLDP)
- Alarm System (with E-mail Notification or Relay Output)
- Industrial Protocols
  - Modbus/TCP
- SD Backup

1.3 Introduction to the Document

There are total of six sections in this document: Introduction, Configuring with a web browser, Monitor, Diagnostics, Maintenance. The first section introduces the device, the software features, and the document. The second section, configuring with a web browser shows users the setting webpage and the meaning of each parameter. The third section, Monitor, allows user to see the current status of the device. The forth section, Diagnostics, allows user to identify problems and troubleshooting through ping and traceroute webpage. Lastly, the fifth section, Maintenance, will let user to restart the device, reset all settings to the default values, as well as, upload software version and save/download/upload/activate/delete the current configuration.

2 Configuring with a Web Browser

There are three ways to configure Atop's Industrial Managed Ethernet Switch: Web browser, Telnet console, and Serial console. How to access the industrial managed switch through web browser is explained in Chapter 2 through Chapter 5. There are only a few differences among these three methods. The web browser and the telnet console methods allow users to access the switch over the Internet or the Ethernet LAN, while the serial console method requires a serial cable connection between the console and the switch. Users are recommended to configure the switch via a web browser because of its user-friendly interface.

Next, we will proceed to use a web browser to introduce the managed switch's functions. It is recommended to use Microsoft Edge 103, Firefox 44, Chrome 48 or later versions. Below is a list of default factory settings. This information will be used during the login process. Make sure that the computer accessing the switch are in the same subnet. That is the computer has an IP address and the subnet mask same as the switch. Please pay attention when inputting the username and password, as they are case sensitive.

IP Address: 10.0.50.1
Subnet Mask: 255.255.0.0
Default Gateway: 0.0.0.0
User Name: admin
Password: default

Before users can access the configuration, they have to log in. This can simply be done in the following steps.

1. Launch a web browser.
2. Type in the switch IP address (e.g. http://10.0.50.1), as shown in Figure 2.1).
   Note: When the user name and the password are left empty, the login prompt will not show.

Figure 2.1 IP Address for Web-based Setting

3. The user can enter a **Username** and a **Password** to access the managed switch. Then, clicking on the **Sign in** button.

Figure 2.2 Login page

4. If the user entered wrong passwords, users can try to re-enter the new username and password again until it is correct. Or users can simply click the **Cancel** button to forfeit the process.

5. If the login process was success, the user will be presented with the Port State Overview webpage which shows the front panel of the managed switch as shown in Figure 2.3.

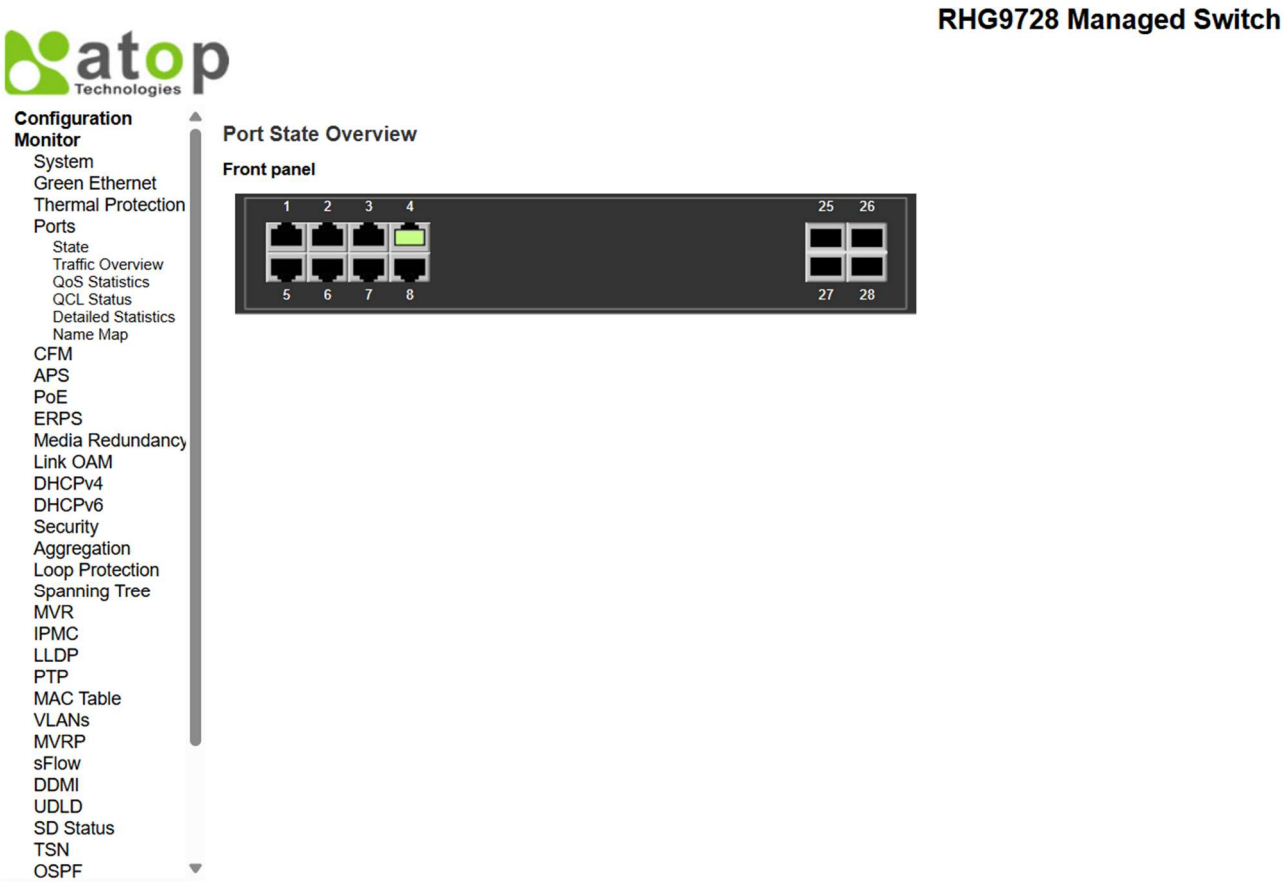


Figure 2.3 Webpage of RHG9728 after a successful login

2.1 System

This section describes how users can configure system information in details. Figure 2.4 shows submenus under the **Configuration→System** main menu.

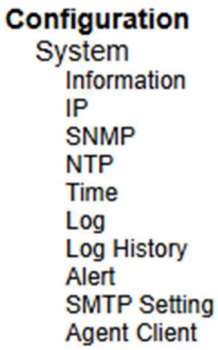


Figure 2.4 Submenus under Configuration→System Menu

2.1.1 Information

This subsection describes how users can assign system's details to the Atop's switch. There are three fields in this **System Information Configuration** webpage: **System Contact**, **System Name**, and **System Location**. By entering this unique and relevant system information, it will help identifying one specific switch among all the others in the network. However, the switch must support a SNMP protocol. Figure 2.5 shows the System Information Configuration Webpage to an RHG9728 managed switch model. Please click the "**Save**" button to update the

information on the switch. Clicking on the Reset button will undo any changes made locally and revert to previously save values. Table 2.1 summarizes the device information setting descriptions and corresponding default factory settings.

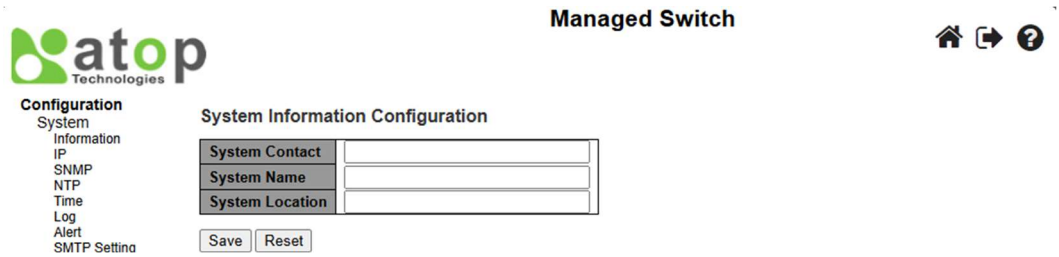


Figure 2.5 System Information Configuration Webpage

Table 2.1 Description of the System Information Configuration

Label	Description	Factory Default
System Contact	Provides contact information for maintenance. Enter the name of whom to contact in case a problem occurs. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.	Null
System Name	Specifies a particular role or application of different switches. The name entered here will also be shown in Atop's Device Management Utility. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.	Null
System Location	The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.	Null

2.1.2 IP

In this subsection, the user may modify network settings on Internet Protocol (**IP**) for the managed switch. This subsection is divided into three parts: **IP Configuration, IP Interfaces**, and **IP Routes**, as shown in

. First, **the IP Configuration** part is related to how the managed switch will be operated as Host. The **IP Interfaces** part is related to IP Address configuration and DHCP configuration for both IPv4 and IPv6. Finally, the **IP Routes** part contains the routing table that provides information about the network destination, gateway, next hop, and distance.

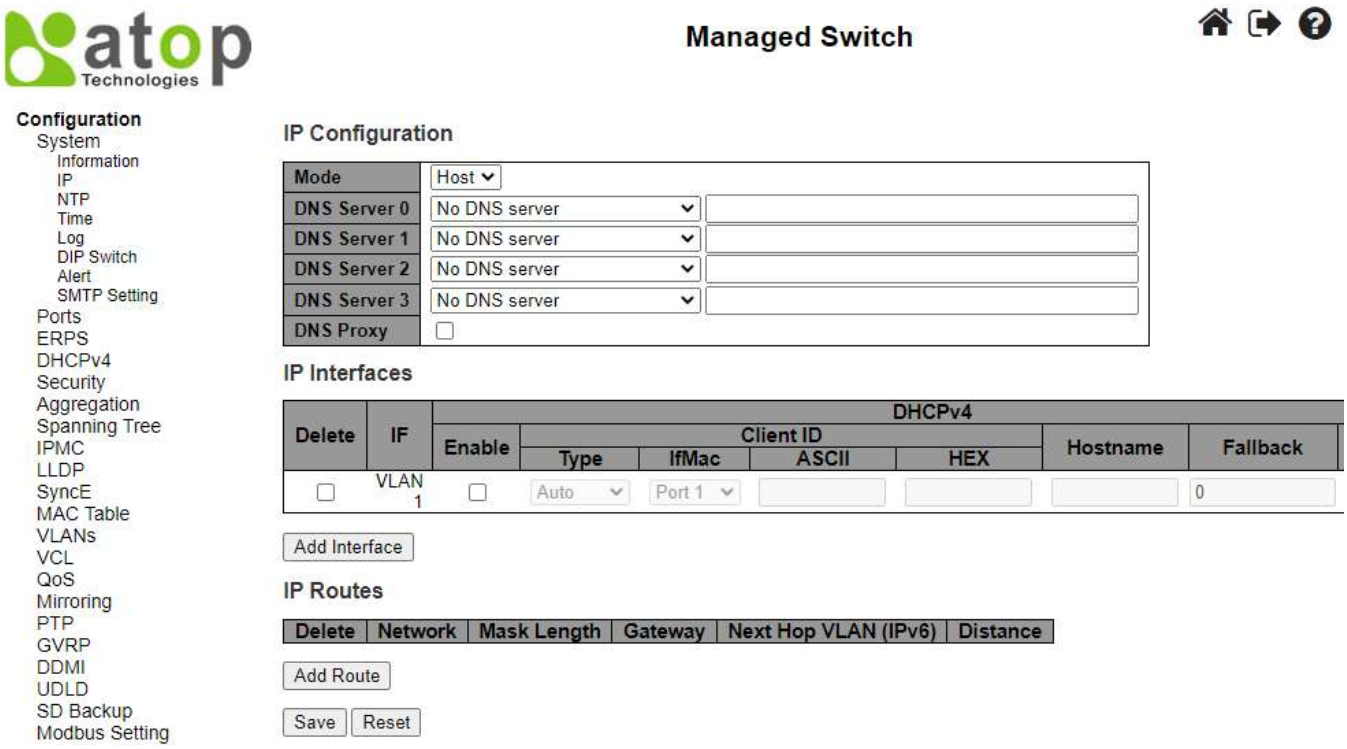


Figure 2.6 Webpage to Configure System's IP Information.

The first part as shown in Figure 2.6 allows the user to set the operating mode of the managed switch. The user can enter up to four DNS Servers. A **DNS** (domain name system) **proxy** allows clients to set up device as a DNS proxy server. A DNS proxy improves domain lookup performance by caching previous lookups. A typical DNS proxy processes DNS queries by issuing a new DNS resolution query to each name server that it has detected until the hostname is resolved. Table 2.2 provides detailed description of each option in this part which is also called basic setting.

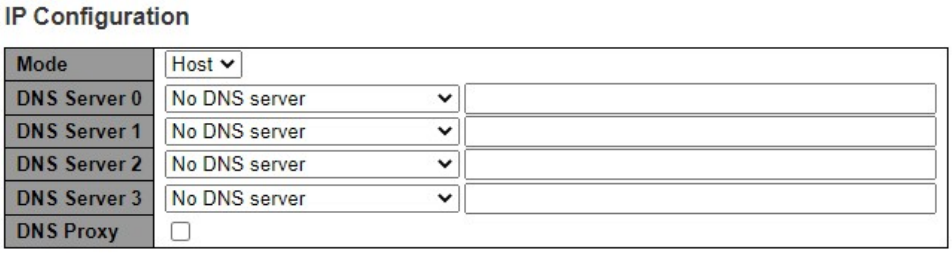


Figure 2.7 Webpage to Configure System's IP Configuration

Table 2.2 Description of Basic Settings

Label	Description
Mode	Configure the IP stack to act as a Host, where IP traffic between interfaces will not be routed.
DNS Server	This setting controls the DNS name resolution done by the switch. There are four servers available for configuration, and the index of the server presents the preference (less index has higher priority) in doing DNS name resolution. The following modes are supported: - **No DNS server**: No DNS server will be used. - **Configured IPv4**: Explicitly provide the valid IPv4 unicast address of the DNS Server in dotted decimal notation. Make sure the configured DNS server could be reachable (e.g. via PING) for activating DNS service.

Label	Description
	- **Configured IPv6**: Explicitly provide the valid IPv6 unicast (except local link) address of the DNS Server. Make sure the configured DNS server could be reachable (e.g. via PING6) for activating DNS service. - **From any DHCPv4 interfaces**: The first DNS server offered from a DHCPv4 lease to a DHCPv4-enabled interface will be used. - **From this DHCPv4 interface**: Specify from which DHCPv4-enabled interface a provided DNS server should be preferred. - **From any DHCPv6 interfaces**: The first DNS server offered from a DHCPv6 lease to a DHCPv6-enabled interface will be used. - **From this DHCPv6 interface**: Specify from which DHCPv6-enabled interface a provided DNS server should be preferred.
DNS Proxy	When DNS proxy is enabled, system will relay DNS requests to the currently configured DNS server, and reply as a DNS resolver to the client devices on the network. Only IPv4 DNS proxy is now supported

The second part of IP Setting section is the **IP Interface** part as shown in Figure 2.8. The user can choose to enable **DHCP** (Dynamic Host Configuration Protocol) for DHCPv4 and/or DHCPv6 by checking the box behind it. That is the IP address and related information can be automatically obtained from a DHCP server in the local network thus reducing the work for an administrator. By disabling this function (DHCP's box is unchecked), the user has an option to setup the static IP address and related fields manually. If DHCP is disabled, the user should enter the IP addresses and Max Length (subnet mask) under IPv4 and/or IPv6 columns. Table 2.3 provides detailed description of each option in this part of IP Interfaces.

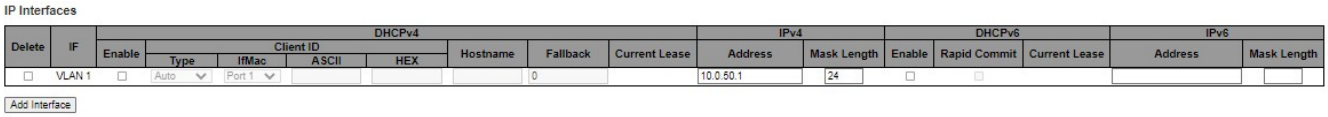


Figure 2.8 Webpage to Configure System's IP Interfaces

Table 2.3 Description of IP Interfaces' Options

Label	Description
Delete	Select this option to delete an existing IP interface.
IF	The VLAN associated with the IP interface. Only ports in this VLAN will be able to access the IP interface. This field is only available for input when creating a new interface
DHCPv4 Enabled	Enable the DHCPv4 client by checking this box. If this option is enabled, the system will configure the IPv4 address and mask of the interface using the DHCPv4 protocol.
DHCPv4 Client ID Type	This specified which of the three types below, i.e. IfMac, ASCII or HEX, shall be used for the Client Identifier. See RFC-2132 section 9.14.
DHCPv4 Client ID ifMac	The interface name of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ifmac', the configured interface's hardware MAC address will be used in the DHCP option 61 field.
DHCPv4 Client ID ASCII	The ASCII string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type is 'ascii', the ASCII string will be used in the DHCP option 61 field.
DHCPv4 Client ID HEX	The hexadecimal string of DHCP client identifier. When DHCPv4 client is enabled and the client identifier type 'hex', the hexadecimal value will be used in the DHCP option 61 field.
DHCPv4 Hostname	The hostname of DHCP client. If DHCPv4 client is enabled, the configured hostname will be used in the DHCP option 12 field. When this value is empty string, the field use the configured system name plus the latest three bytes of system MAC addresses as the hostname.

Label	Description
DHCPv4 Fallback	The number of seconds for trying to obtain a DHCP lease. After this period expires, a configured IPv4 address will be used as IPv4 interface address. A value of zero disables the fall-back mechanism, such that DHCP will keep retrying until a valid lease is obtained. Legal values are 0 to 4294967295 seconds.
DHCPv4 Current Lease	For DHCP interfaces with an active lease, this column shows the current interface address, as provided by the DHCP server.
IPv4 Address	The IPv4 address of the interface in dotted decimal notation. If DHCP is enabled, this field configures the fall-back address. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fall-back address is desired.
IPv4 Mask Length	The IPv4 network mask, in number of bits (prefix length). Valid values are between 0 and 30 bits for an IPv4 address. If DHCP is enabled, this field configures the fall-back address network mask. The field may be left blank if IPv4 operation on the interface is not desired - or no DHCP fall-back address is desired.
DHCPv6 Enable	Enable the DHCPv6 client by checking this box. If this option is enabled, the system will configure the IPv6 address of the interface using the DHCPv6 protocol.
DHCPv6 Rapid Commit	Enable the DHCPv6 Rapid-Commit option by checking this box. If this option is enabled, the DHCPv6 client terminates the waiting process as soon as a Reply message with a Rapid Commit option is received. This option is only manageable when DHCPv6 client is enabled.
DHCPv6 Current Lease	For DHCPv6 interface with an active lease, this column shows the interface address provided by the DHCPv6 server.
IPv6 Address	The IPv6 address of the interface. An IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, fe80::215:c5ff:fe03:4dc7. The symbol :: is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. System accepts the valid IPv6 unicast address only, except IPv4-Compatible address and IPv4-Mapped address. The field may be left blank if IPv6 operation on the interface is not desired.
IPv6 Mask Length	The IPv6 network mask, in number of bits (prefix length). Valid values are between 1 and 128 bits for an IPv6 address. The field may be left blank if IPv6 operation on the interface is not desired.

The third part of IP Setting section is the **IP Routes** part as shown in Figure 2.9. Description of each field or option is summarized in Table 2.4. Please click on the **Save** button to update the IP configuration on the switch. A system reboot is required after each update, so the new network settings can take effect. The user will need to manually update the new IP address in the URL field of the web browser if the IP address of the managed switch is changed.

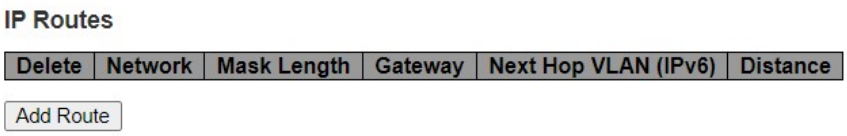


Figure 2.9 Webpage to Configure System's IP Routes

Table 2.4 Description of IP Routes' Options

Label	Description
Delete	Select this option to delete an existing IP route.

Label	Description
Network	The destination IP network or host address of this route. Valid format is dotted decimal notation or a valid IPv6 notation. A default route can use the value 0.0.0.0or IPv6 :: notation.
Mask Length	The destination IP network or host mask, in number of bits (prefix length). It defines how much of a network address that must match, in order to qualify for this route. Valid values are between 0 and 32 bits respectively 128 for IPv6 routes. Only a default route will have a mask length of 0 (as it will match anything).
Gateway	The IP address of the IP gateway. Valid format is dotted decimal notation or a valid IPv6 notation. Gateway and Network must be of the same type.
Next Hop VLAN (IPv6)	The VLAN ID (VID) of the specific IPv6 interface associated with the gateway. - The given VID ranges from 1 to 4095 and will be effective only when the corresponding IPv6 interface is valid. - If the IPv6 gateway address is link-local, it must specify the next hop VLAN for the gateway. - If the IPv6 gateway address is not link-local, system ignores the next hop VLAN for the gateway.
Distance	The distance value of the route entry is used to provide the priority information of the routing protocols to routers. When two or more different routing protocols are involved and have the same destination, the distance value can be used to select the best path.

2.1.3 SNMP

2.1.3.1 SNMP System

Simple **N**etwork **M**anagement **P**rotocol (**SNMP**) is a protocol for managing devices on IP networks**.** It exposes management data in the form of variables on the managed systems which describe the system configuration**.** These variables can then be queried or defined by the users. The SNMP is used by network management system or third-party software to monitor devices such as managed switches in a network to retrieve network status information and to configure network parameters. The Atop's managed switch support SNMP and can be configured in this section.

In this submenu, SNMP system can be configured as shown in Figure 2.10. There are two fields here: **Mode** and **Engine ID**. In **Mode**, users can select **Enabled/Disabled** from the dropdown list to enable SNMP mode operation. In **Engine ID**, it indicates the SNMPv3 engine ID. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users. The default setting is 80000eab030200c14df2e0.

Please click **Save** button for a change to take effect or **Reset** button to undo any changes made locally and revert to previously saved values.

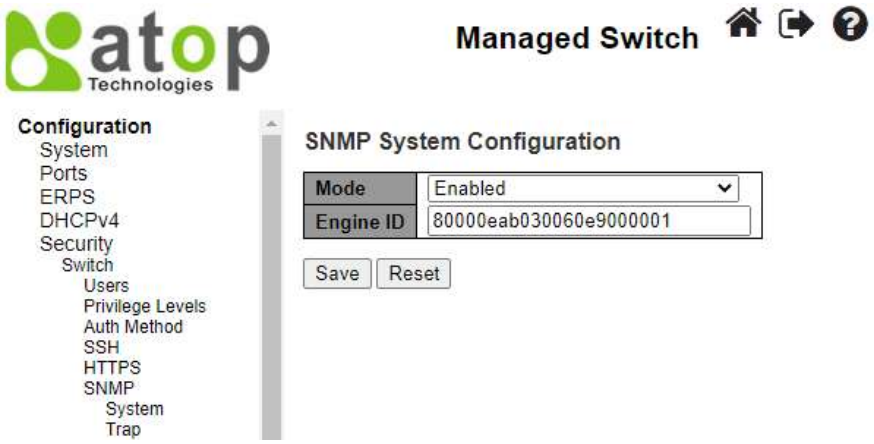


Figure 2.10 Webpage to Configure SNMP System

2.1.3.2 SNMP Trap Destinations

The managed switch provides a trap function that allows switch to send notification to agents with SNMP traps or inform. The notifications are based on the status changes of the switch such as link up, link down, warm start, and cold start. For inform mode, after sending SNMP inform requests, switch will resends inform request if it does not receive response within 10 seconds. The switch will try re-send three times. This option allows users to configure SNMP Trap Setting by setting the destination IP Address of the Trap server, Port Number of the Trap server, and SNMP version for authentication. Figure 2.11 shows these Trap Setting's options. Please click on the **Add New Entry** button to input new entry as shown in Figure 2.12. Table 2.5 summarizes the descriptions of trap destination settings. Please click on the **Save** button afterwards for a change to take effect, or **Reset** button to undo any changes made locally and revert to previously saved values.

Figure 2.11 Webpage to Configure SNMP Trap Destinations

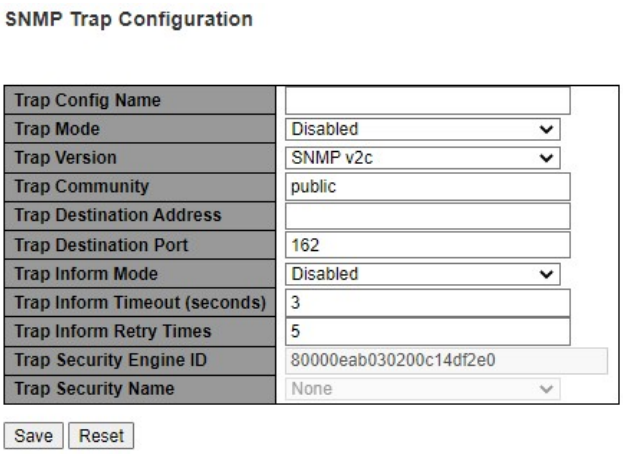


Figure 2.12 Adding New Entry to SNMP Trap Destination Table

Table 2.5 Descriptions of SNMP Trap Destination Configurations

Label	Description
Delete	Users are allowed to delete each entry separately.
Name	Indicates the trap Configuration's name. Indicates the trap destination's name.
Enable	Indicates the trap destination mode operation. Possible modes are: **Enabled:** Enable SNMP trap mode operation. **Disabled:** Disable SNMP trap mode operation.
Version	Indicates the SNMP trap supported version. Possible versions are: **SNMPv1:** Set SNMP trap supported version 1. **SNMPv2c**: Set SNMP trap supported version 2c. **SNMPv3**: Set SNMP trap supported version 3.

Label	Description
Destination Address	Indicates the SNMP trap destination address. It allows a valid IPv4 address in dotted decimal notation ('x.y.z.w'). It also allows a valid hostname. A valid hostname is a string drawn from the alphabet (A-Za-z), digits (0-9), dot (.), dash (-). Spaces are not allowed, the first character must be an alpha character, and the first and last characters must not be a dot or a dash. Indicates the SNMP trap destination IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can appear only once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
Destination Port	Indicates the SNMP trap destination port. SNMP Agent will send SNMP message via this port. The port range is 1~65535.

2.1.3.3 SNMP Trap Sources

This page provides **SNMP Trap Source configurations**. A trap is sent for the given trap source if at least one filter with filter type included matches the filter, and no filters with filter type excluded matches. Figure 2.13 shows the webpage when there is no entry in the trap source configurations. When users click on the Add New Entry button, the webpage will be updated to Figure 2.14. The users can select Name for trap source from the drop-down list and select the type from the second drop-down list. Then, enter the **Subset OID** in the text field. Click on the **Save** button to save the changes or click on the **Reset** button to undo any changes made locally and revert to previously saved values. Table 2.6 provides descriptions of the SNMP Trap Source Configurations.

Figure 2.13 Webpage to Configure SNMP Trap Sources

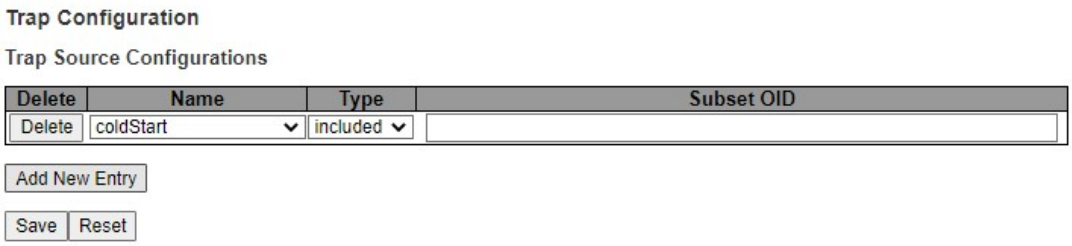


Figure 2.14 Adding New Entry to SNMP Trap Sources

Table 2.6 Description of SNMP Trap Source Configurations

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save. Users are allowed to delete each entry separately.
Name	Indicates the name for the entry. Selectable from the following list. - coldStart - warmStart - linkUp - linkDown - newRoot - topologyChange - psecTrapInterfaces
Type	The filter type for the entry. Possible types are: **included**: An optional flag to indicate a trap is sent for the given trap source is matched. **excluded**: An optional flag to indicate a trap is not sent for the given trap source is matched.
Subset OID	The subset OID for the entry. The value should depend on the what kind of trap name. For example, the ifIdex is the subset OID of linkUp and linkDown. A valid subset OID is one or more digital number (0-4294967295) or asterisk (*) which are separated by dots (.). The first character must not begin with asterisk (*) and the maximum of OID count must not exceed 128.

2.1.3.4 SNMP Communities

This submenu allows users to configure SNMP community table as shown in Figure 2.15. The entry index key is **Community.** This community string option allows the users to set a community string (**Community name** and **Community secret**) for authentication by adding new entry to the table. The users can remove existing community string from the list by clicking on the checkbox of **Delete** column at the beginning of each community string item**.** The users can specify the string names on the **Community Name** field by clicking **Add New Entry** button, as shown in Figure 2.16. Table 2.7 briefly provides descriptions of SNMP's community setting.

Please click on the **Save** button afterwards for a change to take effect, or click **Reset** button to undo any changes made locally and revert to previously saved values.

Typically, an SNMP agent, which is a network management software module residing on the managed switch, can access all objects with read-all-only permissions using the string *public*. Another setting example is that the string *private* has permission of read-write-all.

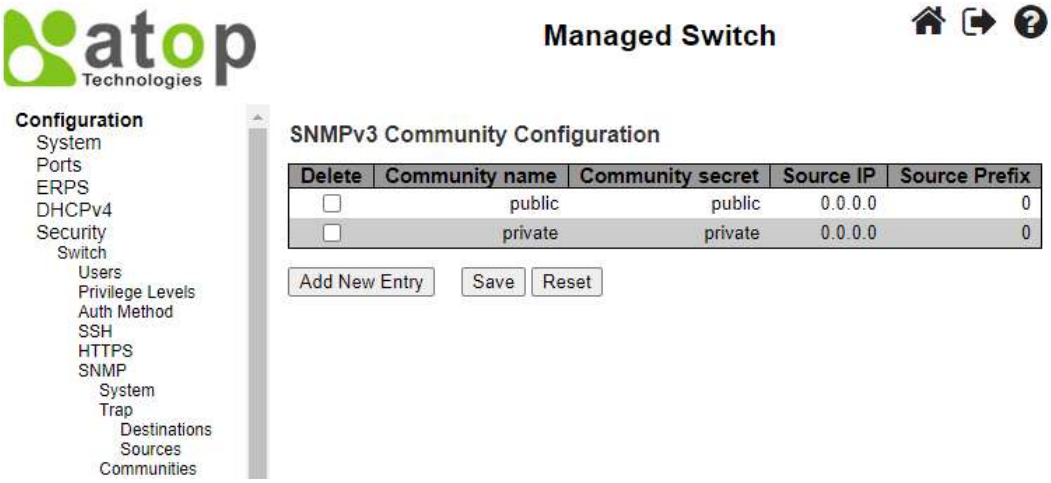


Figure 2.15 Webpage to Configure SNMP Communities

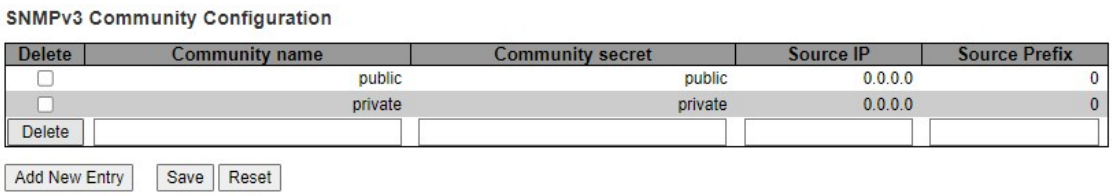


Figure 2.16 Adding New Entry to SNMP Community Configuration

Table 2.7 Descriptions of SNMP Community Configurations

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community Name	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and map a SNMPv1 or SNMPv2c community string.
Community Secret	Indicates the community secret (access string) to permit access using SNMPv1 and SNMPv2c to the SNMP agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
Source IP	Indicates the SNMP access source address. A particular range of source addresses can be used to restrict source subnet when combined with source mask.
Source Prefix	Indicates the SNMP access source address mask.

2.1.3.5 SNMP Users

This submenu allows users to configure SNMPv3 user table on this page. The entry index keys are **Engine ID** and **User Name**. As mentioned earlier, SNMPv3 is a more secure SNMP protocol than earlier versions. In this part, the users will be able to set a password and an encryption key to enhance the data security. When choosing this option, the users can configure SNMPv3's authentication and encryption. MD5 (Message-Digest algorithm 5) is used for authentication password and DES (Data Encryption Standard) is used for data encryption algorithm. Figure 2.17 shows the SNMPv3 Authentication Setting's options. The users can view existing SNMPv3 users' setting on the upper table where it provides information about user name, authentication type, and data encryption (or privacy protocol). The users have an option to remove existing SNMPv3 user by clicking on the **Delete** button under the **Delete** column of each entry. To add a new SNMPv3 user, the users have to click **Add New Entry** button, and enter **Engine ID**, **User Name**, **Security Level, Authentication Protocol**, **Authentication Password**, **Privacy Protocol**, and **Privacy Password**. The authentication password has the maximum length of 31 characters. Note that if no password is provided, there will be no authentication for SNMPv3. Table 2.8 lists the descriptions of SNMPv3 User settings.

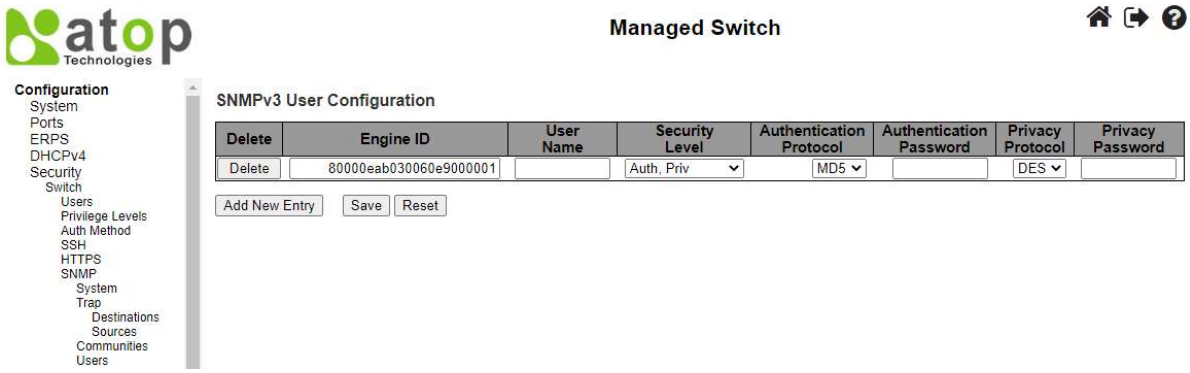


Figure 2.17 Webpage to Configure SNMP Users

Table 2.8 Descriptions of SNMP Users

Label	Description	Factory Default
Delete	Check to delete the entry. It will be deleted during the next save.	

Label	Description	Factory Default
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeros and all-'F's are not allowed. The SNMPv3 architecture uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. For the USM entry, the usmUserEngineID and usmUserName are the entry's keys. In a simple agent, usmUserEngineID is always that agent's own snmpEngineID value. The value can also take the value of the snmpEngineID of a remote SNMP engine with which this user can communicate. In other words, if user engine ID equal system engine ID then it is a local user; otherwise it is a remote user.	Follow DUT's MAC address to create Engine ID
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.	
Security Level	Indicates the security model that this entry should belong to. Possible security models are: **NoAuth, NoPriv**: No authentication and no privacy. **Auth, NoPriv**: Authentication and no privacy. **Auth, Priv**: Authentication and privacy. The value of security level cannot be modified if entry already exists. That means it must first be ensured that the value is set correctly.	Auth, Priv
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are: **None**: No authentication protocol. **MD5**: An optional flag to indicate that this user uses MD5 authentication protocol. **SHA**: An optional flag to indicate that this user uses SHA authentication protocol. The value of security level cannot be modified if entry already exists. That means must first ensure that the value is set correctly.	MD5
Authentication Password	A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. The allowed content is ASCII characters from 33 to 126.	Null
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are: **None**: No privacy protocol. **DES**: An optional flag to indicate that this user uses DES authentication protocol. **AES**: An optional flag to indicate that this user uses AES authentication protocol.	DES
Privacy Password	A string identifying the privacy password phrase. The allowed string length is 8 to 32, and the allowed content is ASCII characters from 33 to 126.	Null

2.1.3.6 SNMP Groups

Figure 2.18 shows SNMPv3 Group Configuration webpage. It contains SNMPv3 group table. The entry index keys are **Security Model** and **Security Name**. Click **Add New Entry** button to add a new group entry to the table. Table 2.9 describes the column labels of the SNMPv3 group table.

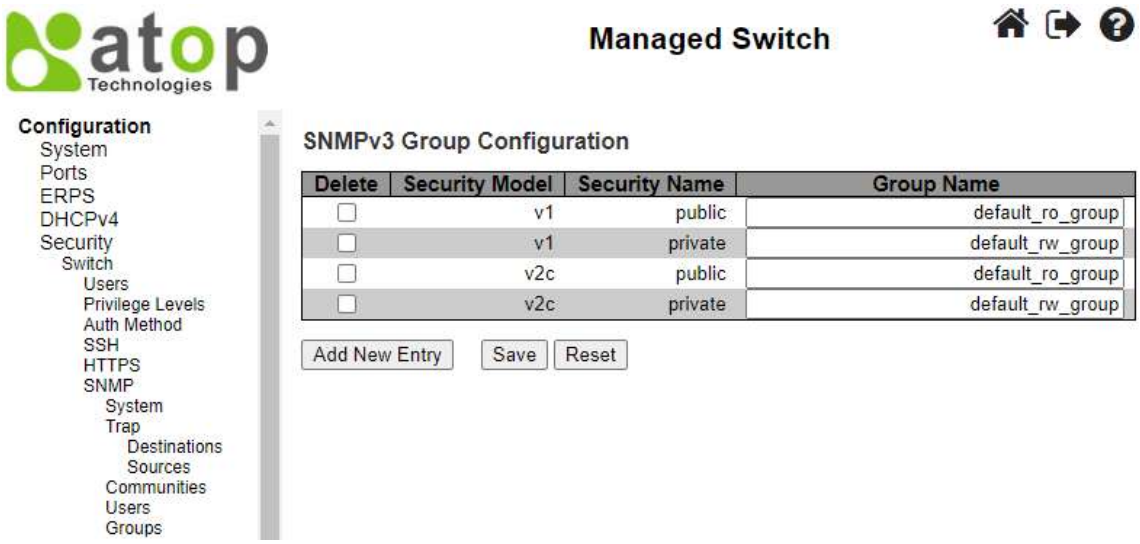


Figure 2.18 Webpage to Configure SNMP Groups

Table 2.9 Descriptions of SNMP Groups

Label	Description	Factory Default
Delete	Check to delete the entry. It will be deleted during the next save.	
Security Model	Indicates the security model that this entry should belong to. Possible security models are: **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: SNMPv3, User-based Security Model (USM).	V1
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.	public
Group Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.	Null

2.1.3.7 SNMP Views

Figure 2.19 shows SNMPv3 View Configuration webpage. It contains SNMPv3 view table. The entry index keys are **View Name** and **OID Subtree**. Click **Add New Entry** button to add a new view entry to the table. Table 2.10 describes the column labels of the SNMPv3 view table. Please click on the **Save** button afterwards for a change to take effect, or click **Reset** button to undo any changes made locally and revert to previously saved values.

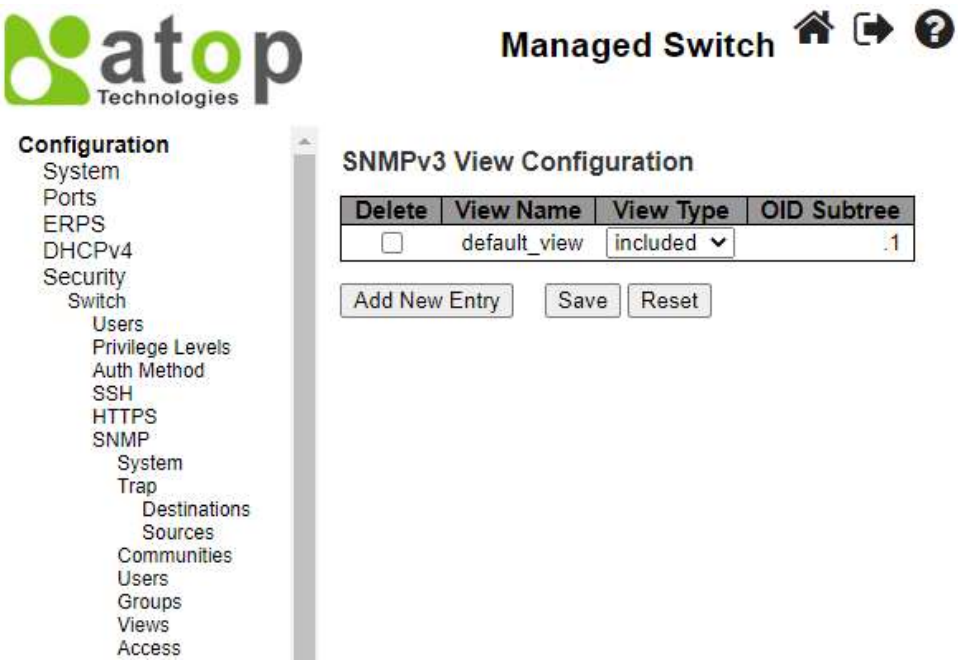


Figure 2.19 Webpage to Configure SNMP Views

Table 2.10 Descriptions of SNMP Views

Label	Description	Factory Default
Delete	Check to delete the entry. It will be deleted during the next save.	
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.	Null
View Type	Indicates the view type that this entry should belong to. Possible view types are: **included**: An optional flag to indicate that this view subtree should be included. **excluded**: An optional flag to indicate that this view subtree should be excluded. In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and it's OID subtree should overstep the 'excluded' view entry.	included
OID Subtree	The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).	Null

2.1.3.8 SNMP Access

Figure 2.20 shows SNMPv3 Access Configuration webpage. It contains SNMPv3 access table. The entry index keys are **Group Name**, **Security Model** and **Security Level**. Click **Add New Entry** button to add a new access entry to the table. Table 2.11 describes the column labels of the SNMPv3 access table. Please click on the **Save** button afterwards for a change to take effect, or click **Reset** button to undo any changes made locally and revert to previously saved values.

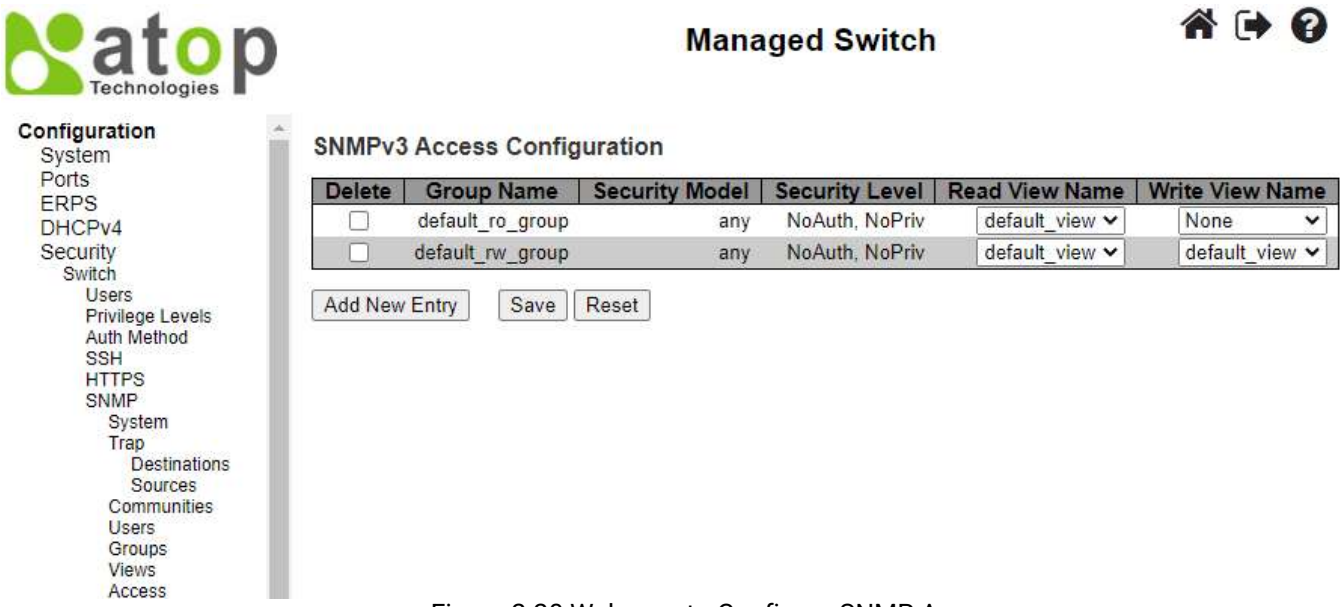


Figure 2.20 Webpage to Configure SNMP Access

Table 2.11 Descriptions of SNMP Access Configuration

Label	Description	Factory Default
Delete	Check to delete the entry. It will be deleted during the next save.	
Group Name	A string identifying the group name that this entry should belong to.	Default_ro_group
Security Model	Indicates the security model that this entry should belong to. Possible security models are: **any**: Any security model accepted(v1|v2c|usm). **v1**: Reserved for SNMPv1. **v2c**: Reserved for SNMPv2c. **usm**: SNMPv3, User-based Security Model (USM).	any
Security Level	Indicates the security model that this entry should belong to. Possible security models are: **NoAuth, NoPriv**: No authentication and no privacy. **Auth, NoPriv**: Authentication and no privacy. **Auth, Priv**: Authentication and privacy.	NoAuth, NoPriv
Read View Name	The name of the MIB view defining the MIB objects for which this request may request the current values.	None
Write View Name	The name of the MIB view defining the MIB objects for which this request may potentially set new values.	None

2.1.4 NTP

Atop's industrial managed switch has internal calendar (date) and clock (or system time) which can be set manually or automatically. Figure 2.21 shows the Network Time Protocol (**NTP**) configuration webpage. Here, users can automatically set the device's time by first selecting **Enabled** from the drop-down menu of **Mode** field. Then, users must enter the IP or Domain address of up to the total of five NTP servers: Server1, Server2, Server3, Server4, and Server 5. This allows the device to synchronise date and time with one of the NTP server. First, it will be synchronized with the Server 1. If it failed to respond, the device will select the second priority server or Server 2 to synchronize time with. If the Server 2 failed to respond, the device will then contact the third priority server or Server 3. This goes on until the device gets the respond from the NTP server, or none of them is respond. If any field is NULL, the device will not contact that server and continue contacting other lower priority servers instead.

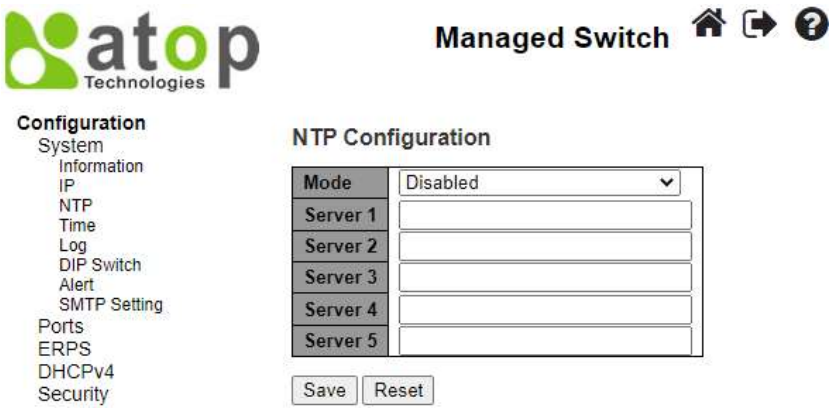


Figure 2.21 Webpage to Configure System NTP

The detailed description of each field is provided in Table 2.12.

Table 2.12 Descriptions of the NTP Settings

Label	Description	Factory Default
Mode	Select to enable or disable an automatically setting of the device time. This option will disable or enable network time protocol (NTP) daemon inside the managed switch which allows this managed device to synchronize its clock with other NTP servers.	Disabled
Server 1	Sets the first IP or Domain address of **NTP Server**; e.g., time.nist.gov.	NULL
Server 2	Sets the second IP or Domain address of NTP Server. Switch will locate the 2nd **NTP Server** if the 1st NTP Server fails to connect; e.g., time-A.timefreq.bldrdoc.gov	NULL
Server 3	Sets the third IP or Domain address of NTP Server. Switch will locate the 3rd **NTP Server** if the 2nd NTP Server fails to connect.	NULL
Server 4	Sets the fourth IP or Domain address of NTP Server. Switch will locate the 4th **NTP Server** if the 3rd NTP Server fails to connect.	NULL
Server 5	Sets the fifth IP or Domain address of NTP Server. Switch will locate the 5th **NTP Server** if the 4th NTP Server fails to connect.	NULL

2.1.5 Time

This **Time** webpage allows the user to configure the time zone and daylight saving for the managed switch. There are three setting parts within this webpage: **System Time Configuration, Time Zone Configuration**, and **Daylight Saving Time Configuration**.

The first part : **System Time Configuration,** users are allowed to set the device's system time by manual. Table 2.6 summarizes the descriptions of options in system time configuration

The second part : **Time Zone Configuration**, users are allowed to set the device's time zone. By clicking the drop-down list of **Time Zone** field, users can select the device's local time zone or **Manual Setting** option. In the **Hours** and **Minutes** fields, users can enter the number of hours and minutes of the device's time that is offset from the local time zone when users selected **Manual Setting** option. Table 2.7 summarizes the descriptions of options in time zone configuration.

The third part : **Daylight-Saving Time Configuration**, if the switch is deployed in a region where daylight saving time is practiced (see note below for explanation), please select the **Recurring** or **Non-Recurring** options for **Daylight Saving Time** field within the **Daylight-Saving Time Configuration** box. Then, users will have to enter the **Start Time settings, End Time settings**, and **Offset settings** in minute(s). Note that the **Start Time settings** and **End Time**

setting will be different between the **Recurring** and **Non-Recurring** options. Recurring option means that the configuration of daylight saving will be repeated very year. On the other hand, non-recurring option means that the daylight saving will be repeated only on the specified years. Table 2.8 summarizes the descriptions of options in daylight saving time configuration.

Note:

- Daylight Saving Time: In certain regions (e.g., US), local time is adjusted during the summer season in order to provide an extra hour of daylight in the afternoon, and one hour is usually shifted forward or backward.

- NTP: **N**etwork **T**ime **P**rotocol is used to synchronize the computer systems' clocks with a standard NTP server: Examples of two NTP servers are *time.nist.gov* and *time-A.timefreq.bldrdoc.gov*.

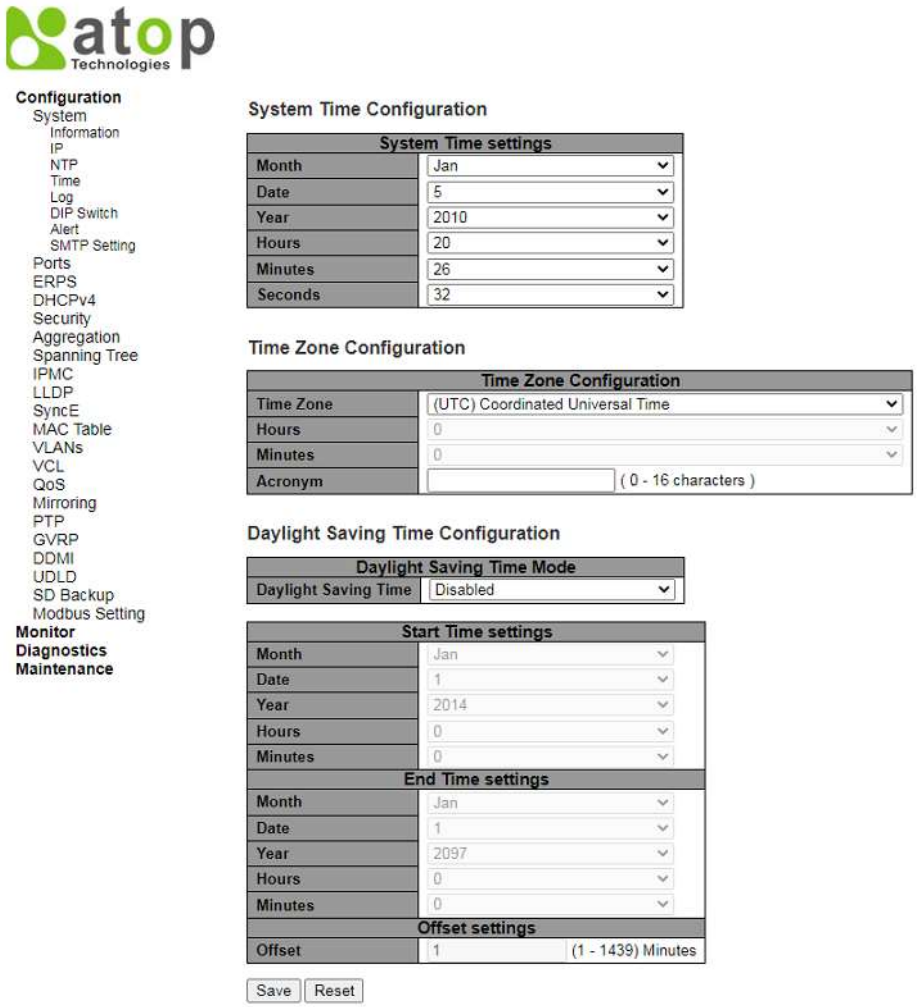


Figure 2.22 Webpage to Configure System Time

Table 2.13 Description of System Time Configuration

Label	Description
Month	Select the month of system time
Date	Select the date of system time
Year	Select the year of system time
Hours	Select the starting hour of system time
Minutes	Select the starting minute of system time
Seconds	Select the starting second of system time

Table 2.14 Description of Time Zone Configuration

Label	Description
Time Zone	Lists various **Time Zones** worldwide. Select appropriate Time Zone from the drop down and click Save to set. The **'Manual Setting'** options is used for the specific time zone which is excluded from the options list.
Hours	Number of hours offset from UTC. The field only available when **Time Zone** is set to **Manual Setting**.
Minutes	Number of minutes offset from UTC. The field only available when **Time Zone** is set to **Manual Setting.**
Acronym	User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 characters) Notice the string '' is a special syntax that is reserved for null input.

Table 2.15 Description of Daylight-Saving Time Configuration

Label	Description
Daylight Saving Time	This is used to set the clock forward or backward according to the configurations set below for a defined Daylight-Saving Time duration. - Select '**Disable**' to disable the Daylight-Saving Time configuration. - Select '**Recurring**' and configure the Daylight-Saving Time duration to repeat the configuration every year. - Select **'Non-Recurring**' and configure the Daylight-Saving Time duration for single time configuration. (Default: Disabled)
Recurring Configuration	
Start Time settings	**Week** - Select the starting week number. **Day** - Select the starting day. **Month** - Select the starting month. **Hours** - Select the starting hour. **Minutes** - Select the starting minute.
End time settings	**Week** - Select the ending week number. **Day** - Select the ending day. **Month** - Select the ending month. **Hours** - Select the ending hour. **Minutes** - Select the ending minute.
Offset settings	**Offset** - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439)
Non-Recurring Configuration	
Start Time settings	**Month** - Select the starting month. **Date** - Select the starting date. **Year** - Select the starting year. **Hours** - Select the starting hour. **Minutes** - Select the starting minute.
End Time settings	**Month** - Select the ending month. **Date** - Select the ending date. **Year** - Select the ending year. **Hours** - Select the ending hour. **Minutes** - Select the ending minute.
Offset settings	**Offset** - Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1439)

2.1.6 Log

Figure 2.23 shows **System Log configuration** setting webpage. System Log or syslog keeps records of messages or events that are related to the overall functionalities of the managed switch. Here the users can enable how the log will be delivered to other system. It can be sent to a remote log server. Select **Enabled** from the drop-down list

of the **Server Mode** field if users want the system log to be saved in the remote log server, or select **Disabled** to disable server mode operation.
The users need to select the log level and provide the IP address of a remote log server. Please click on the **Save** button after finishing the setup or **Reset** button to disregard all changes made locally and revert to previously saved values. Table 2.16 describes the details of parameters setting for the system log. Type of syslog level include: Error, Warning, Notice, and Informational.
Enable **Log History** to sotre the log in the local disk.

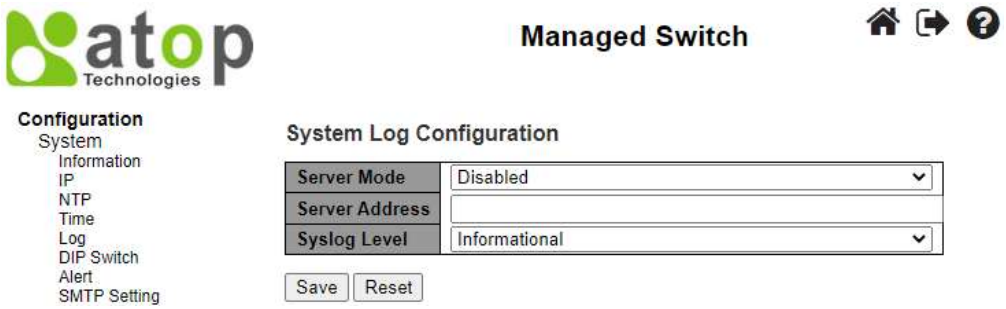


Figure 2.23 Webpage to Configure System Log

Table 2.16 Descriptions of the System Zone Configuration

Field	Detailed description of mode	Default value
Server Mode	Indicates the server mode operation. When the mode operation is enabled, the syslog message will send out to syslog server. The syslog protocol is based on UDP communication and received on UDP port 514 and the syslog server will not send acknowledgments back sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always send out even if the syslog server does not exist. Possible modes are: **Enabled**: Enable server mode operation. **Disabled**: Disable server mode operation.	Disabled
Server Address	Indicates the IPv4 host address of syslog server. If the switch provides DNS feature, it also can be a domain name.	NULL
Syslog Level	Indicates what kind of message will send to syslog server. Possible modes are: - **Error**: Send the specific messages which severity code is less or equal than Error (3). - **Warning**: Send the specific messages which severity code is less or equal than Warning (4). - **Notice**: Send the specific messages which severity code is less or equal than Notice (5). - **Informational**: Send the specific messages which severity code is less or equal than Informational (6).	Informational

2.1.7 Alert

This webpage allows the users to configure how each type of the power status alarm events will be sent or notify the users. Power Status Alarms keep track of power status of the switch based on the available input connectors.

RHG9728 supports two to three power sources. In the example, **Power1**, **Power2** and **Power 3** are illustrated as shown in Figure 2.24**.** Users can enable a notification of each power source separately. Also, they can get notifications through many methods including **Relay**, **Alarm LED**, and **E-mail** by selecting **Enabled** in any of these fields. Click **Save** button to let the setting take effect, or click **Reset** button to change back to the previously saved values.

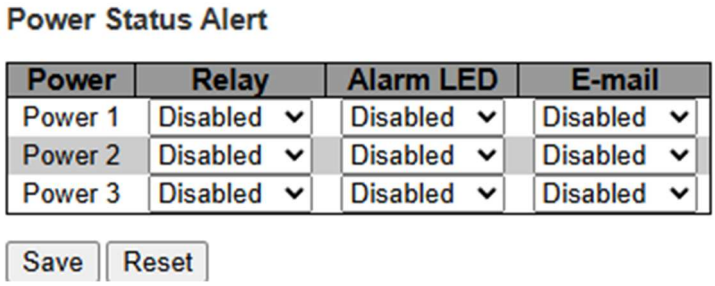


Figure 2.24 Webpage to Configure System Alert

Table 2.17 summarizes the Power Status Alarm event selection.

Table 2.17 Descriptions of Power Status Alarm Event Selection

Label	Description	Factory Default
Power	Indicate specific power supply such as Power 1 and Power 2	-
Relay	Options: Disabled, Power On, or Power Off	Disabled
Alarm LED	Options: Disabled, Power On, or Power Off	Disabled
E-mail	Options: Disabled, Power On, or Power Off	Disabled

2.1.8 SMTP Setting

Simple **M**ail **T**ransfer **P**rotocol (**SMTP**) is an internet standard for e-mail transmission across IP networks. In case any warning events occur, the system can send an alarm message (e.g., Link Status and System Log) to users by e-mail. As shown in Figure 2.25, users can enable/disable server's authentication, input user name and password if enabled, and edit email address of the sender and four recipients. The total of four recipients are allowed to receive an e-mail.

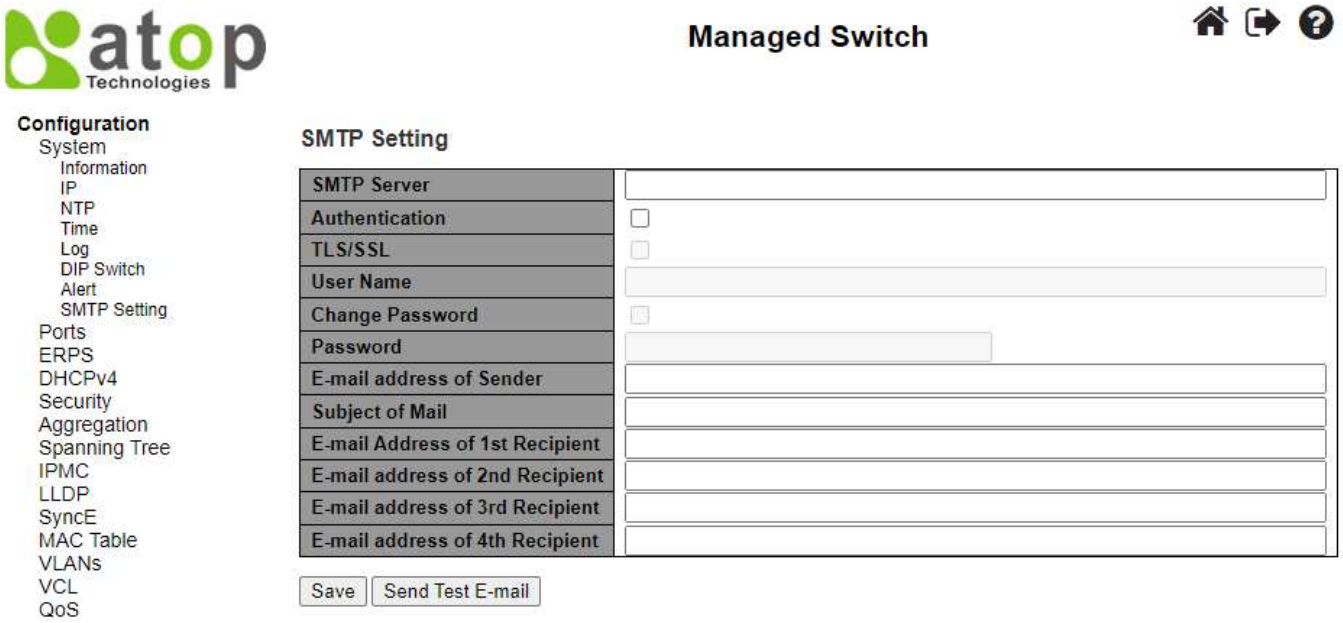


Figure 2.25 Webpage to Configure System SMTP Setting

An example of SMTP Setting is shown in Figure 2.26. When users select the box behind the **Authentication** field, **TLS** field as well as **User Name** and **Change Password** fields are enabled. Users can configure e-mail address of sender, so that the recipient can reply back to the correct person in charge. Also, users can configure the subject of email, so that it can be easily distinguishable from the other e-mails. At last, users can edit e-mail addresses of all four recipients in the order shown in the e-mail. After entering all the necessary fields, please click on the **Save**

button to allow the setting to take effect. Note that users can test sending an e-mail by simply clicking on the **Send Test E-mail** button. The description of each SMTP Setting parameter is summarized in Table 2.18.

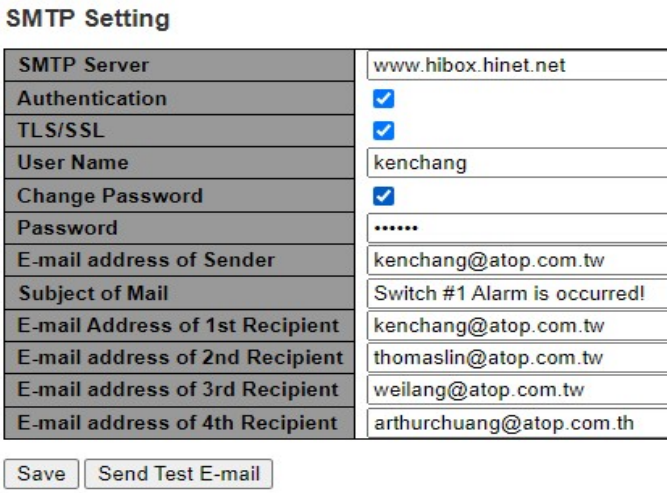


Figure 2.26 Example of SMTP Setting

Table 2.18 Descriptions of SMTP Setting

Label	Description	Factory Default
SMTP Server	Configure the IP address of an out-going e-mail server	NULL
Authentication	By checking on the box, users Enable or disable an authentication login. If enabled, users need an authentication to access the SMTP server. Thus, the users will also need to setup User Name and Password to connect to the SMTP server	Disable (Unchecked)
TLS/SSL	Enable or disable Transport Layer Security (TLS)/ Secure Sockets Layer (SSL) which is an encryption mechanism for communication with the SMTP Server	Disable (Unchecked)
User Name	Set the username (or account name) to login for authentication. Max. 31 characters.	NULL
Change Password	Enable the checkbox if user need to set or change account password. If the checkbox is disabled, the account password will remain the old one. (If the password has not be set before, it will be NULL)	Disable (Unchecked)
Password	Set the account password for login/authentication. Max. 31 characters.	NULL
E-mail Address of Sender	Configure the sender e-mail address	NULL
Subject of Mail	Type the subject of this warning message. Max. 63 characters.	NULL
E-mail Address of 1st Recipient	Set the first receiver's E-mail address.	NULL
E-mail Address of 2nd Recipient	Set the second receiver's E-mail address.	NULL
E-mail Address of 3rd Recipient	Set the third receiver's E-mail address.	NULL
E-mail Address of 4th Recipient	Set the fourth receiver's E-mail address.	NULL
Save	Save these modifications on the managed switch	-
Send Test E-mail	Send a test email to recipient(s) above to check accuracy.	-

2.1.9 AgentClient

The AgentClient is used by Atop Network Management Software (NIMBL). To allow the RHG9728 to be managed by NIMBL, this function must be enabled. The default setting is **Disabled**.

2.2 Ports

Port Setting webpage is shown in Figure 2.27. The users can check the state of each port through **Link** column. Red color means port is down while green color means port is up. Users can also check the **Warning** status of the port. In the speed column, users can check the **Current** speed and configure a new speed through **Configured** column. The possible physical layer connections of each port are listed on the **Adv Duplex** and **Adv speed** column. The port's duplexing (**Duplex**) can be either **Full** duplex (**Fdx**) or **Half** duplex (**Hdx**). The **Half duplex** option allows one-way communication at a time, while the **Full duplex** option allows simultaneous two-way communication. The transmission **Speed** of each port can be chosen from the dropdown list which could be **10**, **100**, and **1000** Mbps.

On the next column, user can select to enable/disable **Flow Control** for each port. The Flow Control mechanism can be enabled to avoid packet loss when congestion occurs. Within this column, there are **Curr Rx** and **Curr Tx** sub-columns, where users can check the status of flow control on the receiving and transmitting link, respectively.

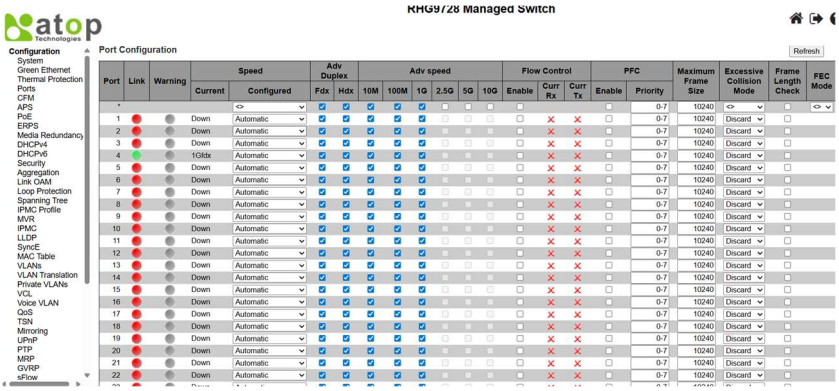


Figure 2.27 Webpage to Configure Ports of RHG9728

Table 2.19 Descriptions of Port Configuration

Field Label	Subfield Label	Description	Factory Default
Port		Indicate port number. e.g., ranging from 1 to 11. In the first row, port * will show all possible configurable options for the device.	-
Link		Show link status. Red colour for port down, and green colour for port up.	-
Warning		Indicate a warning when there is a problem with the port. Different colours are used to indicate the severity of port problem. : No warnings : There are warnings, use tooltip to see.	Grey colour
Speed	**Current**	Show current speed of the port. e.g., 100 fdx for 100 Mbps full duplex. If port is currently down, this field will show "down".	-
	Configured	Selects any available link speed for the given switch port. Only speeds supported by the specific port is shown. Possible speeds are: - **Disabled** - Disables the switch port operation. - **Automatic** - Port auto negotiating speed and duplex with the link partner and selects the highest speed that is compatible with the link partner.	Automatic

Field Label	Subfield Label	Description	Factory Default
		- **10Mbps HDX** - Forces the port in 10Mbps half-duplex mode. - **10Mbps FDX** - Forces the port in 10Mbps full duplex mode. - **100Mbps HDX** - Forces the port in 100Mbps half-duplex mode. - **100Mbps FDX** - Forces the port in 100Mbps full duplex mode. - **1Gbps FDX** - Forces the port in 1Gbps full duplex - **2.5Gbps FDX** - Forces the port in 2.5Gbps full duplex	
Adv Duplex	When duplex is set as auto i.e. auto negotiation, the port will only advertise the specified duplex as either Fdx or Hdx to the link partner. By default, port will advertise all the supported duplexes if the Duplex is Auto.		
	Fdx	Full duplex mode of the link. Click a checkbox to enable the option.	-
	Hdx	Half-duplex mode of the link. Click a checkbox to enable the option.	-
Adv Speed	When Speed is set as auto i.e. auto negotiation, the port will only advertise the specified speeds (10M, 100M, 1G) to the link partner. By default, port will advertise all the supported speeds if speed is set as Auto.		
	10M	Click to enable 10 Mbps link speed for this port.	-
	100M	Click to enable 100 Mbps link speed for this port.	-
	1G	Click to enable 1 Gbps link speed for this port.	-
Flow Control	When Auto Speed is selected on a port, this section indicates the flow control capability that is advertised to the link partner. When a fixed-speed setting is selected, that is what is used. The Current Rx column indicates whether pause frames on the port are obeyed, and the Current Tx column indicates whether pause frames on the port are transmitted. The Rx and Tx settings are determined by the result of the last Auto Negotiation. Check the configured column to use flow control. This setting is related to the setting for Configured Link Speed. NOTICE: The 100FX standard does not support Auto Negotiation, so when in 100FX mode the flow control capabilities will always be shown as "disabled"		
	Enable	The Flow Control mechanism can be enabled to avoid packet loss when congestion occurs.	
	Curr Rx	Symbol √ for showing that flow control is active on the receiving traffic. Symbol ✕ for showing that flow control is not active on the receiving traffic.	✕
	Curr Tx	Symbol √ for showing that flow control is active on the transmitting traffic. Symbol ✕ for showing that flow control is not active on the transmitting traffic.	✕

2.3 ERPS

Ethernet **R**ing **P**rotection **S**witching (**ERPS**) is a protocol for Ethernet layer network rings. The protocol specifies the protection mechanism for sub-50 ms delay time. ERPS provides highly reliable and stable protection in the ring topology, and it never forms loops, which can affect network operation and service availability. Figure 2.28 depicts an example of ring topology forming by four Atop's managed switch series.

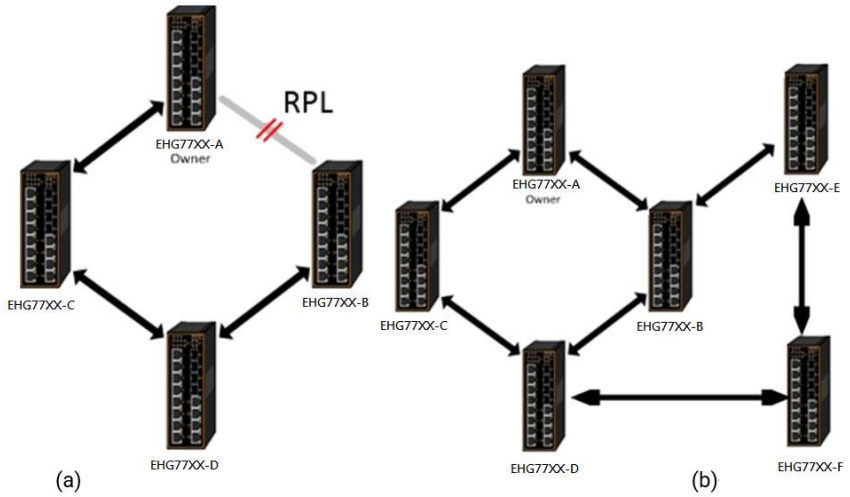


Figure 2.28 An Example of Ring Topology (a) Major Ring, and (b) Sub-Ring

An ERPS ring consists of interconnected Layer 2 switching devices configured with the same control VLAN. An ERPS ring can be a major ring or a sub-ring, as shown in Figure 2.28. By default, an ERPS ring is a major ring. The **major ring** is a closed ring, whereas a **sub-ring** is a non-closed ring. The major ring and sub-ring can be configured through **type** field. On the network shown in Figure 2.28, switch RHG9728-A to RHG9728-C via RHG9728-B and RHG9728-D constitute a major ring, and switch RHG9728-E through switch RHG9728-F constitute a sub-ring.

In the Ethernet ring, loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any time. This particular link is called **Ring Protection Link (RPL)**. A control message called **Ring Automatic Protection Switch (R-APS)** coordinates the activities of switching on/off the RPL. Under normal conditions, this link is blocked by the designated Ethernet Ring Node called **RPL Owner Node** to ensure that there is no loop formed for the Ethernet traffic. The node at the other end of the RPL is known as **RPL Neighbor Node**. In case an Ethernet ring failure occurs, the RPL Owner Node will be responsible for unblocking its end of the RPL to allow RPL to be used as a backup link. The RPL is the backup link when one link failure occurs. Other ring ports called common port will help monitoring the status of the directly connected ERPS link and send RAPS PDUs to notify the other ports of its link status changes.

In case that users do not want their clients to detect the fault and would like sometimes to rectify the problem, users may use the Holdoff timer. If the fault occurs, the fault is not immediately sent to ERPS until the **Holdoff timer** expires.

If an RPL owner port is unblocked due to a link or node recovery after its faulty, the involved port may not be changed to Up state immediately since it may cause network flapping. To prevent this problem, in **revertive** switching, the node where the RPL owner port resides starts the **wait to restore (WTR) timer** after receiving a **RAPS No Request (NR)** message. If the node receives a **RAPS Signal Fail (SF)** message before the timer expires, it will terminate the WTR timer. Otherwise, the RPL owner will block its own port, and send out RAPS (no request or NR, root blocked or RB) messages to inform the other nodes of the link or node recovery and starts the **Guard timer**. Before the Guard timer expires, other nodes do not process any RAPS (NR) messages to avoid receiving out-of-date RAPS (NR) messages. After the **Guard timer** expires, if the other nodes still receive RAPS (NR) messages, the nodes set their recovered ports on the ring to the Forwarding state. In **non-revertive** switching, the WTR timer is not started, and the original faulty link is still blocked. **ERPSv1** supports only revertive switching. **ERPSv2** supports both revertive and non-revertive switching.

Control messages of each ERPS ring (e.g., R-APS PDUs) are transmitted through a configuration of **a control VLAN**. For an ERPS ring that is already configured a control VLAN, when users add a port to the ERPS ring, the port is automatically added to the control VLAN. Different ERPS rings cannot be configured with the same control VLAN ID. The control VLAN must be mapped to an **Ethernet Ring Protection (ERP) instance**, so that ERPS forwards or blocks the VLAN packets based on blocking rules, protecting the ring network from broadcast storms.

Figure 2.29 shows the ERPS Configuration webpage. And Table 2.14 summarizes the descriptions of columns in EPRS Configuration's table.

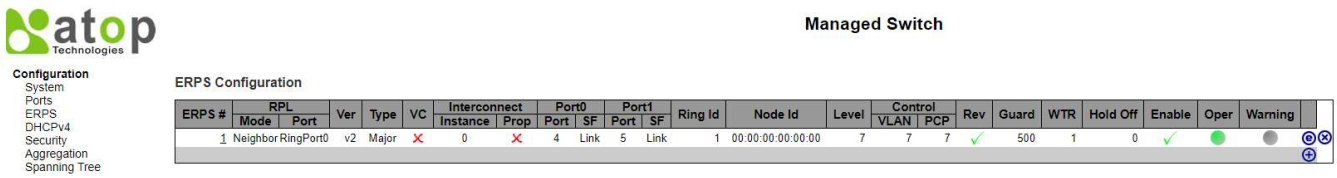


Figure 2.29 Webpage to Configure ERPS

Table 2.20 Description of EPRS Configuration Table

Label	Description
ERPS #	The ID of ERPS. Valid range 1 - 64.
RPL Mode	Ring Protection Link mode. Possible values: Ring Protection Link mode. Possible values: **None:** This switch doesn't have the RPL port in the ring. **Owner:** This switch doesn't have the RPL port in the ring. **Neighbor:** This switch is RPL neighbor for the ring.
RPL Port	Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is **None**.
Ver	ERPS protocol version. **v1** and **v2** are supported.
Type	Type of ring. Possible values: **Major:** ERPS major ring (G.8001-2016, clause 3.2.39) **Sub:** ERPS sub-ring (G.8001-2016, clause 3.2.66) **InterSub:** ERPS sub-ring on an interconnection node (G.8001-2016, clause 3.2.66)
VC	Controls whether to use a Virtual Channel with a sub-ring.
Interconnect Instance	For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected.
Interconnect Prop	Controls whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes.
Port0/Port1 Interface	Interface index of ring protection Port0/Port1.
Port0/Port1 SF	Selects whether Signal Fail (SF) comes from the link state of a given interface, or from a Down-MEP. Possible values: **MEP**: Down-MEP **Link**: Link
Ring Id	The Ring ID is used - along with the control VLAN - to identify R-APS PDUs as belonging to a particular ring.
Node Id	The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring.
Level	MD/MEG Level of R-APS PDUs we transmit.
Control VLAN	The VLAN on which R-APS PDUs are transmitted and received on the ring ports.
Control PCP	The PCP value used in the VLAN tag of the R-APS PDUs.
Rev	Revertive (true) or Non-revertive (false) mode.
Guard	Guard time in ms. Valid range is 10 - 2000 ms.
WTR	Wait-to-Restore time (WTR) in seconds. Valid range 1 - 720 sec.
Hold Off	Hold off time in ms. Value is rounded down to 100ms precision. Valid range is 0 - 10000 ms.
Enable	The administrative state of this APS ERPS. Check to make it function normally and uncheck to make it cease functioning.
Oper	The operational state of ERPS instance. ●: Active ●: Disabled or Internal error.
Warning	Operational warnings of ERPS instance. ●: No warnings ●: There are warnings, use tooltip to see.

Please click ⊕ to start configuring the ERPS. After clicking the ⊕, Figure 2.30 below will be appeared.

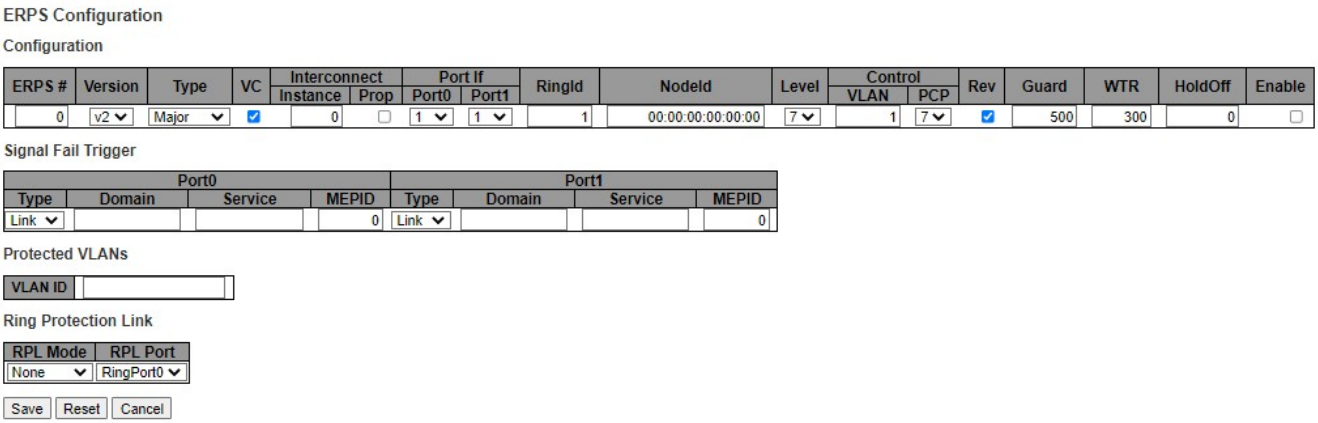


Figure 2.30 After Clicking ⊕ to Configure ERPS

Table 2.21 shows the descriptions of each field and subfields in the ERPs configuration webpage in details.

Table 2.21 Descriptions of ERPS Configuration Webpage

Field Label	Subfield Label	Description	Factory Default
ERPS #		Configure ERPS number to indicate a ring. Ranging from 1 to 64.	0
Version		Indicate the version that ERPS protocol is using. Two options are available: v1 and v2.	V2
Type		Indicate type of ERPS ring. There are three options: Major, Sub, Intersub.	Major
VC		Controls whether to use a Virtual Channel with a sub-ring. The Virtual Channel that's used to pass through R-APS message packet of sub-ring. User must add control VLAN of sub-ring to each ring ports of Major-ring. If selected, the virtual channel is enabled.	Clicked
Interconnect	**Instance**	For a sub-ring on an interconnection node, this must reference the instance ID of the ring to which this sub-ring is connected. Ethernet Ring Protection (ERP) Instance to forwards or blocks the VLAN packets based on blocking rules.	0
	Prop	Controls whether the ring referenced by Interconnect Instance shall propagate R-APS flush PDUs whenever this sub-ring's topology changes.	Unclicked
Port If	**Port0**	Select which port on the managed switch will be on Ring Port0. Ranging from 1 to maximum number of ports.	1
	Port1	Select which port on the managed switch will be on Ring Port1. Ranging from 1 to maximum number of ports.	1
RingId		Indicate ring identification number, ranging from 1 to 9999. The Ring ID is used - along with the control VLAN - to identify R-APS PDUs as belonging to a particular ring.	1
NodeId		The Node ID is used inside the R-APS specific PDU to uniquely identify this node (switch) on the ring. Enter a MAC address manually.	00:00:00:00:00:00
Level		MD/MEG Level of R-APS PDUs we transmit. Ranging from 0 to 7.	7
Control	**VLAN**	The VLAN on which R-APS PDUs are transmitted and received on the ring ports. Specify the virtual local area network that this static MAC belongs to, ranging from 1 to 4096.	1
	PCP	The PCP value used in the VLAN tag of the R-APS PDUs. Priority Code Point within the Ethernet frame header. PCP 0 is the lowest priority and 7 is the highest priority.	7

Field Label	Subfield Label	Description	Factory Default
Rev		Revertive (true) or Non-revertive (false) mode. Click/Unclick to enable the revertive/non-revertive switching.	Clicked
Guard		Set the guard time of the ring. Range is from 10 to 2000 ms	500
WTR		Set the wait-to-restore (WTR) time of the ring in seconds. Lower value has lower protection time. Range of the WTR Timer is from 1 to 720 seconds.	300
HoldOff		Set the holdoff time of the ring. Range is from 0 to 10000 ms	0
Enable		The administrative state of this ERPS. Check to make it function normally and uncheck to make it cease functioning.	Unclicked
VLAN ID		Indicate Identification number of VLAN (Virtual Local Area Network). VLANs which are protected by this ring instance. At least one VLAN must be protected. Specify as a comma separated list of vlan numbers or vlan ranges. Ex.: 1,4,7,30-70.	NULL
RPL Mode		There are three types of Ring Protection Link (RPL0 mode: None, Owner, Neighbour where: • None is RPL common port. This switch doesn't have the RPL port in the ring • Owner is RPL owner port. This switch is RPL owner for the ring. • Neighbour is RPL neighbour port (only in ERPSv2). This switch is RPL neighbour for the ring	None
RPL Port		Indicates whether it is port0 or port1 that is the Ring Protection Link. Not used if RPL Mode is **None**.	RingPort0

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values. Click **Cancel** button to return to the previous page; any changes made locally will be undone.

2.4 Media Redundancy Protocol

Media Redundancy Protocol (MRP) is an Ethernet redundancy protocol defined in IEC 62439-2. It is commonly used in industrial networks to ensure high availability and fast network recovery in ring topologies. MRP allows network devices to be connected in a ring structure while preventing network loops during normal operation. One device in the ring is designated as the MRP Manager, and the others operate as MRP Clients. Under normal conditions, the Manager blocks one ring port to maintain a loop-free topology. If a link failure or device failure occurs within the ring, MRP quickly reconfigures the network by unblocking the previously blocked port.

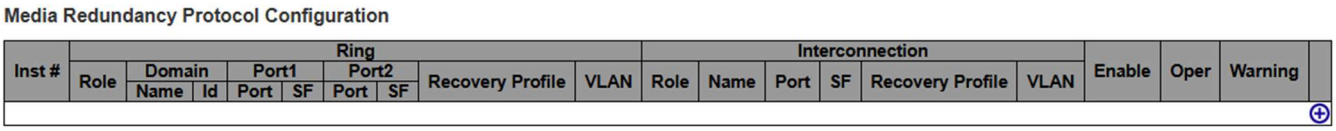


Figure 2.31 After Clicking ⊕ to Configure MRPs

2.5 DHCPv4

Atop's RHG9728 managed switch can act as a DHCPv4 (Dynamic Host Configuration Protocol over IP version 4) server in the local network. By enabling this function in the managed switch, an IPv4 addresses and related fields will be automatically assigned and delivered by the DHCPv4 server running inside the managed switch to other network devices connected to the managed switch. Under this Configuration→DHCPv4 menu, there are two submenus, Snooping and Relay as shown in Figure 2.32. The following subsections will describe them in more details.

Figure 2.32 Submenus under the DHCP Main Configuration Menu

2.5.1 Snooping

A rogue DHCP (Dynamic Host Control Protocol) server may be set up by an attacker in the network to provide falsify network configuration to a DHCP client such as wrong IP address, in-correct subnet mask, malicious gateway, and malicious DNS server. The purpose of DHCP spoofing attack may be to redirect the traffic of the DHCP client to a malicious domain and try to eavesdrop the traffic or simply try to prevent a successful network connection establishment. To protect against a network security attack of rogue DHCP server or DHCP spoofing attack, Atop's RHG9728 provide DHCP Snooping feature. When this feature is enabled on specific port(s) of RHG9728 managed switch, the RHG9728 will allow the DHCP messages from trusted ports to pass through while it will discard or filter the DHCP messages from untrusted ports.

To enable the DHCP Snooping feature, select the **Enabled** option from the dropdown menu behind the **Snooping Mode** option under the **DHCP Snooping Configuration** webpage as shown in Figure 2.33. By default, all interfaces of RHG9728 are untrusted for DHCP Snooping. To configure specific port(s) as trusted port(s), simply select the **Trusted** option under the **Mode** column for that particular Port(s). Finally, click the **Save** button at the bottom of the webpage to activate the DHCP Snooping on the selected port(s). Click Reset button to undo any change made locally and revert to previously saved values. Table 2.22 describes the options of DHCP Snooping Configuration.

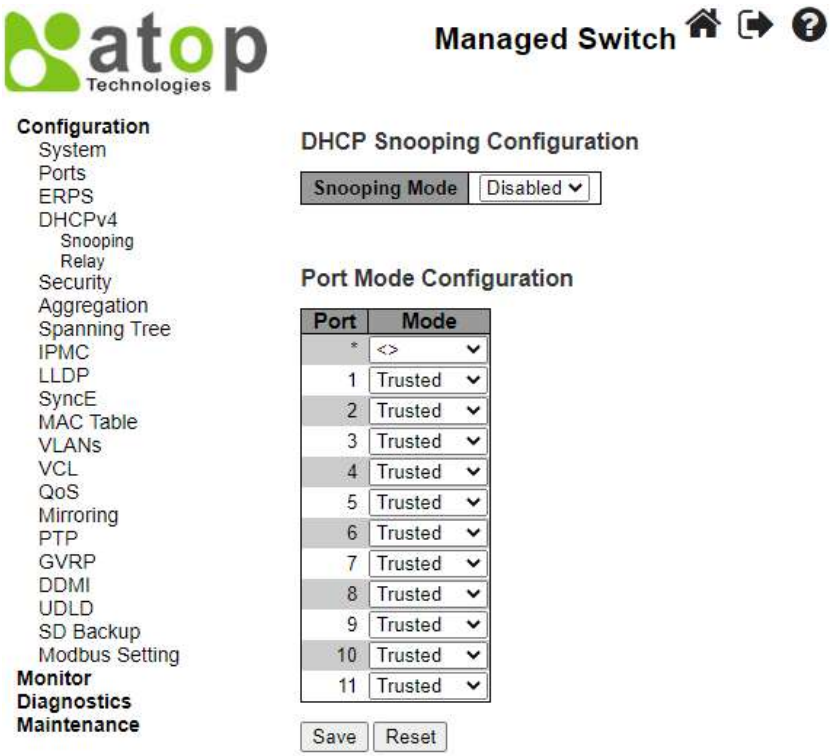


Figure 2.33 Webpage to Configure DHCPv4 Snooping

Table 2.22 Description of DHCP Snooping Configuration

Field Label	Description	Factory Default
Snooping Mode	Indicates the DHCP snooping mode operation. Possible modes are: **Enabled**: Enable DHCP snooping mode operation. When DHCP snooping mode operation is enabled, the DHCP request messages will be forwarded to trusted ports and only allow reply packets from trusted ports. **Disabled**: Disable DHCP snooping mode operation.	Disabled
Port Mode Configuration	Indicates the DHCP snooping port mode. Possible port modes are: **Trusted**: Configures the port as trusted source of the DHCP messages. **Untrusted**: Configures the port as untrusted source of the DHCP messages.	Trusted

2.5.2 Relay

A DHCP relay agent is a small program that relays DHCP/BOOTP messages between clients and servers on different subnets. DHCP/BOOTP relay agents are parts of the DHCP and BOOTP standards and function according to the Request for Comments (RFCs). It stores the incoming interface IP address in the GIADDR field of the DHCP packet. The DHCP server can use the value of GIADDR field to determine the assigned subnet. For such condition, please make sure the switch configuration of VLAN interface IP address and PVID (Port VLAN ID) correctly.

A relay agent relays DHCP/BOOTP messages that are broadcast on one of its connected physical interfaces, such as a network adapter, to other remote subnets to which it is connected by other physical interfaces. Figure 2.34 shows the **DHCP Relay** configuration webpage. Users can enable the DHCP Relay by selecting the **Enabled** box behind the **Relay Mode** option. Then, users can enter a Relay server's IP address in the **Relay Server** field.

Users also have a choice to enable the DHCP Relay Information Mode. If it is enabled, the switch will insert information about the client's network location into the packet header of the DHCP request, which is coming from the client on an untrusted interface. Then, the switch will send the modified request to the DHCP server. The DHCP server will inspect the information in the packet header and use it to generate the IP address or other parameters for the client. When the DHCP server returns the response to the switch, the switch will have an option to Replace, Keep, and Drop the information from the response packet and forward it to the client. After finishing the DHCP Relay setup, please click on the **Save** button to allow the change to take effect.

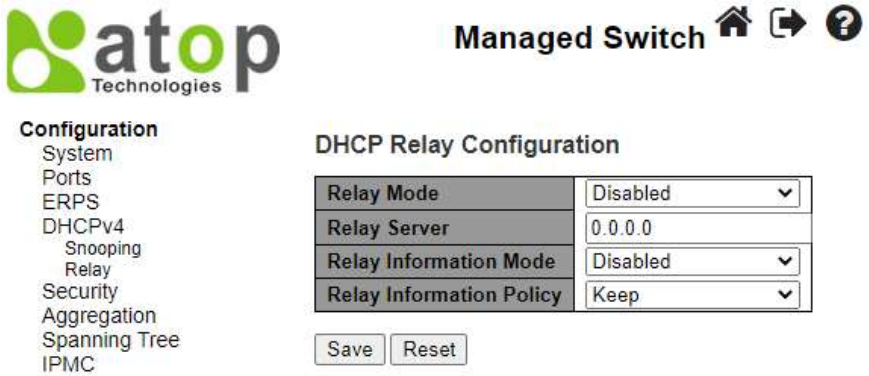


Figure 2.34 Webpage to Configure DHCPv4 Relay

Table 2.23 Description of DHCP Relay Configuration

Field Label	Description	Factory Default
Relay Mode	There are two modes here: Disabled or Enabled. Click the dropdown box to deactivate or activate the relay mode. **Enabled:** Enable DHCP relay mode operation. When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.	Disabled

Field Label	Description	Factory Default
	Disabled: Disable DHCP relay mode operation.	
Relay Server	Enter an IPv4 address of the DHCP relay server.	0.0.0.0
Relay Information Mode	There are two modes here: Disabled and Enabled. Click the dropdown list to deactivate or activate the information mode of the DHCP relay server. **Enabled:** Enable DHCP relay information mode operation. When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client. It only works when DHCP relay operation mode is enabled. **Disabled:** Disable DHCP relay information mode operation.	Disabled
Relay Information Policy	Set the information policy for the DHCP relay server. There are three modes here: Replace, Keep, and Drop. When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy. The 'Replace' policy is invalid when relay information mode is disabled. **Replace:** Replace the original relay information when a DHCP message that already contains it is received. **Keep:** Keep the original relay information when a DHCP message that already contains it is received. **Drop:** Drop the package when a DHCP message that already contains relay information is received.	Keep

2.6 Security

Security Configuration of Atop's RHG9728 managed switch consists of three main parts: **Switch**, **Network**, and **AAA**. There are a number of submenus for each of these main security configuration parts as shown in Figure 2.35.

- Security
  - Switch
    - Users
    - Privilege Levels
    - Auth Method
    - SSH
    - HTTPS
    - SNMP
      - System
      - Trap
      - Communities
      - Users
      - Groups
      - Views
      - Access
    - RMON
      - Statistics
      - History
      - Alarm
      - Event
  - Network
    - Port Security
      - Configuration
      - MAC Addresses
    - NAS
    - ACL
      - Ports
      - Rate Limiters
      - Access Control List
    - IP Source Guard
      - Configuration
      - Static Table
    - ARP Inspection
      - Port Configuration
      - VLAN Configuration
      - Static Table
      - Dynamic Table
  - AAA
    - RADIUS
    - TACACS+

Figure 2.35 Configuration-> Security Menu

2.6.1 Switch

The first submenu under Configuration→Security is the Switch menu as shown in Figure 2.36. There are other submenus under this Switch menu which are Users, Privilege Levels, Auth Method, SSH, HTTPS, SNMP, and RMON. The following subsections will explain each of these menus in more details.

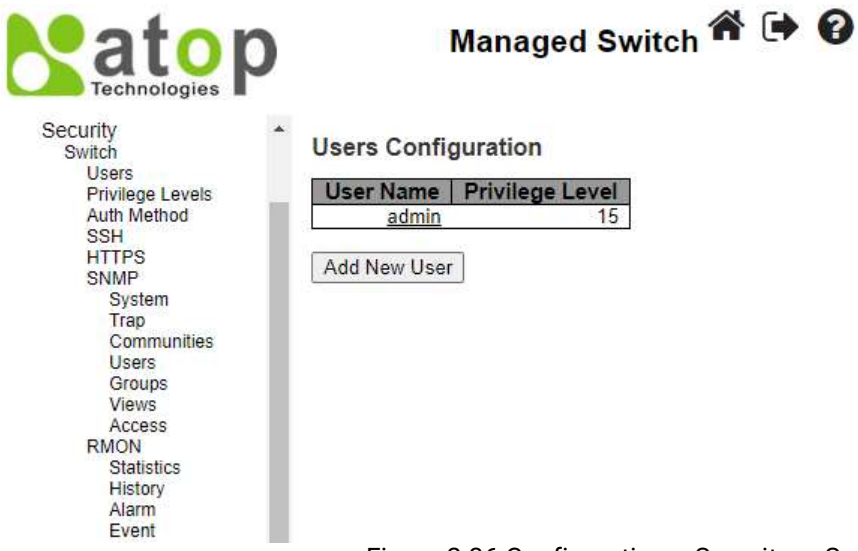


Figure 2.36 Configuration-> Security -> Switch Menu

2.6.1.1 Switch Users

A simple way of providing terminal access control in your network device (managed switch) is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device. RHG9728 managed switch uses privilege levels to provide password security for different levels of switch operation. The privilege level of the user is ranging from 0 to 15. If the user has the privilege level value of 15, it means that the user is granted the full control of the device, which is being an administrator. The system maintenance, such as software upload and factory defaults, need a user privilege level of 15. Guest account usually is assigned with the privilege level 5, and has the read-only access. Whereas, a standard user usually is assigned with the privilege level of 10 and has the read-write access.

When users first enter this **Users Configuration** webpage, users will see an overview of the current users. The user overview webpage consists of **User Name** and **Privilege Level** columns, as shown in Figure 2.37. Currently the only way to login as another user on the web server of the managed switch is to close and reopen the web browser. Table 2.24 provides explanation for the User Configuration webpage.

Figure 2.37 Webpage to Configure Security Switch Users

Table 2.24 Description of Users Configuration

Field Label	Description
User Name	The name identifying the user. This is also a link to Add/Edit User.
Privilege Level	The privilege level of the user. The allowed range is **0** to **15**. If the privilege level value is 15, it can access all groups, i.e., that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15.

Field Label	Description
	Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

There is also a hyperlink to Add/Edit User in each username. Users can also click **Add New User** button to add a new user. After clicked, the webpage in Figure 2.38 will be shown. Table 2.25 summarizes the descriptions of the Add User webpage. Figure 2.39 shows an example of Edit User webpage.

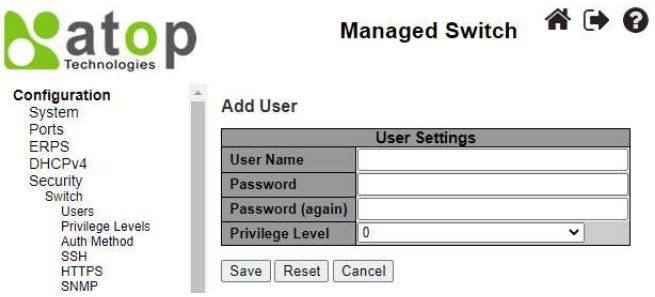


Figure 2.38 Webpage to Configure Security Switch Users – After Clicked **Add New User** Button

Table 2.25 Descriptions of Users Configuration – After Clicked **Add New User** Button

Label	Description	Factory Default
Username	A string identifying the user name that this entry should belong to. The allowed string length is **1** to **31**. The valid user name allows letters, numbers and underscores.	NULL
Password	The password of the user. The allowed string length is **0** to **31**. Any printable characters including space is accepted.	NULL
Password (again)	Re-enter the password for the user.	NULL
Privilege Level	The privilege level of the user. The allowed range is **0** to **15**. If the privilege level value is 15, it can access all groups, i.e., that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults and etc.) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.	0

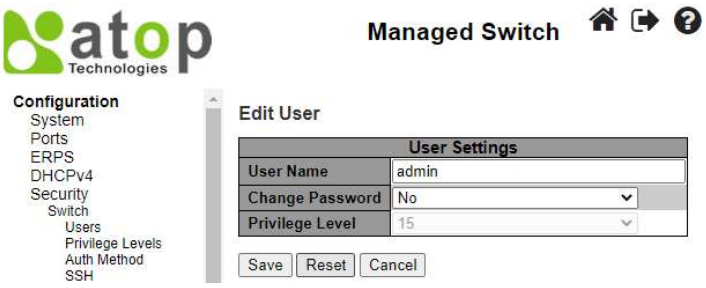


Figure 2.39 Webpage to Edit User

2.6.1.2 Switch Privilege Levels

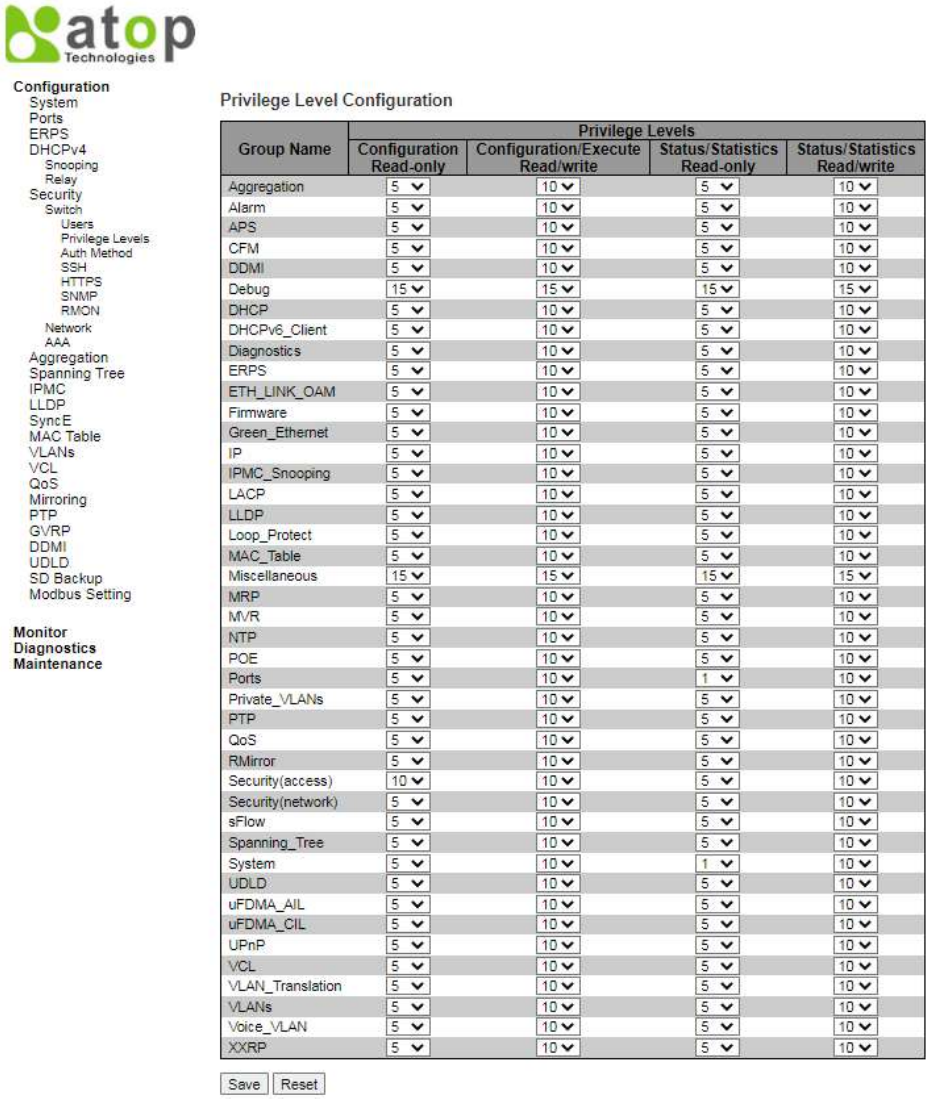
This subsection describes on the Privilege Level Configuration webpage as shown in Figure 2.40. The user can customize the privilege level in the table on this webpage.

Group Name is the name identifying the privilege group. In most cases, a privilege level group consists of a single module (e.g., LACP, RSTP or QoS), but a few of them contains more than one. Table 2.26 shows examples of some group name in details:

Table 2.26 Examples of Group Name

Label	Description
System	Contact, Name, Location, Time zone, Daylight Saving Time, Log.
Security	Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection, IP source guard.
IP	Everything except 'ping'.
Port	Everything except 'VeriPHY'.
Diagnostics	'ping' and 'VeriPHY'.
Maintenance	CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.
Debug	Only present in CLI.

Privilege Levels in every group has an authorization Privilege level for the following sub groups: **Configuration Read only, Configuration/Execute Read-Write, Status/Statistics Read-only, Status/Statistics Read-Write** (e.g., for clearing of statistics). User Privilege should be the same or greater than the authorization Privilege level to have the access to that group.



Group Name	Privilege Levels			
	Configuration Read-only	Configuration/Execute Read/write	Status/Statistics Read-only	Status/Statistics Read/write
Aggregation	5	10	5	10
Alarm	5	10	5	10
APS	5	10	5	10
CFM	5	10	5	10
DDMI	5	10	5	10
Debug	15	15	15	15
DHCP	5	10	5	10
DHCPv6_Client	5	10	5	10
Diagnostics	5	10	5	10
ERPS	5	10	5	10
ETH_LINK_OAM	5	10	5	10
Firmware	5	10	5	10
Green_Ethernet	5	10	5	10
IP	5	10	5	10
IPMC_Snooping	5	10	5	10
LACP	5	10	5	10
LLDP	5	10	5	10
Loop_Protect	5	10	5	10
MAC_Table	5	10	5	10
Miscellaneous	15	15	15	15
MRP	5	10	5	10
MVR	5	10	5	10
NTP	5	10	5	10
POE	5	10	5	10
Ports	5	10	1	10
Private_VLANs	5	10	5	10
PTP	5	10	5	10
QoS	5	10	5	10
RMirror	5	10	5	10
Security(access)	10	10	5	10
Security(network)	5	10	5	10
sFlow	5	10	5	10
Spanning_Tree	5	10	5	10
System	5	10	1	10
UDLD	5	10	5	10
uFDMA_AIL	5	10	5	10
uFDMA_CIL	5	10	5	10
UPnP	5	10	5	10
VCL	5	10	5	10
VLAN_Translation	5	10	5	10
VLANs	5	10	5	10
Voice_VLAN	5	10	5	10
XXRP	5	10	5	10

Figure 2.40 Webpage to Configure Privilege Levels of the Switch

2.6.1.3 Switch Auth Method

The authentication section allows you to configure how a user is authenticated when he/she logs into the switch via one of the management client interfaces. Note that management client interfaces are console, telnet, ssh, and http. There are three separated tables in this webpage: **Authentication Method Configuration, Command Authorization Method configuration,** and **Accounting Method Configuration webpage**, as shown in Figure 2.41. In the **Authentication Method Configuration**, users can configure how a user is authenticated when he/she logs into the switch via one of the management client interfaces. In **Command Authorization Method configuration**, users can configure the limitation of the CLI commands available to a user. In the **Accounting Method Configuration** webpage, users can configure command and **exec** (login) accounting. Table 2.27 shows descriptions of these methods in details. Please click **Save** button for a change to take effect, or click **Reset** button to undo any changes made locally and revert to previously saved values.

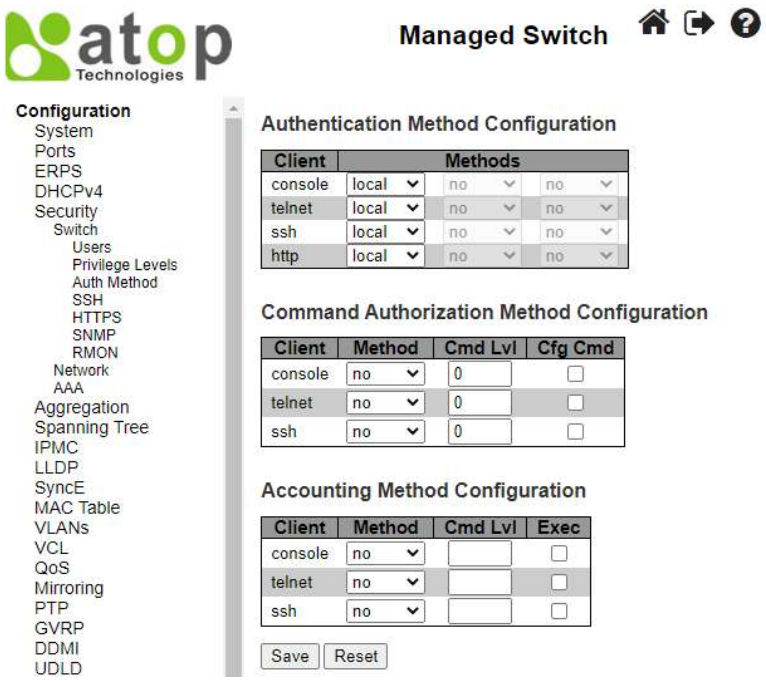


Figure 2.41 Webpage to Configure Switch Authentication Method

Table 2.27 Descriptions of Switch Authentication Method

Label	Description	Factory Default
Authentication Method Configuration		
Client	The management client for which the configuration below applies, which consists of console, telnet, ssh.	-
Methods	Set to one of the following values: • No: Authentication is disabled and login is not possible. • Local: Use the local user database on the switch for authentication. • Radius: Use remote RADIUS server(s) for authentication. • Tacacs: Use remote TACACS+ server(s) for authentication. Methods that involve remote servers are timed out if the remote servers are offline. In this case the next method is tried. Each method is tried from left to right and continues until a method either approves or rejects a user. If a remote server is used for primary authentication it is recommended to configure secondary authentication as 'local'. This will enable the management client to login via the local user database if none of the configured authentication servers are alive.	local, no, no
Command Authorization Method configuration		
Client	The management client for which the configuration below applies.	-
Method	Method can be set to one of the following values: • No: Command authorization is disabled. User is granted access to CLI commands according to his privilege level. • Tacacs: Use remote TACACS+ server(s) for command authorization. If all remote servers are offline, the user is granted access to CLI commands according to his privilege level.	no
Cmd Lvl	Authorize all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15.	0
Cfg Cmd	Also authorize configuration commands.	Unclicked
Accounting Method Configuration webpage		
Client	The management client for which the configuration below applies.	-
Method	Method can be set to one of the following values: • No: Accounting is disabled. • Tacacs: Use remote TACACS+ server(s) for accounting.	no

Label	Description	Factory Default
Cmd Lvl	Enable accounting of all commands with a privilege level higher than or equal to this level. Valid values are in the range 0 to 15. Leave the field empty to disable command accounting.	NULL
Exec	Enable exec (login) accounting.	Unclicked

2.6.1.4 Switch SSH

Users can enabled/disabled SSH (Secure Shell) mode through **SSH Configuration** webpage, as shown in Figure 2.42. Here, users can select **Enabled/Disabled** from the drop-down list of **Mode** field. Please click **Save** button for a change to take effect or **Reset** button to undo any changes made locally and revert to previously saved values.

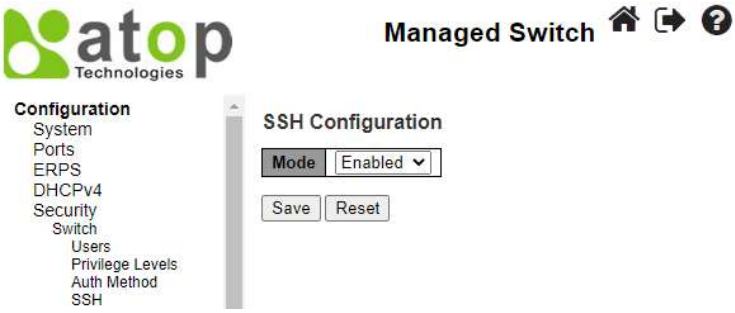


Figure 2.42 Webpage to Configure SSH

2.6.1.5 HTTPS

Users can enabled/disabled HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) mode through **HTTPS Configuration** Webpage, as shown in Figure 2.43. HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons. HTTPS is really just the use of Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

There are total of four fields: **Mode**, **Automatic Redirect**, **Certificate Maintain,** and **Certificate Status.** In the **Mode** field, users can select **Enabled/Disabled** the HTTPs mode. In the **Automatic Redirect** field, users can select to **Enabled/Disabled** this mode. When it is enabled, a HTTP connection will be automatically redirected to be a HTTPS connection. Note here that the browser may not allow to redirection if the browser does not trust the switch certificate. In such case, users need to initialize the HTTPS connection manually. For the **Certificate Maintain** field, users can choose type of operation whether to do nothing (**None**), delete the current certificate (**Delete**), upload a new certificate (**Upload**), and generate a new certificate (**Generate**). In the last field, **Certificate Status**, it displays the current status of certificate on the switch. Please click **Save** button for a change to take effect or **Reset** button to undo any changes made locally and revert to previously saved values.

If the user selects the **Upload** option for **Certificate Maintain** field, the webpage will be updated with additional fields which are **Certificate Pass Phrase**, **Certificate Upload**, and **File Upload** as shown in Figure 2.44. Table 2.28 summarizes the descriptions of fields in HTTPS Configuration webpage.

Note that to upload a certificate PEM file into the switch, the file should contain the certificate and private key together. If users have two separated files for saving certificate and private key, users can use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem. The RSA certificate is recommended since most of the new version of browsers has removed support for DSA in certificate

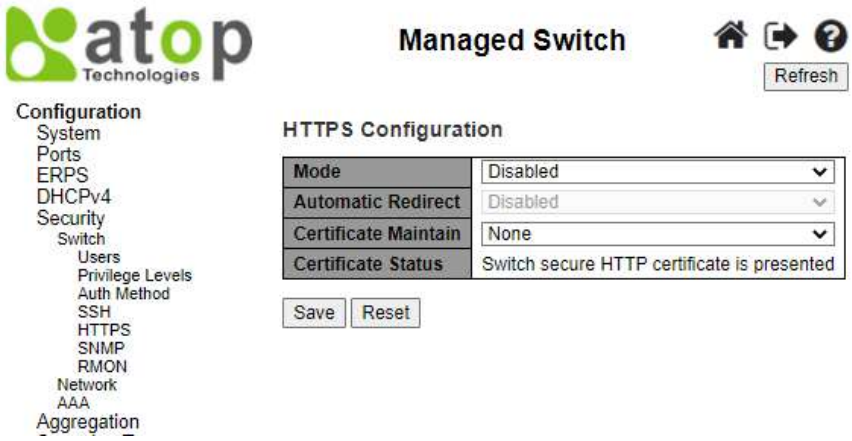


Figure 2.43 Webpage to HTTPS Configuration

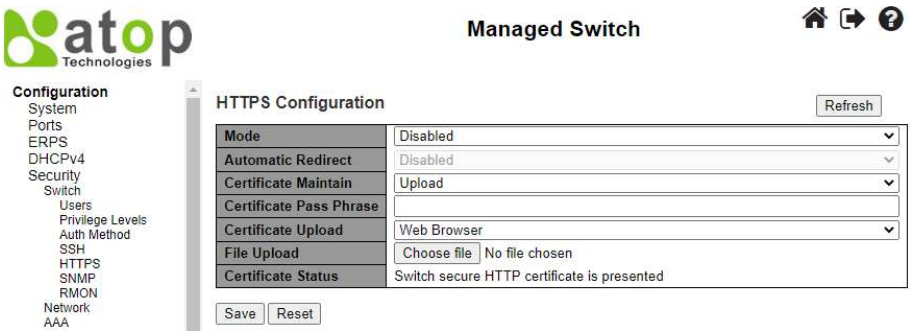


Figure 2.44 Webpage to HTTPS Configuration with Certificate Uploading

Table 2.28 Description of HTTPS Configuration Webpage

Label	Description	Factory Default
Mode	Indicate the HTTPS mode operation. **Enabled:** Enable HTTPS mode operation. **Disabled:** Disable HTTPS mode operation.	Disabled
Automatic Redirect	Indicate the HTTPS redirect mode operation. It is only significant when "HTTPS Mode Enabled" is selected. When the redirect mode is enabled, the HTTP connection will be redirected to HTTPS connection automatically. Note that the browser may not allow the redirect operation due to the security consideration unless the switch certificate is trusted to the browser. You need to initialize the HTTPS connection manually for this case. Possible modes are: **Enabled:** Enable HTTPS redirect mode operation. **Disabled:** Disable HTTPS redirect mode operation.	Disabled-
Certificate Maintain	Indicate the operation of certificate maintenance. **None**: No operation. **Delete**: Delete the current certificate. **Upload:** Upload a certificate PEM file. Possible methods are: Web Browser or URL. **Generate:** Generate a new self-signed RSA certificate.	None
Certificate Pass Phrase	Enter the pass phrase in this field if your uploading certificate is protected by a specific passphrase.	-
Certificate Upload	Upload a certificate PEM file into the switch. The file should contain the certificate and private key together. If you have two separated files for saving certificate and private key. Use the Linux cat command to combine them into a single PEM file. For example, cat my.cert my.key > my.pem. Note that the RSA	-

Label	Description	Factory Default
	certificate is recommended since most of the new version of browsers has removed support for DSA in certificate, e.g. Firefox v37 and Chrome v39. Possible methods are: **Web Browser**: Upload a certificate via Web browser. **URL**: Upload a certificate via URL, the supported protocols are HTTP, HTTPS, TFTP and FTP. The URL format is <protocol>://[<username>[:<password>]@]< host>[:<port>][/<path>]/<file_name>. For example, tftp://10.10.10.10/new_image_path/new_image.dat, http://username:password@10.10.10.10:80/new_image_path/new_image.dat. A valid file name is a text string drawn from alphabet (A-Za-z), digits (0-9), dot (.), hyphen (-), under score (_). The maximum length is 63 and hyphen must not be first character. The file name content that only contains '.' is not allowed.	
Certificate Status	Display the current status of certificate on the switch. Possible statuses are: **Switch secure HTTP certificate is presented.** **Switch secure HTTP certificate is not presented.** **Switch secure HTTP certificate is generating ....**	Switch secure HTTP certificate is presented

2.6.1.6 RMON

2.6.1.6.1 RMON Statistics

Figure 2.45 shows **RMON** (Remote Network Monitoring) **Statistics** Configuration. Atop's managed switch can monitoring network traffic on remote Ethernet segment to detect problem inside the network. The entry index key is **ID** for RMON Statistics table. Click **Add New Entry** button to add a new RMON Statistics entry to the table as shown in Figure 2.46. Table 2.29 describes the column labels of the RMON Statistics table. Please click on the **Save** button afterwards for a change to take effect, or click **Reset** button to undo any changes made locally and revert to previously saved values.

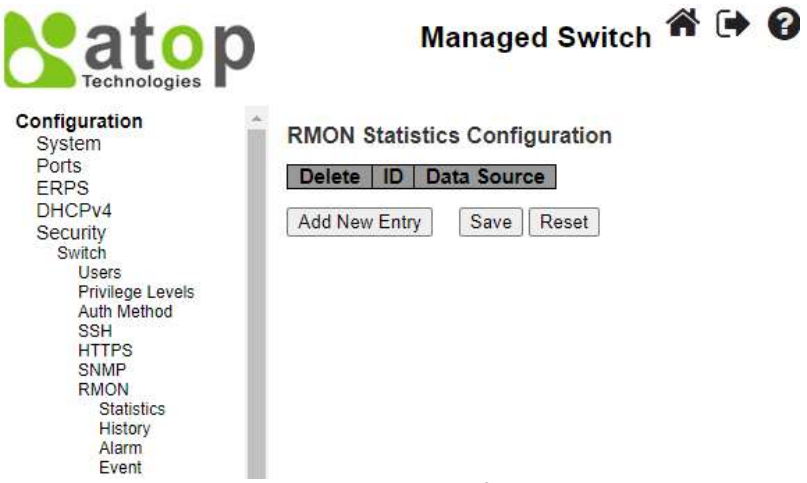


Figure 2.45 Webpage to Configure RMON Statistics

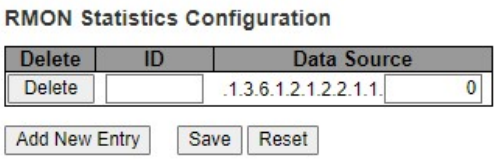


Figure 2.46 Adding New Entry to RMON Statistics Configuration

Table 2.29 Descriptions of RMON Statistics

Label	Description	Factory Default

Delete	Check to delete the entry. It will be deleted during the next save.	
ID	Indicates the index of the entry. The range is from 1 to 65535.	Null
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.	.1.3.6.1.2.1.2.2.1.1.0

2.6.1.6.2 RMON History

Figure 2.47 shows **RMON** (Remote Network Monitoring) **History** Configuration. It displays RMON history table. The entry index key is **ID** for RMON history table. Click **Add New Entry** button to add a new RMON history entry to the table as shown in Figure 2.48. Table 2.30 describes the column labels of the RMON Statistics table. Please click on the **Save** button afterwards for a change to take effect, or click **Reset** button to undo any changes made locally and revert to previously saved values.

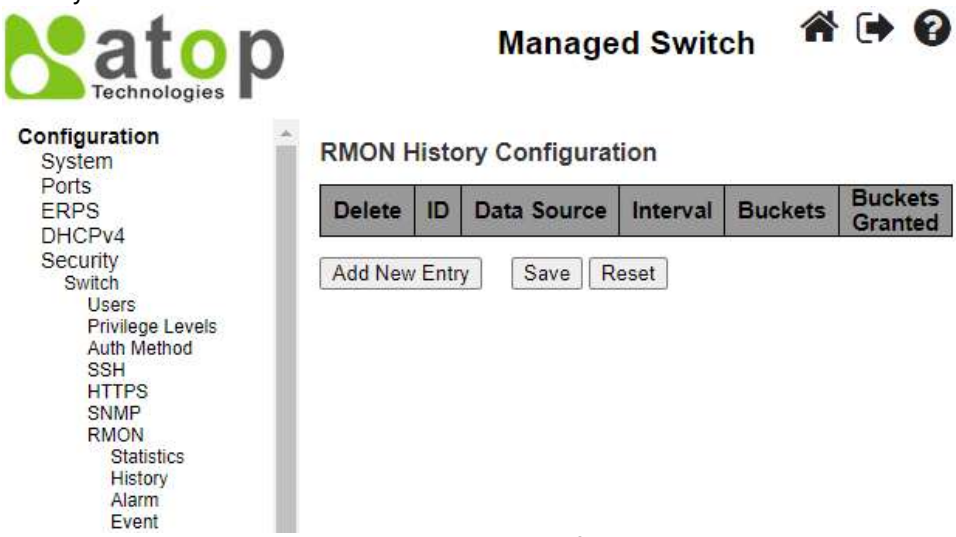


Figure 2.47 Webpage to Configure RMON History

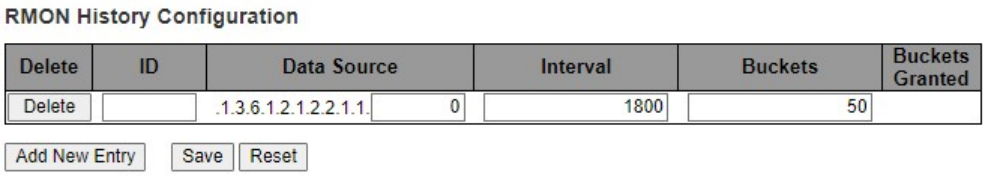


Figure 2.48 Adding New Entry to RMON History Table

Table 2.30 Descriptions of RMON History

Label	Description	Factory Default
Delete	Check to delete the entry. It will be deleted during the next save.	
ID	Indicates the index of the entry. The range is from 1 to 65535.	Null
Data Source	Indicates the port ID which wants to be monitored. If in stacking switch, the value must add 1000000*(switch ID-1), for example, if the port is switch 3 port 5, the value is 2000005.	.1.3.6.1.2.1.2.2.1.1.0
Interval	Indicates the interval in seconds for sampling the history statistics data. The range is from 1 to 3600, default value is 1800 seconds.	1800
Buckets	Indicates the maximum data entries associated this History control entry stored in RMON. The range is from 1 to 3600, default value is 50.	50
Buckets Granted	The number of data shall be saved in the RMON.	

2.6.1.6.3 RMON Alarm

Figure 2.49 shows **RMON Alarm** Configuration. It displays RMON alarm table. The entry index key is ID for RMON alarm table. Click **Add New Entry** button to add a new RMON alarm entry to the table as shown in Figure 2.49. Table 2.31 describes the column labels of the RMON alarm table. Please click on the **Save** button afterwards for a change to take effect, or click **Reset** button to undo any changes made locally and revert to previously saved values.

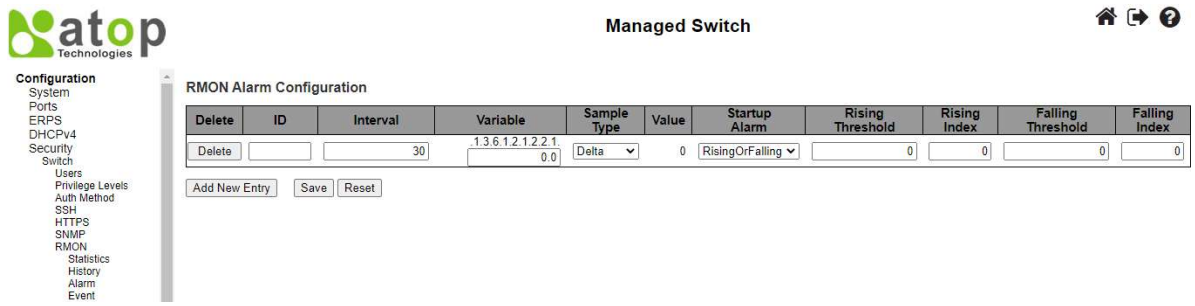


Figure 2.49 Webpage to Configure RMON Alarm

Table 2.31 Descriptions of RMON Alarm

Label	Description	Factory Default
Delete	Check to delete the entry. It will be deleted during the next save.	
ID	Indicates the index of the entry. The range is from 1 to 65535.	Null
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^{31}-1.	30
Variable	Indicates the particular variable to be sampled, the possible variables are: **InOctets**: The total number of octets received on the interface, including framing characters. **InUcastPkts:** The number of uni-cast packets delivered to a higher-layer protocol. **InNUcastPkts**: The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. **InDiscards**: The number of inbound packets that are discarded even the packets are normal. **InErrors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. **InUnknownProtos**: the number of the inbound packets that were discarded because of the unknown or un-support protocol. **OutOctets**: The number of octets transmitted out of the interface , including framing characters. **OutUcastPkts**: The number of uni-cast packets that request to transmit. **OutNUcastPkts**: The number of broad-cast and multi-cast packets that request to transmit. **OutDiscards**: The number of outbound packets that are discarded event the packets is normal. **OutErrors**: The number of outbound packets that could not be transmitted because of errors. **OutQLen**: The length of the output packet queue (in packets).	.1.3.6.1.2.1.2.2.1.0.0
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: **Absolute**: Get the sample directly. **Delta**: Calculate the difference between samples (default).	Delta
Value	The value of the statistic during the last sampling period.	0

Label	Description	Factory Default
Start-up Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: **Rising**Trigger alarm when the first value is larger than the rising threshold. **Falling**Trigger alarm when the first value is less than the falling threshold. **RisingOrFalling**Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).	RisingOrFalling
Rising Threshold	Rising threshold value (-2147483648-2147483647).	0
Rising Index	Rising event index (0-65535). If this value is zero, no associated event will be generated, as zero is not a valid event index.	0
Falling Threshold	Falling threshold value (-2147483648-2147483647)	0
Falling Index	Falling event index (0-65535). If this value is zero, no associated event will be generated, as zero is not a valid event index.	0

2.6.1.6.4 RMON Event

Figure 2.50 shows **RMON Event Configuration**. It displays RMON event table. The entry index key is ID for RMON event table. Click **Add New Entry** button to add a new RMON event entry to the table as shown in Figure 2.50. Table 2.32 describes the column labels of the RMON alarm table. Please click on the **Save** button afterwards for a change to take effect, or click **Reset** button to undo any changes made locally and revert to previously saved values.

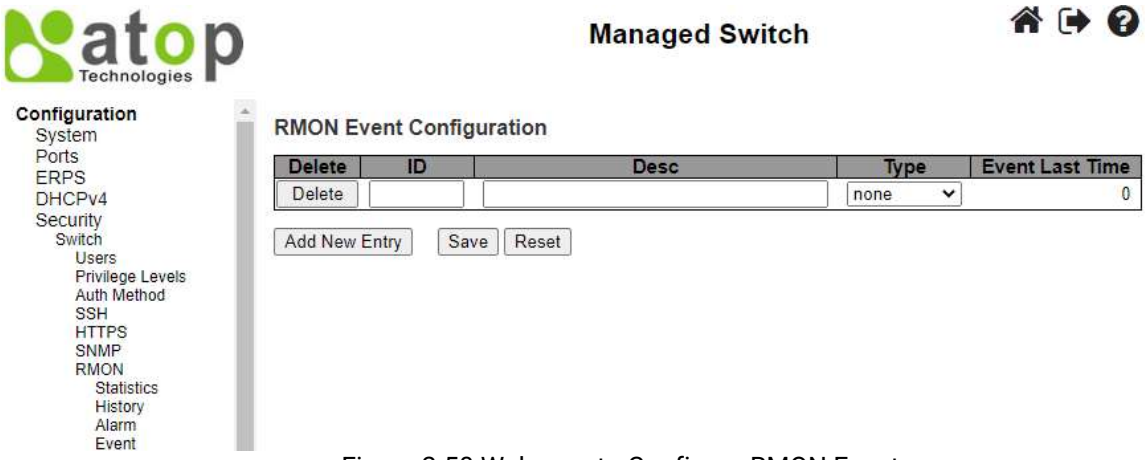


Figure 2.50 Webpage to Configure RMON Event

Table 2.32 Descriptions of RMON Event

Label	Description	Factory Default
Delete	Check to delete the entry. It will be deleted during the next save.	
ID	Indicates the index of the entry. The range is from 1 to 65535.	Null
Desc	Indicates this event, the string length is from 0 to 127, default is a null string.	Null
Type	Indicates the notification of the event, the possible types are: **none**: No SNMP log is created, no SNMP trap is sent. **log**: Create SNMP log entry when the event is triggered. **snmptrap**: Send SNMP trap when the event is triggered. **logandtrap**: Create SNMP log entry and sent SNMP trap when the event is triggered.	None
Event Last Time	Indicates the value of sysUpTime at the time this event entry last generated an event.	0

2.6.2 Network

Under this **Security→Network** submenus, the users can configure network security for the RHG9728 managed switch. Figure 2.51 shows list of menus under the **Security→Network**. Under this section, the users can setup security for port, network access server (NAS), access control list (ACL), IP source guard, and ARP (Address Resolution Protocol) inspection.

- Security
  - Switch
  - Network
    - Port Security
      - Configuration
      - MAC Addresses
    - NAS
    - ACL
      - Ports
      - Rate Limiters
      - Access Control List
    - IP Source Guard
      - Configuration
      - Static Table
    - ARP Inspection
      - Port Configuration
      - VLAN Configuration
      - Static Table
      - Dynamic Table
  - . . .

Figure 2.51 Configuration-> Security -> Network Menu

2.6.2.1 Port Security

2.6.2.1.1 Port Security Configuration

Global and per-port security of the managed switch can be configured in this webpage as shown in Figure 2.52. **Port Security** allows for limiting the number of users on a given port. A user is identified by a MAC address and VLAN ID. If **Port Security** is enabled on a port, the limit specifies the maximum number of users on the port. If this number is exceeded, an action is taken depending on violation mode. The violation mode can be one of the four different described below. The **Port Security Configuration** on this page consists of two sections: **Global Configuration** and **Port Configuration**. Table 2.33 summarizes the description of options for global and per-port configuration settings.

Please click on the **Save** button afterwards for a change to take effect, or click **Reset** button to undo any changes made locally and revert to previously saved values.

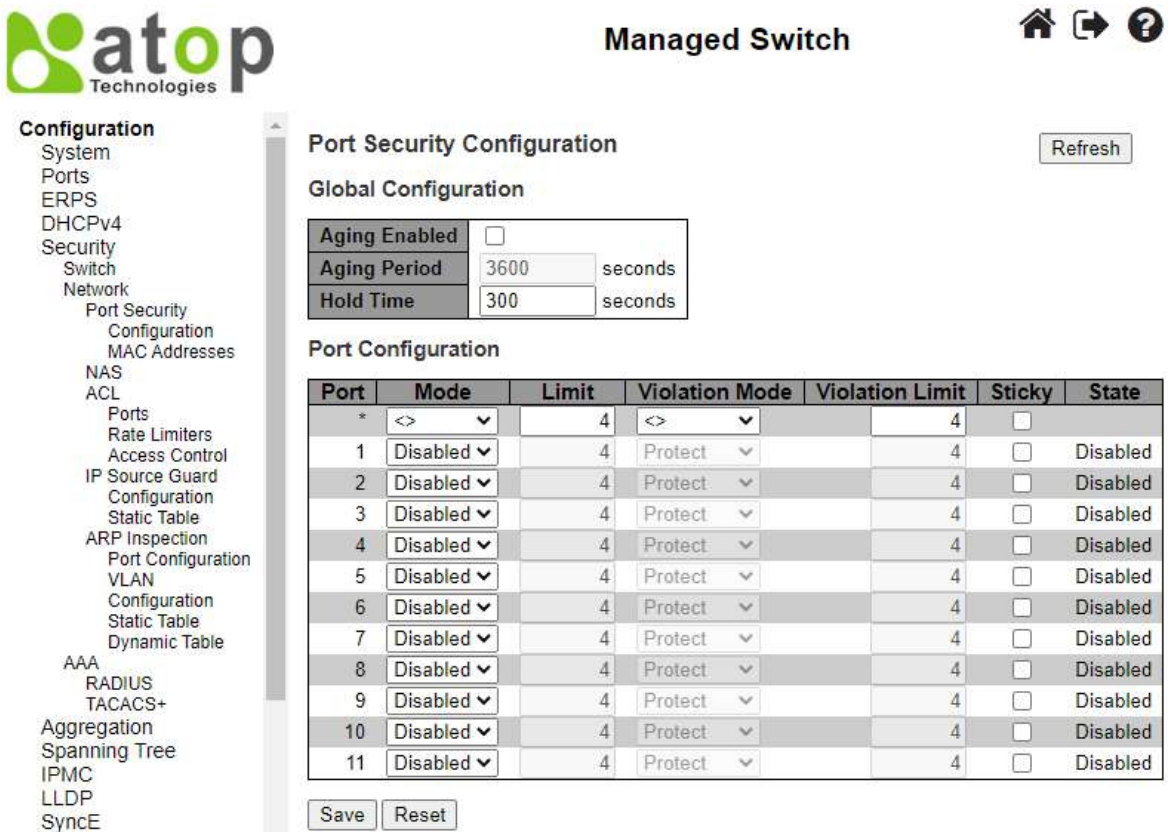


Figure 2.52 Webpage to Configure Network Port Security

Table 2.33 Descriptions of Port Security Configuration

Label	Description	Factory Default
	Global Configuration	
Aging Enabled	If checked, secured MAC addresses are subject to aging as discussed under Aging Period .	Disabled
Aging Period	If Aging Enabled is checked, then the aging period is controlled with this input. If other modules are using the underlying functionality for securing MAC addresses, they may have other requirements to the aging period. The underlying functionality will use the shorter requested aging period of all modules that have aging enabled. The Aging Period can be set to a number between 10 and 10000000 seconds with a default of 3600 seconds. To understand why aging may be desired, consider the following scenario: Suppose an end-host is connected to a 3rd party switch or hub, which in turn is connected to a port on this switch on which Port Security is enabled. The end-host will be allowed to forward if the limit is not exceeded. Now suppose that the end-host logs off or powers down. If it wasn't for aging, the end-host would still take up resources on this switch and will be allowed to forward. To overcome this situation, enable aging. With aging enabled, a timer is started once the end-host gets secured. When the timer expires, the switch starts looking for frames from the end-host, and if such frames are not seen within the next Aging Period, the end-host is assumed to be disconnected, and the corresponding resources are freed on the switch.	3600
Hold Time	The hold time - measured in seconds - is used to determine how long a MAC address is held in the MAC table if it has been found to violate the limit. Valid range is between 10 and 10000000 seconds with a default of 300 seconds. The reason for holding a violating MAC address in the MAC table is	300

Label	Description	Factory Default
	primarily to ensure that the same MAC address doesn't give rise to continuous notifications (if notifications on violation count is enabled).	
	Port Configuration	
Port	The port number to which the configuration below applies.	Port no. 1 ~ 11
Mode	Controls whether Port Security is enabled on this port. Notice that other modules may still use the underlying port security features without enabling Port Security on a given port.	Disabled
Limit	The maximum number of MAC addresses that can be secured on this port. This number cannot exceed 1023. Default is 4. If the limit is exceeded, an action is taken corresponding to the violation mode. The switch is "born" with a total number of MAC addresses from which all ports draw whenever a new MAC address is seen on a Port Security-enabled port. Since all ports draw from the same pool, it may happen that a configured maximum cannot be granted, if the remaining ports have already used all available MAC addresses.	4
Violation Mode	If Limit is reached, the switch can take one of the following actions: **Protect**: Do not allow more than Limit MAC addresses on the port, but take no further action. **Restrict**: If Limit is reached, subsequent MAC addresses on the port will be counted and marked as violating. Such MAC addresses are removed from the MAC table when the hold time expires. At most Violation Limit MAC addresses can be marked as violating at any given time. **Shutdown**: If Limit is reached, one additional MAC address will cause the port to be shut down. This implies that all secured MAC addresses be removed from the port, and no new addresses be learned. There are three ways to re-open the port: 1) In the "Configuration→Ports" page's "Configured" column, first disable the port, then restore the original mode. 2) Make a Port Security configuration change on the port. 3) Boot the switch.	Protect
Violation Limit	The maximum number of MAC addresses that can be marked as violating on this port. This number cannot exceed 1023. Default is 4. It is only used when Violation Mode is **Restrict**.	4
Sticky	Enables sticky learning of MAC addresses on this port. When the port is in sticky mode, all MAC addresses that would otherwise have been learned as dynamic are learned as sticky. Sticky MAC addresses are part of the running-config and can therefore be saved to start-up-config. Sticky MAC addresses survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config. A port can be Sticky-enabled whether or not Port Security is enabled on that interface. In that way, it is possible to add sticky MAC addresses managementwise before enabling Port Security. To do that, use the "Configuration→Security→Port Security→MAC Addresses" page.	Unclicked
State	This column shows the current Port Security state of the port. The state takes one of four values: **Disabled**: Port Security is disabled on the port. **Ready**: The limit is not yet reached. This can be shown for all violation modes. **Limit Reached**: Indicates that the limit is reached on this port. This can be shown for all violation modes. **Shutdown**: Indicates that the port is shut down by Port Security. This state can only be shown if violation mode is set to **Shutdown**.	Disabled

2.6.2.1.2 Port Security MAC Addresses

In this webpage as shown in Figure 2.53, the users may add and delete static and sticky MAC addresses managed by Port Security. The port security defines three types of MAC addresses, of which static and sticky can be added and removed on this page:

- **Static**: A MAC address added by end-user through management. Static MAC addresses are not subject to aging and will be added to the MAC address table once Port Security gets enabled on the interface. Static entries are part of the running-config and will survive interface link state changes and reboots if saved to startup-config. Static entries can be added to the running-config at any time whether or not Port Security is enabled.
- **Sticky**: When the interface is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky. Like static entries, sticky entries are part of the running-config and will survive interface link state changes and reboots if saved to the startup-config. Though not the intention with Sticky entries, they can be added by management to the running-config at any time whether or not Port Security is enabled on the interface, as long as the interface is in Sticky mode. Sticky entries will disappear if the interface is taken out of Sticky mode.

To add a new entry to the table of **Port Security Static and Sticky MAC Addresses**, click on **Add New MAC Entry** button. The new entry as shown in Figure 2.53 allows for adding static or sticky MAC address to a particular interface. When adding is finished, click the **Save** button to save the changes to running-config. Notice that sticky entries are normally added automatically through learning on the interface. Table 2.34 provides descriptions of the fields for Port Security Static and Sticky MAC Addresses.

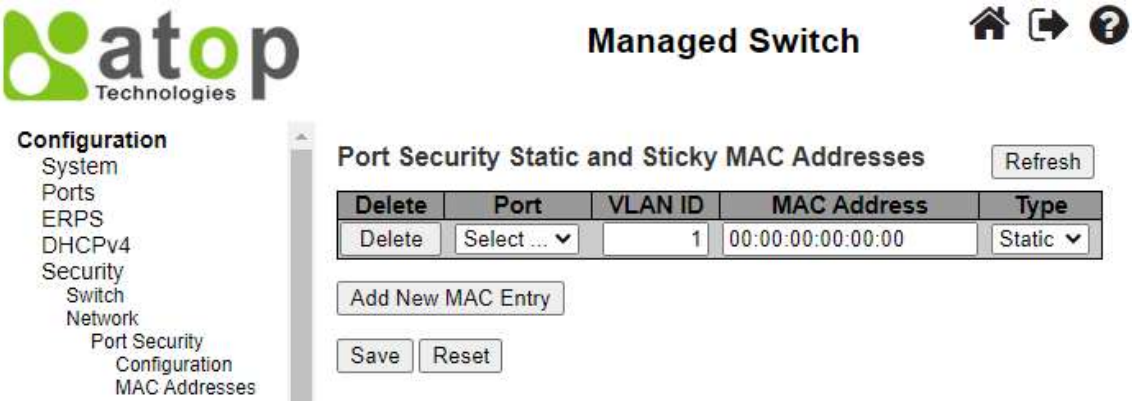


Figure 2.53 Webpage to Configure Network Port Security MAC Addresses

Table 2.34 Descriptions of RMON Event

Label	Description	Factory Default
Delete	Press this button to remove the entry from the MAC address table (if present) and the running-config. Notice that dynamic entries may be removed all-together on an interface through "Monitor→Security→Port Security→Switch" and one-by-one through "Monitor→Security→Port Security→Port"	
Port	The port number to which this MAC address is bound.	Select …
VLAN ID	The VLAN ID in question.	1
MAC Address	The MAC address in question.	00:00:00:00:00:00
Type	Indicates the type of entry and may be either Static or Sticky (see description above).	Static

2.6.2.2 NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the

client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers, the backend servers, determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the "**Configuration→Security→AAA**" webpage. The IEEE802.1X standard defines port-based operation, but non-standard variants overcome security limitations.

MAC-based authentication allows for authentication of more than one user on the same port, and doesn't require the user to have special 802.1X supplicant software installed on his/her system. The switch uses the user's MAC address to authenticate against the backend server. Intruders can create counterfeit MAC addresses, which makes MAC-based authentication less secure than 802.1X authentication.

This feature provides access control on a port basis. There are two types of authentications: **IEEE 802.1X** and **MAC-based**. The 802.1X supports **Port-based 802.1X** authentication type. The following three terms are used in the 802.1X context: *Supplicant*, *Authenticator,* and the *Authentication server*. The Supplicant is the client (PC) with some 801.1X software, where the Authenticator is the switch, and the Authentication server is such as a RADIUS server. The supplicant/client is connected to the authenticator/switch on some port, and the authenticator can reach an authentication server. The idea is that the supplicant wants access to the port, so it sends an **Extensible Authentication Protocol over LAN** (EAPoL) message to the authenticator, which in turn asks the authenticator server if this supplicant can be accepted. Then the authenticator opens the port for the supplicant, and communication can begin. Depending on how the authenticator is configured, this process behaves in different ways.

In **Port-based 802.1X**, if the supplicant S is on network N (connected to the authenticator on Port A) and S opens Port A, then everyone on network N will have access. However, only the supplicant that opened the port on the authenticator is allowed to transmit and receive packets. This is done through the MAC address of the supplicant.

A supplicant can be seen as a combination of a client and a supplicant component (that takes care of negotiating the port opening when the client transmits the first packet). This embedded supplicant component then uses the MAC address of the client as the username and password in the form aa-bb-cc-dd-ee-ff. This has the advantage that the client does not need to have supplicant software.

The **Configuration→Security→Network→NAS** (Network Access Server) webpage as shown in Figure 2.54 allows the user to configure the IEEE 802.1X and MAC-based authentication system and port settings. The NAS configuration consists of two sections: a system- (**System Configuration**) and a port-wide (**Port Configuration**). Table 2.35 provides detailed descriptions of options for both System Configuration and Port Configuration.

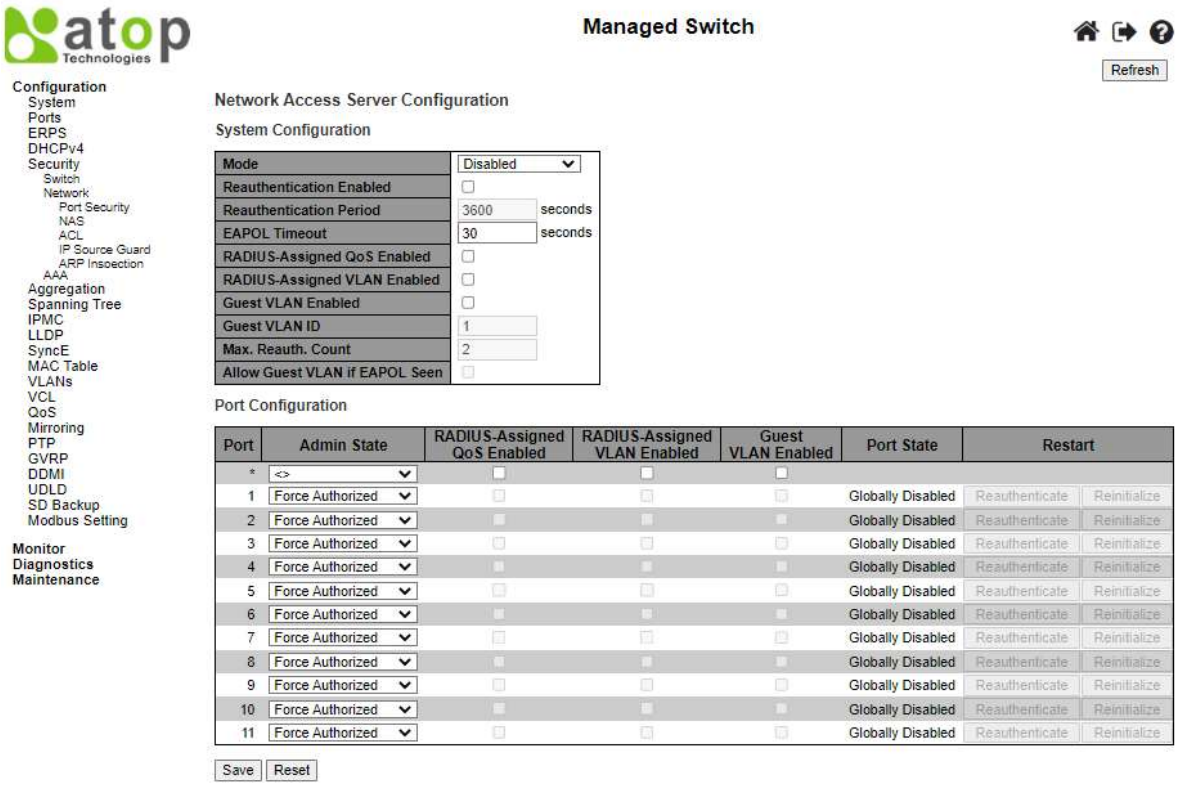


Figure 2.54 Webpage to Configure Network NAS

Table 2.35 Descriptions of Network NAS

Label	Description	Factory Default
System Configuration		
Mode	Indicates if NAS is globally enabled or disabled on the switch. If globally disabled, all ports are allowed forwarding of frames.	Disabled
Reauthentication Enabled	If checked, successfully authenticated supplicants/clients are reauthenticated after the interval specified by the Reauthentication Period. Reauthentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port or if a supplicant is no longer attached. For MAC-based ports, reauthentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore doesn't imply that a client is still present on a port (see Aging Period below).	Unclicked
Reauthentication Period	Determines the period, in seconds, after which a connected client must be reauthenticated. This is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds.	3600
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid values are in the range 1 to 65535 seconds. This has no effect for MAC-based ports.	30
Aging Period	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • MAC-Based Auth. When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number	300

Label	Description	Factory Default
	between 10 and 1000000 seconds. If reauthentication is enabled and the port is in an 802.1X-based mode, this is not so critical, since supplicants that are no longer attached to the port will get removed upon the next reauthentication, which will fail. But if reauthentication is not enabled, the only way to free resources is by aging the entries. For ports in MAC-based Auth. mode, reauthentication doesn't cause direct communication between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.	
Hold Time	This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses: • MAC-Based Auth. If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Configuration→Security→AAA" page) - the client is put on hold in the Unauthorized state. The hold timer does not count during an on-going authentication. In MAC-based Auth. mode, the switch will ignore new frames coming from the client during the hold time. The Hold Time can be set to a number between 10 and 1000000 seconds.	10
RADIUS-Assigned QoS Enabled	RADIUS-assigned QoS provides a means to centrally control the traffic class to which traffic coming from a successfully authenticated supplicant is assigned on the switch. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned QoS Enabled below for a detailed description). The "RADIUS-Assigned QoS Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned QoS Class functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned QoS Class is enabled on that port. When unchecked, RADIUS-server assigned QoS Class is disabled on all ports.	Unclicked
RADIUS-Assigned VLAN Enabled	RADIUS-assigned VLAN provides a means to centrally control the VLAN on which a successfully authenticated supplicant is placed on the switch. Incoming traffic will be classified to and switched on the RADIUS-assigned VLAN. The RADIUS server must be configured to transmit special RADIUS attributes to take advantage of this feature (see RADIUS-Assigned VLAN Enabled below for a detailed description). The "RADIUS-Assigned VLAN Enabled" checkbox provides a quick way to globally enable/disable RADIUS-server assigned VLAN functionality. When checked, the individual ports' ditto setting determines whether RADIUS-assigned VLAN is enabled on that port. When unchecked, RADIUS-server assigned VLAN is disabled on all ports.	Unclicked
Guest VLAN Enabled	A Guest VLAN is a special VLAN - typically with limited network access - on which 802.1X-unaware clients are placed after a network administrator-defined timeout. The switch follows a set of rules for entering and leaving the Guest VLAN as listed below. The "Guest VLAN Enabled" checkbox provides a quick way to globally enable/disable Guest VLAN functionality. When checked,	Unclicked

Label	Description	Factory Default
	the individual ports' ditto setting determines whether the port can be moved into Guest VLAN. When unchecked, the ability to move to the Guest VLAN is disabled on all ports.	
Guest VLAN ID	This is the value that a port's Port VLAN ID is set to if a port is moved into the Guest VLAN. It is only changeable if the Guest VLAN option is globally enabled. Valid values are in the range [1; 4095].	1
Max. Reauth. Count	The number of times the switch transmits an EAPOL Request Identity frame without response before considering entering the Guest VLAN is adjusted with this setting. The value can only be changed if the Guest VLAN option is globally enabled. Valid values are in the range [1; 255].	2
Allow Guest VLAN if EAPOL Seen	The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port. The value can only be changed if the Guest VLAN option is globally enabled.	Unclicked
Port Configuration		
Port	The port number for which the configuration below applies.	
Admin State	If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available: **Force Authorized** In this mode, the switch will send one EAPOL Success frame when the port link comes up, and any client on the port will be allowed network access without authentication. **Force Unauthorized** In this mode, the switch will send one EAPOL Failure frame when the port link comes up, and any client on the port will be disallowed network access. **Port-based 802.1X** In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.	Force Authorized

Label	Description	Factory Default
	When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant. **Note:** Suppose two backend servers are enabled and that the server timeout is configured to X seconds (using the AAA configuration page), and suppose that the first server in the list is currently down (but not considered dead). Now, if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, then it will never get authenticated, because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. And since the server hasn't yet failed (because the X seconds haven't expired), the same server will be contacted upon the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate. **MAC-based Auth.** Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string on the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly. When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based Authentication has nothing to do with the 802.1X standard. The advantage of MAC-based authentication over 802.1X-based authentication is that the clients don't need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.	
RADIUS-Assigned QoS Enabled	When RADIUS-Assigned QoS is both globally enabled and enabled (checked) on a given port, the switch reacts to QoS Class information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, traffic received on the supplicant's port will be classified to the given QoS Class. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a QoS Class or it's invalid, or the supplicant is otherwise no longer present on the port, the port's QoS Class is	Unclicked

Label	Description	Factory Default
	immediately reverted to the original QoS Class (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • Port-based 802.1X • Single 802.1X **RADIUS attributes used in identifying a QoS Class:** The User-Priority-Table attribute defined in RFC4675 forms the basis for identifying the QoS Class in an Access-Accept packet. Only the first occurrence of the attribute in the packet will be considered, and to be valid, it must follow this rule: • All 8 octets in the attribute's value must be identical and consist of ASCII characters in the range '0' - '7', which translates into the desired QoS Class in the range [0; 7].	
RADIUS-Assigned VLAN Enabled	When RADIUS-Assigned VLAN is both globally enabled and enabled (checked) for a given port, the switch reacts to VLAN ID information carried in the RADIUS Access-Accept packet transmitted by the RADIUS server when a supplicant is successfully authenticated. If present and valid, the port's Port VLAN ID will be changed to this VLAN ID, the port will be set to be a member of that VLAN ID, and the port will be forced into VLAN unaware mode. Once assigned, all traffic arriving on the port will be classified and switched on the RADIUS-assigned VLAN ID. If (re-)authentication fails or the RADIUS Access-Accept packet no longer carries a VLAN ID or it's invalid, or the supplicant is otherwise no longer present on the port, the port's VLAN ID is immediately reverted to the original VLAN ID (which may be changed by the administrator in the meanwhile without affecting the RADIUS-assigned). This option is only available for single-client modes, i.e. • Port-based 802.1X • Single 802.1X For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. **RADIUS attributes used in identifying a VLAN ID:** RFC2868 and RFC3580 form the basis for the attributes used in identifying a VLAN ID in an Access-Accept packet. The following criteria are used: • The Tunnel-Medium-Type, Tunnel-Type, and Tunnel-Private-Group-ID attributes must all be present at least once in the Access-Accept packet. • The switch looks for the first set of these attributes that have the same Tag value and fulfil the following requirements (if Tag == 0 is used, the Tunnel-Private-Group-ID does not need to include a Tag): - Value of Tunnel-Medium-Type must be set to "IEEE-802" (ordinal 6). - Value of Tunnel-Type must be set to "VLAN" (ordinal 13). - Value of Tunnel-Private-Group-ID must be a string of ASCII chars in the range '0' - '9', which is interpreted as a decimal string representing the VLAN ID. Leading '0's are discarded. The final value must be in the range [1; 4095].	Unclicked

Label	Description	Factory Default
Guest VLAN Enabled	When Guest VLAN is both globally enabled and enabled (checked) for a given port, the switch considers moving the port into the Guest VLAN according to the rules outlined below. This option is only available for EAPOL-based modes, i.e.: • Port-based 802.1X • Single 802.1X • Multi 802.1X For trouble-shooting VLAN assignments, use the "Monitor→VLANs→VLAN Membership and VLAN Port" pages. These pages show which modules have (temporarily) overridden the current Port VLAN configuration. **Guest VLAN Operation:** When a Guest VLAN enabled port's link comes up, the switch starts transmitting EAPOL Request Identity frames. If the number of transmissions of such frames exceeds Max. Reauth. Count and no EAPOL frames have been received in the meanwhile, the switch considers entering the Guest VLAN. The interval between transmission of EAPOL Request Identity frames is configured with EAPOL Timeout. If Allow Guest VLAN if EAPOL Seen is enabled, the port will now be placed in the Guest VLAN. If disabled, the switch will first check its history to see if an EAPOL frame has previously been received on the port (this history is cleared if the port link goes down or the port's Admin State is changed), and if not, the port will be placed in the Guest VLAN. Otherwise it will not move to the Guest VLAN, but continue transmitting EAPOL Request Identity frames at the rate given by EAPOL Timeout. Once in the Guest VLAN, the port is considered authenticated, and all attached clients on the port are allowed access on this VLAN. The switch will not transmit an EAPOL Success frame when entering the Guest VLAN. While in the Guest VLAN, the switch monitors the link for EAPOL frames, and if one such frame is received, the switch immediately takes the port out of the Guest VLAN and starts authenticating the supplicant according to the port mode. If an EAPOL frame is received, the port will never be able to go back into the Guest VLAN if the "Allow Guest VLAN if EAPOL Seen" is disabled.	Unclicked
Port Status	The current state of the port. It can undertake one of the following values: **Globally Disabled:** NAS is globally disabled. **Link Down:** NAS is globally enabled, but there is no link on the port. **Authorized:** The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized. **Unauthorized:** The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server. **X Auth/Y Unauth:** The port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.	Globally Disabled
Restart	Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based mode. Clicking these buttons will not cause settings changed on the page to take effect. **Reauthenticate:** Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). The button only has effect for successfully authenticated clients on	-

Label	Description	Factory Default
	the port and will not cause the clients to get temporarily unauthorized. **Reinitialize:** Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.	

Click **Refresh** button to refresh the page. Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

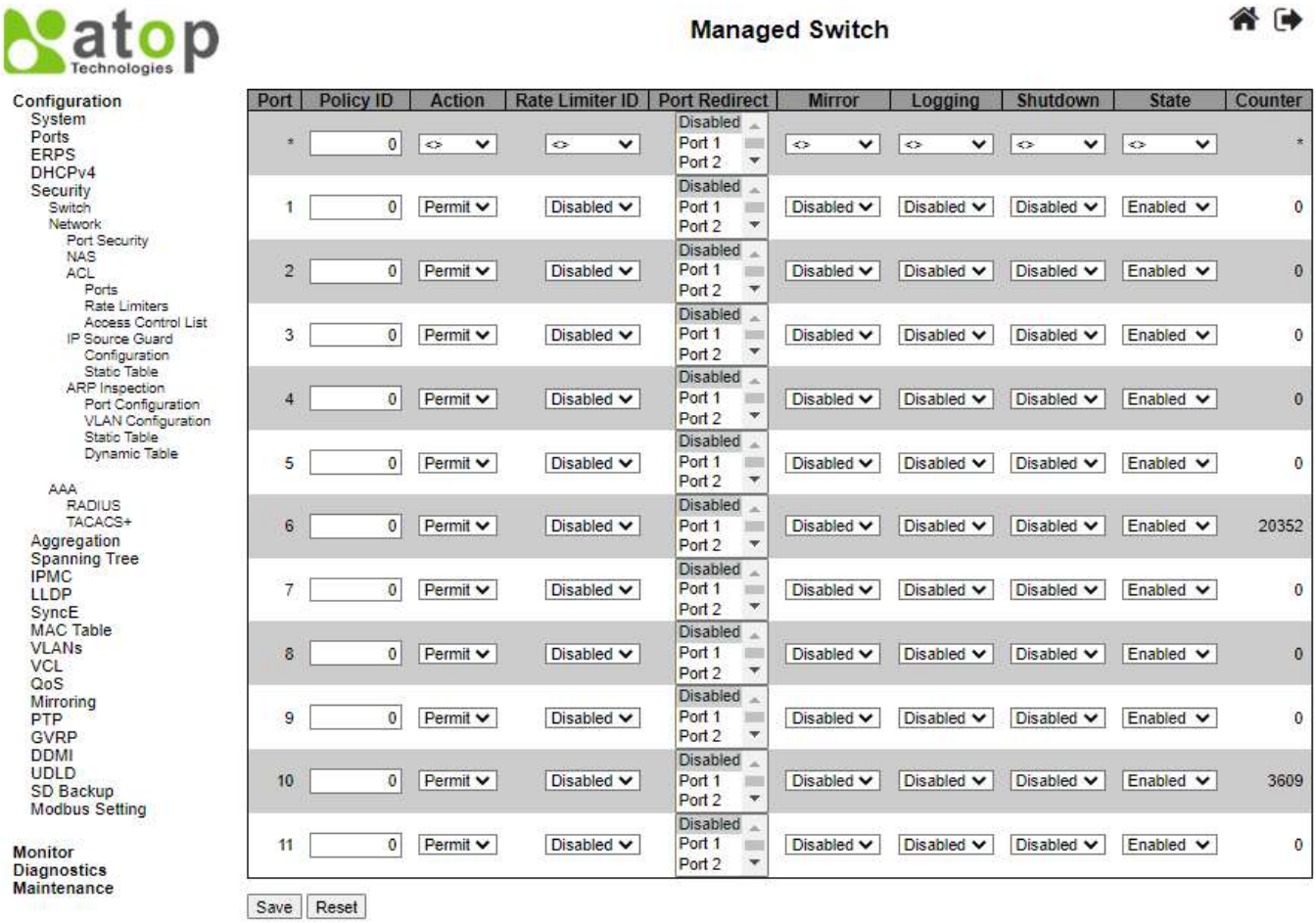
2.6.2.3 ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing Access Control Entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.
ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.
There are 3 web-pages associated with the manual ACL configuration: **ACL Ports**, **ACL Rate Limiters**, and **ACL Access Control List**. Figure 2.55 shows the list of ACL menus. The following subsections will describe each ACL configuration.

Figure 2.55 Access Control List's Submenus

2.6.2.3.1 ACL Ports

The **ACL→Ports** webpage is depicted in Figure 2.56. The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE (Access Control Entry) matching without getting matched. In that case a counter associated with that port is incremented. Table 2.36 summarizes description for each specific port property.



Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled / Port 1 / Port 2	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
3	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
4	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
5	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
6	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	20352
7	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
8	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
9	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0
10	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	3609
11	0	Permit	Disabled	Disabled / Port 1 / Port 2	Disabled	Disabled	Disabled	Enabled	0

Figure 2.56 Webpage to Configure Network ACL Ports

Table 2.36 Descriptions of Network ACL Ports

Label	Description	Factory Default
Port	The logical port for the settings contained in the same row.	Port ID from 1 to 11
Policy ID	Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.	0
Action	Select whether forwarding is permitted ("Permit") or denied ("Deny"). The default value is "Permit".	Permit
Rate Limiter ID	Select which rate limiter to apply on this port. The allowed values are Disabled or the values 1 through 16. The default value is "Disabled".	Disabled
Port Redirect	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".	Disabled
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".	Disabled
Logging	Specify the logging operation of this port. Notice that the logging message doesn't include the 4 bytes CRC. The allowed values are: Enabled: Frames received on the port are stored in the System Log. Disabled: Frames received on the port are not logged. The default value is "Disabled". Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.	Disabled
Shutdown	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled".	Disabled

Label	Description	Factory Default
	Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).	
State	Specify the port state of this port. The allowed values are: Enabled: To reopen ports by changing the volatile port configuration of the ACL user module. Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".	Disabled
Counter	Counts the number of frames that match this ACE.	0

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.6.2.3.2 ACL Rate Limiters

The **ACL→Rate Limiters** webpage is shown in Figure 2.57. Under this page, the users can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s). Table 2.37 describes the labels of ACL Rate Limiters Configuration.

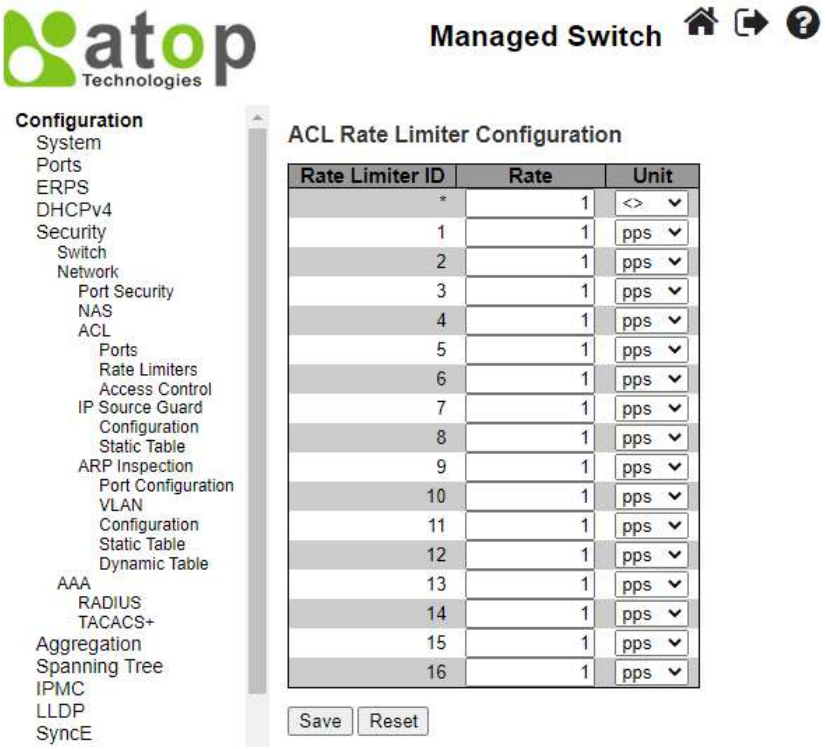


Figure 2.57 Webpage to Configure Network ACL Rate Limiters

Table 2.37 Descriptions of Network ACL Rate Limiters

Label	Description	Factory Default
Rate Limiter ID	The rate limiter ID for the settings contained in the same row and its range is 1 to 16.	Limiter ID 1 to 16
Rate	The valid rate is **0 - 99, 100, 200, 300, ..., 1092000** in pps or **0, 100, 200, 300, ..., 1000000** in kbps.	1
Unit	Specify the rate unit. The allowed values are: **pps**: packets per second. **kbps**: Kbits per second.	pps

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.6.2.3.3 ACL Access Control List

The **ACL→Access Control List** webpage shows the ACEs in a prioritized way, highest (top) to lowest (bottom). By default, the table is empty as shown in Figure 2.58. When click on the plus sign icon ⊕ at the end of the table, a set of parameters are listed as three tables under the ACE Configuration webpage as shown in Figure 2.59.

In Figure 2.58, users can select **auto-refresh** option by checking the **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Users can click **Refresh** button to refresh the page; any changes made locally will be undone. Users can click **Clear** button to clear the counters. Lastly, users can click **Remove All** button to remove all ACEs.

An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will act (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Table 2.38 provides additional information for each parameter to configure the ACL. The maximum number of ACEs is 64.

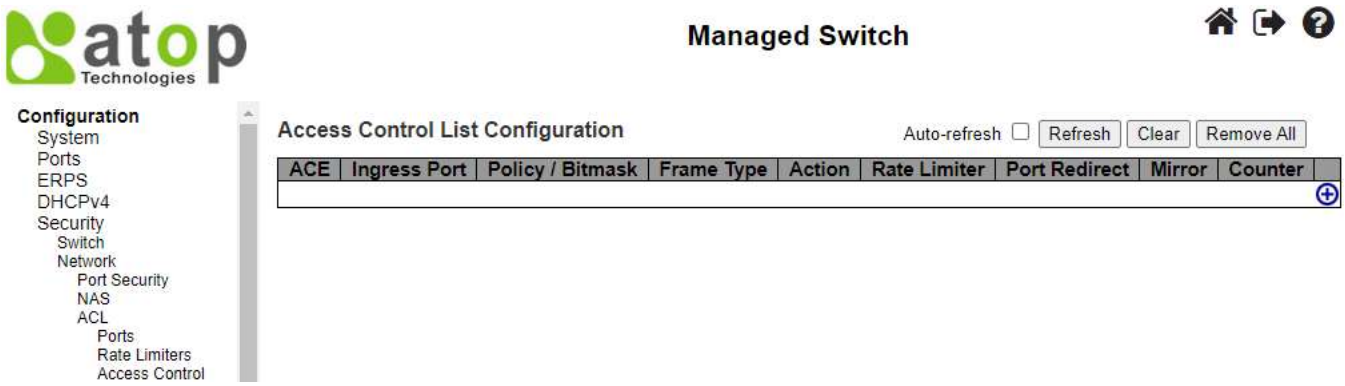


Figure 2.58 Webpage to Configure Network ACL Access Control

Table 2.38 Summary of Label, Description, and Factory Default for ACL (Access Control List)

Label	Description	Factory Default
ACE Configuration		
ACE	Indicates the ACE ID.	Disabled
Ingress Port	Indicates the ingress port of the ACE. Possible values are: **All:** The ACE will match all ingress port. **Port:** The ACE will match a specific ingress port.	All
Policy/Bitmask	Indicates the policy number and bitmask of the ACE.	Any
Frame Type	Indicates the frame type of the ACE. Possible values are: - **Any**: The ACE will match any frame type. **- EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. - **ARP**: The ACE will match ARP/RARP frames. **- IPv4**: The ACE will match all IPv4 frames. - **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. **- IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. - IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. - **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. - **IPv6**: The ACE will match all IPv6 standard frames.	Any
Action	Indicates the forwarding action of the ACE.	Permit

	- **Permit:** Frames matching the ACE may be forwarded and learned. - **Deny**: Frames matching the ACE are dropped. - **Filter**: Frames matching the ACE are filtered.	
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.	Disabled
Port Redirect	Indicates the port redirect operation of the ACE. Frames matching the ACE are redirected to the port number. The allowed values are Disabled or a specific port number. When Disabled is displayed, the port redirect operation is disabled.	Disabled
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".	Disabled
Counter	The counter indicates the number of times the ACE was hit by a frame.	Disabled
Modification Buttons	You can modify each ACE (Access Control Entry) in the table using the following buttons: ⊕: Inserts a new ACE before the current row. ⓔ: Edits the ACE row. ⬆: Moves the ACE up the list. ⬇: Moves the ACE down the list. ⊗: Deletes the ACE. ⊕: The lowest plus sign adds a new entry at the bottom of the ACE listings	

After clicking on the plus sign to insert a new ACE (Access Control Entry), the users can configure an ACE on the webpage as shown in Figure 2.59. An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the **ingress port** for the ACE, and then select the **frame type**. Different parameter options are displayed depending on the **frame type** selected. That is additional table and parameters will be available for settings. A frame that hits this ACE matches the configuration that is defined here. Table 2.39 to Table 2.47 summarizes description of all ACL Configuration with different frame types.

Click **Save** button to save the setting. Click **Reset** button to change the setting back to factory default. Click **Cancel** button to keep the current setting.

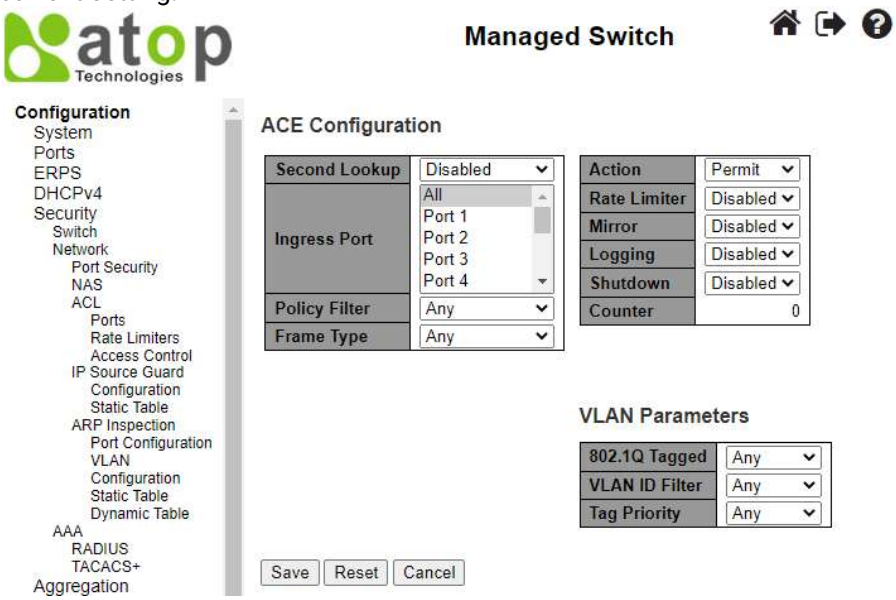


Figure 2.59 Webpage to Configure Network ACL Access Control After Clicked + to add new entry

Table 2.39 Description of ACL Configuration

Label	Description
Second Lookup	Specify the second lookup operation of the ACE.
Ingress Port	Select the ingress port for which this ACE applies. **All**: The ACE applies to all port. **Port *n***: The ACE applies to this port number, where *n* is the number of the switch port.
Policy Filter	Specify the policy number filter for this ACE. **Any**: No policy filter is specified. (policy filter status is "don't-care".) **Specific**: If you want to filter a specific policy with this ACE, choose this value. Two field for entering a policy value and bitmask appears.
Policy Value	When "Specific" is selected for the policy filter, you can enter a specific policy value. The allowed range is **0** to **63**.
Policy Bitmask	When "Specific" is selected for the policy filter, you can enter a specific policy bitmask. The allowed range is **0x0** to **0x3f**. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [policy_value & policy_bitmask]. For example, if the policy value is 3 and the policy bitmask is 0x10(bit 0 is "don't-care" bit), then policy 2 and 3 are applied to this rule.
Frame Type	Select the frame type for this ACE. These frame types are mutually exclusive. **Any**: Any frame can match this ACE. **Ethernet Type**: Only Ethernet Type frames can match this ACE. The IEEE 802.3 describes the value of Length/Type Field specifications to be greater than or equal to 1536 decimal (equal to 0600 hexadecimal) and the value should not be equal to 0x800(IPv4), 0x806(ARP) or 0x86DD(IPv6). **ARP**: Only ARP frames can match this ACE. Notice the ARP frames won't match the ACE with ethernet type. **IPv4**: Only IPv4 frames can match this ACE. Notice the IPv4 frames won't match the ACE with ethernet type. **IPv6**: Only IPv6 frames can match this ACE. Notice the IPv6 frames won't match the ACE with Ethernet type.
Action	Specify the action to take with a frame that hits this ACE. **Permit**: The frame that hits this ACE is granted permission for the ACE operation. **Deny**: The frame that hits this ACE is dropped. **Filter**: Frames matching the ACE are filtered.
Rate Limiter	Specify the rate limiter in number of base units. The allowed range is **1** to **16**. **Disabled** indicates that the rate limiter operation is disabled.
Port Redirect	Frames that hit the ACE are redirected to the port number specified here. The rate limiter will affect these ports. The allowed range is the same as the switch port number range. **Disabled** indicates that the port redirect operation is disabled and the specific port number of 'Port Redirect' can't be set when action is permitted.
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The rate limiter will not affect frames on the mirror port. The allowed values are: **Enabled**: Frames received on the port are mirrored. **Disabled**: Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Specify the logging operation of the ACE. Notice that the logging message doesn't include the 4 bytes CRC information. The allowed values are: **Enabled**: Frames matching the ACE are stored in the System Log. **Disabled**: Frames matching the ACE are not logged.

Label	Description
	Note: The logging feature only works when the packet length is less than 1518(without VLAN tags) and the System Log memory size and logging rate is limited.
Shutdown	Specify the port shut down operation of the ACE. The allowed values are: **Enabled**: If a frame matches the ACE, the ingress port will be disabled. **Disabled**: Port shut down is disabled for the ACE. Note: The shutdown feature only works when the packet length is less than 1518(without VLAN tags).
Counter	The counter indicates the number of times the ACE was hit by a frame.

Table 2.40 Description of ACL Configuration with MAC Parameters

Label	Description
SMAC Filter	*(Only displayed when the frame type is Ethernet Type or ARP.)* Specify the source MAC filter for this ACE. **Any**: No SMAC filter is specified. (SMAC filter status is "don't-care".) **Specific**: If you want to filter a specific source MAC address with this ACE, choose this value. A field for entering a SMAC value appears.
SMAC Value	When "Specific" is selected for the SMAC filter, you can enter a specific source MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this SMAC value.
DMAC Filter	Specify the destination MAC filter for this ACE. **Any**: No DMAC filter is specified. (DMAC filter status is "don't-care".) **MC**: Frame must be multicast. **BC**: Frame must be broadcast. **UC**: Frame must be unicast. **Specific**: If you want to filter a specific destination MAC address with this ACE, choose this value. A field for entering a DMAC value appears.
DMAC Value	When "Specific" is selected for the DMAC filter, you can enter a specific destination MAC address. The legal format is "xx-xx-xx-xx-xx-xx" or "xx.xx.xx.xx.xx.xx" or "xxxxxxxxxxxx" (x is a hexadecimal digit). A frame that hits this ACE matches this DMAC value.

Table 2.41 Description of ACL Configuration with VLAN Parameters

Label	Description	Factory Default
802.1Q Tagged	Specify whether frames can hit the action according to the 802.1Q tagged. The allowed values are: **Any**: Any value is allowed ("don't-care"). **Enabled**: Tagged frame only. **Disabled**: Untagged frame only. The default value is "Any".	Any
VLAN ID Filter	Specify the VLAN ID filter for this ACE. **Any**: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".) **Specific**: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears.	Any
VLAN ID	When "Specific" is selected for the VLAN ID filter, you can enter a specific VLAN ID number. The allowed range is **1** to **4095**. A frame that hits this ACE matches this VLAN ID value.	1

Label	Description	Factory Default
Tag Priority	Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is **0** to **7** or range **0-1**, **2-3**, **4-5**, **6-7**, **0-3** and **4-7**. The value **Any** means that no tag priority is specified (tag priority is "don't-care".)	Any

Table 2.42 Description of ACL Configuration with ARP Parameters

Label	Description	Factory Default
ARP/RARP	Specify the available ARP/RARP opcode (OP) flag for this ACE. **Any**: No ARP/RARP OP flag is specified. (OP is "don't-care".) **ARP**: Frame must have ARP opcode set to ARP. **RARP**: Frame must have RARP opcode set to RARP. **Other**: Frame has unknown ARP/RARP Opcode flag.	Any
Request/Reply	Specify the available Request/Reply opcode (OP) flag for this ACE. **Any**: No Request/Reply OP flag is specified. (OP is "don't-care".) **Request**: Frame must have ARP Request or RARP Request OP flag set. **Reply**: Frame must have ARP Reply or RARP Reply OP flag.	Any
Sender IP Filter	Specify the sender IP filter for this ACE. **Any**: No sender IP filter is specified. (Sender IP filter is "don't-care".) **Host**: Sender IP filter is set to Host. Specify the sender IP address in the SIP Address field that appears. **Network**: Sender IP filter is set to Network. Specify the sender IP address and sender IP mask in the SIP Address and SIP Mask fields that appear.	Any
Sender IP Address	When "Host" or "Network" is selected for the sender IP filter, you can enter a specific sender IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.	-
Sender IP Mask	When "Network" is selected for the sender IP filter, you can enter a specific sender IP mask in dotted decimal notation.	-
Target IP Filter	Specify the target IP filter for this specific ACE. **Any**: No target IP filter is specified. (Target IP filter is "don't-care".) **Host**: Target IP filter is set to Host. Specify the target IP address in the Target IP Address field that appears. **Network**: Target IP filter is set to Network. Specify the target IP address and target IP mask in the Target IP Address and Target IP Mask fields that appear.	Any
Target IP Address	When "Host" or "Network" is selected for the target IP filter, you can enter a specific target IP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.	-
Target IP Mask	When "Network" is selected for the target IP filter, you can enter a specific target IP mask in dotted decimal notation.	-
ARP Sender MAC Match	Specify whether frames can hit the action according to their sender hardware address field (SHA) settings. **0**: ARP frames where SHA is not equal to the SMAC address. **1**: ARP frames where SHA is equal to the SMAC address. **Any**: Any value is allowed ("don't-care").	Any
RARP Target MAC Match	Specify whether frames can hit the action according to their target hardware address field (THA) settings. **0**: RARP frames where THA is not equal to the target MAC address.	Any

Label	Description	Factory Default
	1: RARP frames where THA is equal to the target MAC address. **Any**: Any value is allowed ("don't-care").	
IP/Ethernet Length	Specify whether frames can hit the action according to their ARP/RARP hardware address length (HLN) and protocol address length (PLN) settings. **0**: ARP/RARP frames where the HLN is not equal to Ethernet (0x06) or the (PLN) is not equal to IPv4 (0x04). **1**: ARP/RARP frames where the HLN is equal to Ethernet (0x06) and the (PLN) is equal to IPv4 (0x04). **Any**: Any value is allowed ("don't-care").	Any
IP	Specify whether frames can hit the action according to their ARP/RARP hardware address space (HRD) settings. **0**: ARP/RARP frames where the HLD is not equal to Ethernet (1). **1**: ARP/RARP frames where the HLD is equal to Ethernet (1). **Any**: Any value is allowed ("don't-care").	Any
Ethernet	Specify whether frames can hit the action according to their ARP/RARP protocol address space (PRO) settings. **0**: ARP/RARP frames where the PRO is not equal to IP (0x800). **1**: ARP/RARP frames where the PRO is equal to IP (0x800). **Any**: Any value is allowed ("don't-care").	Any

Table 2.43 Description of ACL Configuration with IPv4 Parameters

Label	Description	Factory Default
IP Protocol Filter	Specify the IP protocol filter for this ACE. **Any**: No IP protocol filter is specified ("don't-care"). **Specific**: If you want to filter a specific IP protocol filter with this ACE, choose this value. A field for entering an IP protocol filter appears. **ICMP**: Select ICMP to filter IPv4 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. **UDP**: Select UDP to filter IPv4 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. **TCP**: Select TCP to filter IPv4 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.	Any
IP Protocol Value	When "Specific" is selected for the IP protocol value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IP protocol value.	-
IP TTL	Specify the Time-to-Live settings for this ACE. **zero**: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry. **non-zero**: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. **Any**: Any value is allowed ("don't-care").	Any
IP Fragment	Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame. **No**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. **Yes**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than	Any

Label	Description	Factory Default
	zero must be able to match this entry. **Any**: Any value is allowed ("don't-care").	
IP Option	Specify the options flag setting for this ACE. **No**: IPv4 frames where the options flag is set must not be able to match this entry. **Yes**: IPv4 frames where the options flag is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").	Any
SIP Filter	Specify the source IP filter for this ACE. **Any**: No source IP filter is specified. (Source IP filter is "don't-care".) **Host**: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears. **Network**: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear.	Any
SIP Address	When "Host" or "Network" is selected for the source IP filter, you can enter a specific SIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.	-
SIP Mask	When "Network" is selected for the source IP filter, you can enter a specific SIP mask in dotted decimal notation.	-
DIP Filter	Specify the destination IP filter for this ACE. **Any**: No destination IP filter is specified. (Destination IP filter is "don't-care".) **Host**: Destination IP filter is set to Host. Specify the destination IP address in the DIP Address field that appears. **Network**: Destination IP filter is set to Network. Specify the destination IP address and destination IP mask in the DIP Address and DIP Mask fields that appear.	Any
DIP Address	When "Host" or "Network" is selected for the destination IP filter, you can enter a specific DIP address in dotted decimal notation. Notice the invalid IP address configuration is acceptable too, for example, 0.0.0.0. Normally, an ACE with invalid IP address will explicitly adding deny action.	-
DIP Mask	When "Network" is selected for the destination IP filter, you can enter a specific DIP mask in dotted decimal notation.	-

Table 2.44 Description of ACL Configuration with IPv6 Parameters

Label	Description	Factory Default
Next Header Filter	Specify the IPv6 next header filter for this ACE. **Any**: No IPv6 next header filter is specified ("don't-care"). **Specific**: If you want to filter a specific IPv6 next header filter with this ACE, choose this value. A field for entering an IPv6 next header filter appears. **ICMP**: Select ICMP to filter IPv6 ICMP protocol frames. Extra fields for defining ICMP parameters will appear. These fields are explained later in this help file. **UDP**: Select UDP to filter IPv6 UDP protocol frames. Extra fields for defining UDP parameters will appear. These fields are explained later in this help file. **TCP**: Select TCP to filter IPv6 TCP protocol frames. Extra fields for defining TCP parameters will appear. These fields are explained later in this help file.	Any
Next Header Value	When "Specific" is selected for the IPv6 next header value, you can enter a specific value. The allowed range is **0** to **255**. A frame that hits this ACE matches this IPv6 protocol value.	-

Label	Description	Factory Default
SIP Filter	Specify the source IPv6 filter for this ACE. **Any**: No source IPv6 filter is specified. (Source IPv6 filter is "don't-care".) **Specific**: Source IPv6 filter is set to Network. Specify the source IPv6 address and source IPv6 mask in the SIP Address fields that appear.	Any
SIP Address	When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 address. The field only supported last 32 bits for IPv6 address.	-
SIP BitMask	When "Specific" is selected for the source IPv6 filter, you can enter a specific SIPv6 mask. The field only supported last 32 bits for IPv6 address. Notice the usage of bitmask, if the binary bit value is "0", it means this bit is "don't-care". The real matched pattern is [sipv6_address & sipv6_bitmask] (last 32 bits). For example, if the SIPv6 address is 2001::3 and the SIPv6 bitmask is 0xFFFFFFFE (bit 0 is "don't-care" bit), then SIPv6 address 2001::2 and 2001::3 are applied to this rule.	-
Hop Limit	Specify the hop limit settings for this ACE. **zero**: IPv6 frames with a hop limit field greater than zero must not be able to match this entry. **non-zero**: IPv6 frames with a hop limit field greater than zero must be able to match this entry. **Any**: Any value is allowed ("don't-care").	Any

Table 2.45 Description of ACL Configuration with ICMP Parameters

Label	Description	Factory Default
ICMP Type Filter	Specify the ICMP filter for this ACE. **Any**: No ICMP filter is specified (ICMP filter status is "don't-care"). **Specific**: If you want to filter a specific ICMP filter with this ACE, you can enter a specific ICMP value. A field for entering an ICMP value appears.	Any
ICMP Type Value	When "Specific" is selected for the ICMP filter, you can enter a specific ICMP value. The allowed range is **0** to **255**. A frame that hits this ACE matches this ICMP value.	-
ICMP Code Filer	Specify the ICMP code filter for this ACE. **Any**: No ICMP code filter is specified (ICMP code filter status is "don't-care"). **Specific**: If you want to filter a specific ICMP code filter with this ACE, you can enter a specific ICMP code value. A field for entering an ICMP code value appears.	Any
ICMP Code Value	When "Specific" is selected for the ICMP code filter, you can enter a specific ICMP code value. The allowed range is **0** to **255**. A frame that hits this ACE matches this ICMP code value.	-

Table 2.46 Description of ACL Configuration with TCP/UDP Parameters

Label	Description	Factory Default
TCP/UDP Source Filter	Specify the TCP/UDP source filter for this ACE. **Any**: No TCP/UDP source filter is specified (TCP/UDP source filter status is "don't-care"). **Specific**: If you want to filter a specific TCP/UDP source filter with this ACE, you can enter a specific TCP/UDP source value. A field for entering a TCP/UDP source value appears. **Range**: If you want to filter a specific TCP/UDP source range filter with this	Any

Label	Description	Factory Default
	ACE, you can enter a specific TCP/UDP source range value. A field for entering a TCP/UDP source value appears.	
TCP/UDP Source No.	When "Specific" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.	-
TCP/UDP Source Range	When "Range" is selected for the TCP/UDP source filter, you can enter a specific TCP/UDP source range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP source value.	-
TCP/UDP Destination Filter	Specify the TCP/UDP destination filter for this ACE. **Any**: No TCP/UDP destination filter is specified (TCP/UDP destination filter status is "don't-care"). **Specific**: If you want to filter a specific TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination value. A field for entering a TCP/UDP destination value appears. **Range**: If you want to filter a specific range TCP/UDP destination filter with this ACE, you can enter a specific TCP/UDP destination range value. A field for entering a TCP/UDP destination value appears.	Any
TCP/UDP Destination Number	When "Specific" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value	-
TCP/UDP Destination Range	When "Range" is selected for the TCP/UDP destination filter, you can enter a specific TCP/UDP destination range value. The allowed range is **0** to **65535**. A frame that hits this ACE matches this TCP/UDP destination value.	-
TCP FIN	Specify the TCP "No more data from sender" (FIN) value for this ACE. **0**: TCP frames where the FIN field is set must not be able to match this entry. **1**: TCP frames where the FIN field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").	Any
TCP SYN	Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE. **0**: TCP frames where the SYN field is set must not be able to match this entry. **1**: TCP frames where the SYN field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").	Any
TCP RST	Specify the TCP "Reset the connection" (RST) value for this ACE. **0**: TCP frames where the RST field is set must not be able to match this entry. **1**: TCP frames where the RST field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").	Any
TCP PSH	Specify the TCP "Push Function" (PSH) value for this ACE. **0**: TCP frames where the PSH field is set must not be able to match this entry. **1**: TCP frames where the PSH field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").	Any
TCP ACK	Specify the TCP "Acknowledgment field significant" (ACK) value for this ACE. **0**: TCP frames where the ACK field is set must not be able to match this entry. **1**: TCP frames where the ACK field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care").	Any
TCP URG	Specify the TCP "Urgent Pointer field significant" (URG) value for this ACE. **0**: TCP frames where the URG field is set must not be able to match this entry. **1**: TCP frames where the URG field is set must be able to match this entry. **Any**: Any value is allowed ("don't-care")	Any

Table 2.47 Description of ACL Configuration with Ethernet Type Parameters

Label	Description	Factory Default
EtherType Filter	Specify the Ethernet type filter for this ACE. **Any**: No EtherType filter is specified (EtherType filter status is "don't-care"). **Specific**: If you want to filter a specific EtherType filter with this ACE, you can enter a specific EtherType value. A field for entering an EtherType value appears.	-
Ethernet Type Value	When "Specific" is selected for the EtherType filter, you can enter a specific EtherType value. The allowed range is **0x600** to **0xFFFF** but excluding 0x800(IPv4), 0x806(ARP) and 0x86DD(IPv6). A frame that hits this ACE matches this EtherType value.	-

2.6.2.4 IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host. This is to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address.

2.6.2.4.1 IP Source Guard Configuration

IP Source Guard Configuration webpage is shown in Figure 2.60. For each port, select the option for **Mode** and **Max Dynamic Clients** under the **Port Mode Configuration** table. Table 2.48 describe the options under **IP Source Guard Configuration**.

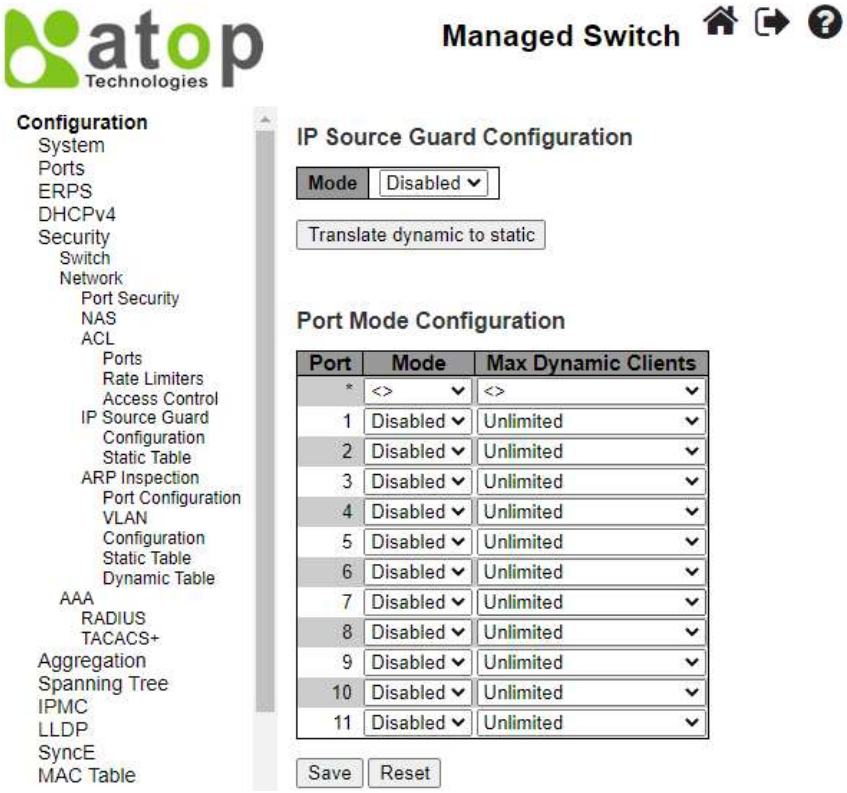


Figure 2.60 Webpage to IP Source Guard Configuration

Table 2.48 Descriptions of Network IP Source Guard Configuration

Label	Description	Factory Default
IP Source Guard Configuration		
Mode	Enable the Global IP Source Guard or disable the Global IP Source Guard. All configured ACEs will be lost when the mode is enabled.	Disabled
Port Mode Configuration		
Mode	Specify IP Source Guard is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, IP Source Guard is enabled on this given port.	Disabled
Max Dynamic Clients	Specify the maximum number of dynamic clients that can be learned on given port. This value can be 0, 1, 2 or unlimited. If the port mode is enabled and the value of max dynamic client is equal to 0, it means only allow the IP packets forwarding that are matched in static entries on the specific port.	Unlimited

Click the **Save** buttons to save changes. Click **Reset** buttons to undo any changes made locally and revert to previously saved values. Click **Translate dynamic to static** button to translate all dynamic entries to static entries.

2.6.2.4.2 IP Source Guard Static Table

The user can configure staic **IP Source Guard Static** rules in this webpage. The user can add a new entry to the **IP Soruce Guard table** as shown in Figure 2.61. The maximum number of rules is 112 on the switch. Table 2.49 summarizes the column labels for Static IP Source Guard Table.

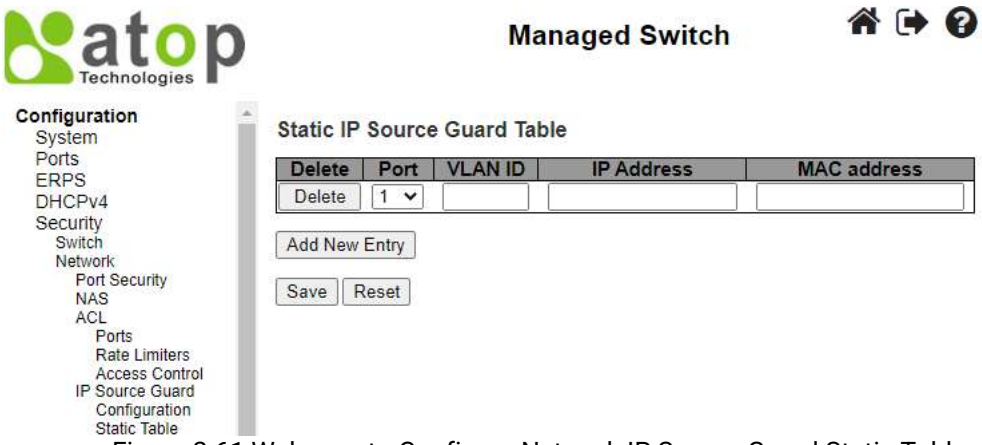


Figure 2.61 Webpage to Configure Network IP Source Guard Static Table

Table 2.49 Descriptions of Network IP Source Guard Static

Label	Description	Factory Default
Delete	Click entry **Delete** button to delete the entry. It will be deleted during the next save.	
Port	The logical port for the settings.	1
VLAN ID	The VLAN Id for the entry.	Null
IP Address	Allowed Source IP address.	Null
MAC Address	Allowed Source MAC address.	Null

Click **Add New Entry** button to add a new entry to the Static IP Source Guard table. Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.6.2.5 ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. For example, man-in-the-middle attack occurs when a malicious

node intercepts packets intended for other nodes by poisoning the ARP caches of its unsuspecting neighbours. To create the attack, the malicious node sends ARP requests or responses mapping another node's IP address to its own MAC address. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device. Figure 2.62 shows the list of submenus under the **Security→Network→ARP Inspection**. It contains **Port Configuration**, **VLAN Configuration**, **Static Table** and **Dynamic Table**.

ARP Inspection
- Port Configuration
- VLAN Configuration
- Static Table
- Dynamic Table

Figure 2.62 ARP Inspection Menu

2.6.2.5.1 Port Configuration

To configure ARP Inspection for port(s) on the managed switch, the users can use the webpage shown in Figure 2.63. First, enable the **ARP Inspection** by selecting the **Mode** option. Then, configure the **Mode**, **Check VLAN** and **Log Type** for each port in the table below. Table 2.50 summarizes the descriptions of column labels of Port Mode Configuration.

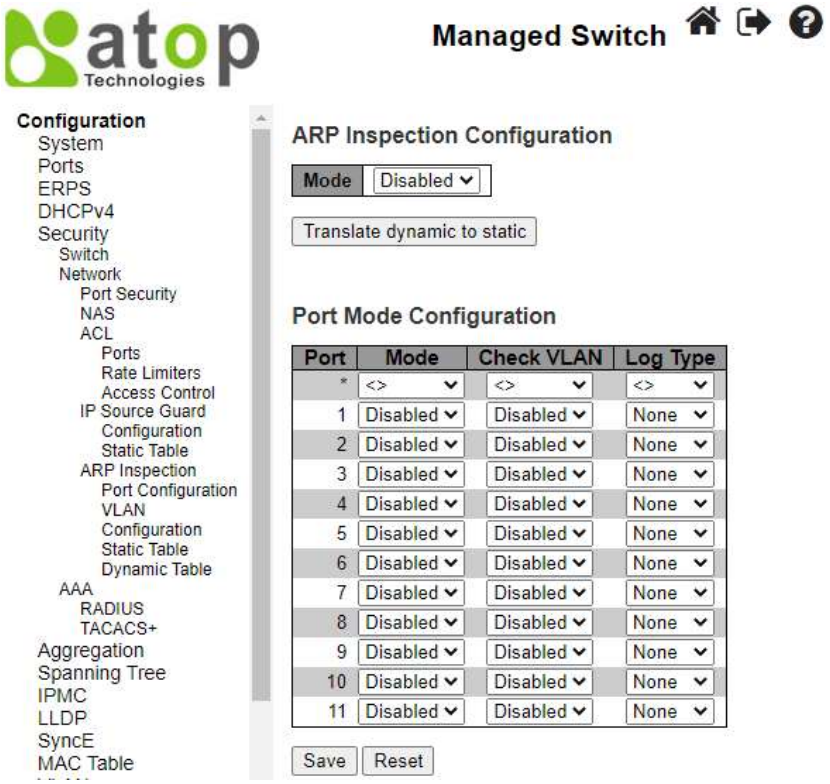


Figure 2.63 Webpage to Configure Network ARP Inspection Port

Table 2.50 Descriptions of ARP Inspection Port Configuration

Label	Description	Factory Default
ARP Inspection Configuration		
Mode	Enable the Global ARP Inspection or disable the Global ARP Inspection.	Disabled
Port Mode Configuration		
Port	Port Number	-
Mode	Specify ARP Inspection is enabled on which ports. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Possible modes are:	Disabled

Label	Description	Factory Default
	Enabled: Enable ARP Inspection operation. **Disabled**: Disable ARP Inspection operation.	
Check VLAN	If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are: **Enabled**: Enable check VLAN operation. **Disabled**: Disable check VLAN operation.	Disabled
Log Type	Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types are: **None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.	None

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values. Click **Translate dynamic to static** button to translate all dynamic entries to static entries.

2.6.2.5.2 VLAN Configuration

Figure 2.64 illustrates the ARP Inspection VLAN Configuration webpage. Each page can show up to 9999 entries from the VLAN table, default being 20. The user can change the number of visible entries through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table.

Clicking the refresh button will update the displayed table starting from that or the closest next VLAN Table match. The right arrow button will use the next entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached the warning, message is shown in the displayed table. Use the left arrow button to start over. Table 2.51 summarizes the column labels of the ARP Inspection VLAN table.

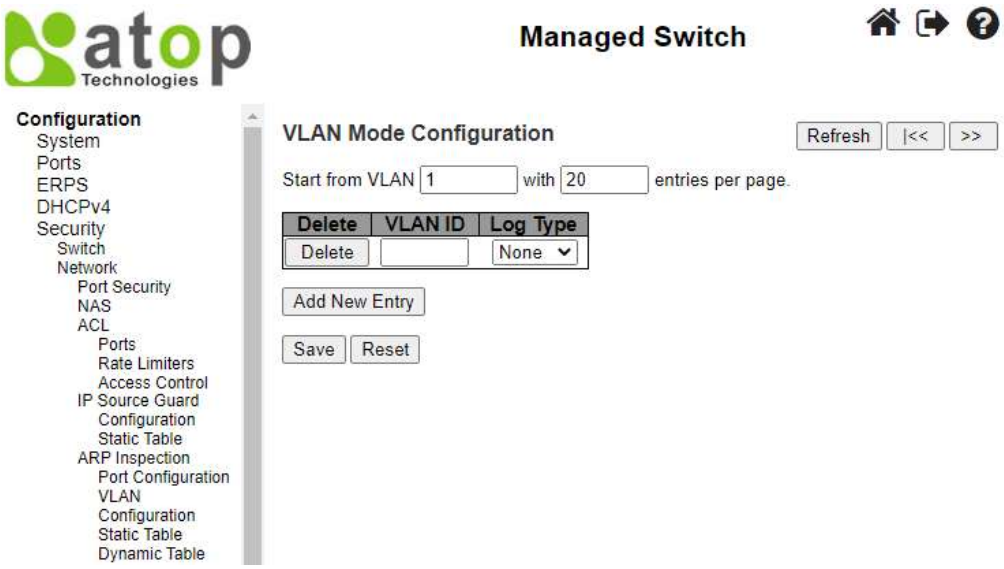


Figure 2.64 Webpage to Configure Network ARP Inspection VLAN

Table 2.51 Descriptions of ARP Inspection VLAN Table

Label	Description	Factory Default
Delete	Click entry Delete button to delete the entry.	-
VLAN ID	Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration webpage (previous subsection). Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page.	-
Log Type	The log type also can be configured on per VLAN setting. Possible types are: **None**: Log nothing. **Deny**: Log denied entries. **Permit**: Log permitted entries. **ALL**: Log all entries.	None

Click **Add New Entry** button to add a new entry to the ARP Inspection VLAN Table. Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.6.2.5.3 Static Table

To configure **Static ARP Inspection** for port(s) on the managed switch, the users can use the webpage shown in Figure 2.65. After click the **Add New Entry** button, select the **Port** number from the drop down. Then, enter the **VLAN ID**, **MAC Address** and **IP Address** for each port to have static ARP Inspection. Table 2.52 summarizes the descriptions of column labels of **Static ARP Inspection Table**.

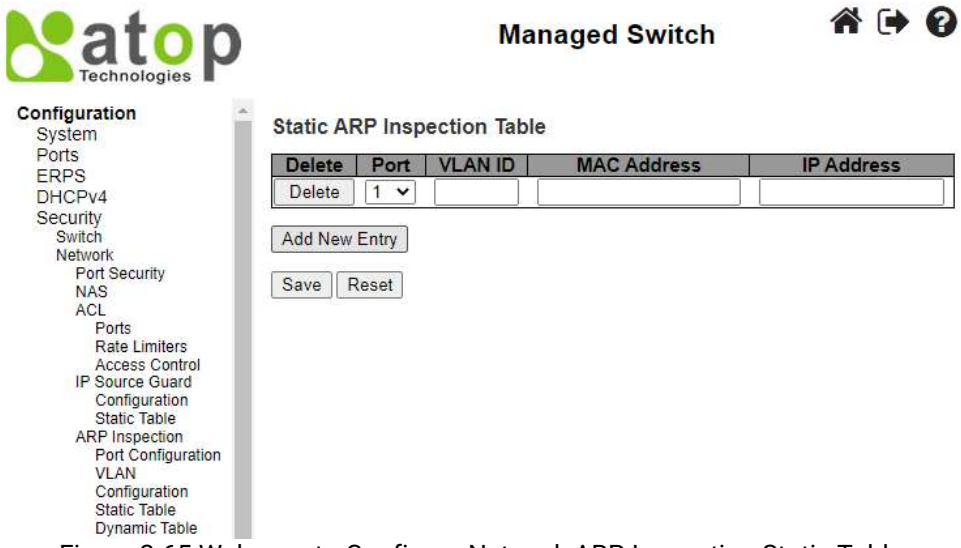


Figure 2.65 Webpage to Configure Network ARP Inspection Static Table

Table 2.52 Descriptions of Static ARP Inspection Table

Label	Description	Factory Default
Delete	Check to delete the entry. It will be deleted during the next save.	-
Port	The logical port for the settings.	1
VLAN ID	The VLAN ID for the settings.	Null
MAC Address	Allowed Source MAC address in ARP request packets.	Null
IP Address	Allowed Source IP address in ARP request packets.	Null

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.6.2.5.4 Dynamic Table

To configure **Dynamic ARP Inspection** for port(s) on the managed switch, the users can use the webpage shown in Figure 2.66. Entries in the **Dynamic ARP Inspection Table** are shown on this page. The **Dynamic ARP Inspection Table** contains up to 256 entries, and is sorted first by port, then by **VLAN ID**, then by **MAC address**, and then by **IP address**. All dynamic entries are learning from DHCP Snooping. Table 2.53 summarizes the descriptions of column labels of **Dynamic ARP Inspection Table**.

Each webpage can show up to 99 entries from the Dynamic ARP Inspection table. The default maximum entries per page is 20. This can be selected through the "**entries per page**" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table.

The "**Start from port address**", "**VLAN**", "**MAC address**" and "**IP address**" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address.
The **>>** button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "**No more entries**" is shown in the displayed table. Use the **|<<** button to start over.

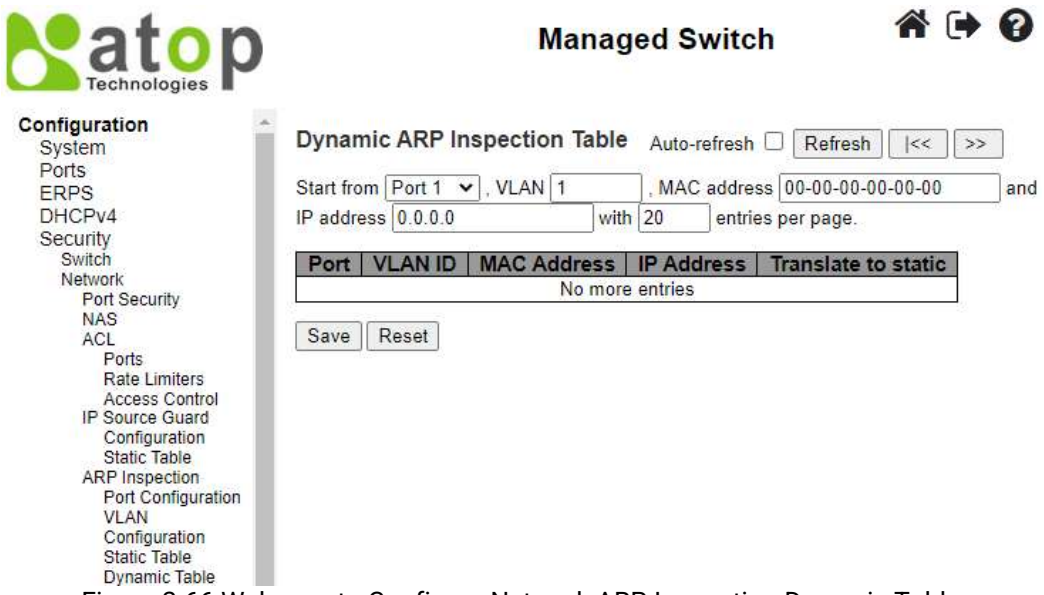


Figure 2.66 Webpage to Configure Network ARP Inspection Dynamic Table

Table 2.53 Descriptions of ARP Inspection Dynamic Table

Label	Description	Factory Default
Port	Switch Port Number for which the entries are displayed.	Port1
VLAN ID	VLAN-ID in which the ARP traffic is permitted.	1
MAC Address	User MAC address of the entry.	00-00-00-00-00-00
IP Address	User IP address of the entry.	0.0.0.0
Translate to static	Select the checkbox to translate the entry to static entry.	-

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.6.3 AAA

The authentication, authorization, and accounting (AAA) features allows you to verify the identity of, grant access to, and track the actions of users managing RHG9728 switches. The RHG9728 switches support **Remote Access Dial-In User Service** (**RADIUS**) or **Terminal Access Controller Access Control System Plus** (**TACACS+**) protocols. Based on the user ID and password combination that users provide, the RHG9728 switches perform local authentication or authorization using the local database or remote authentication or authorization using one or more AAA servers. A preshared secret key provides security for communication between the switch and AAA servers. You can configure a common secret key for all AAA servers or for only a specific AAA server.

AAA security provides the following services:

- **Authentication**—Identifies users, including login and password dialog, challenge and response, messaging support, and encryption depending on the security protocol that you select. Authentication is the process of verifying the identity of the person or device accessing the RHG9728 switches. This process is based on the user ID and password combination provided by the entity trying to access the switch. The RHG9728 switches allow user to perform local authentication (using the local lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).
- **Authorization**—Provides access control. AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in RHG9728 switches is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.
- **Accounting**—Provides the method for collecting information, logging the information locally, and sending the information to the AAA server for billing, auditing, and reporting. The accounting feature tracks and maintains a log of every management session used to access RHG9728 switches. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

AAA increases flexibility and control of access configuration, scalability, standardized authentication methods, such as RADIUS and TACACS+, and multiple backup devices.

2.6.3.1 RADIUS

RADIUS (Remote Authentication Dial in User Service) is an access server that uses authentication, authorization, and accounting (AAA) protocol for authentication and authorization. It is a distributed security system that secures remote access to networks and network services against unauthorized access. The RADIUS specification is described in RFC 2865, which obsoletes RFC 2138. Figure 2.67 shows the **RADIUS Server Configuration** webpage which allows the users to configure up to 5 RADIUS servers. It is divided into two parts: **Global Configuration** and **Server Configuration**. Table 2.54 summarizes the parameters for the **RADIUS Server Configuration**.

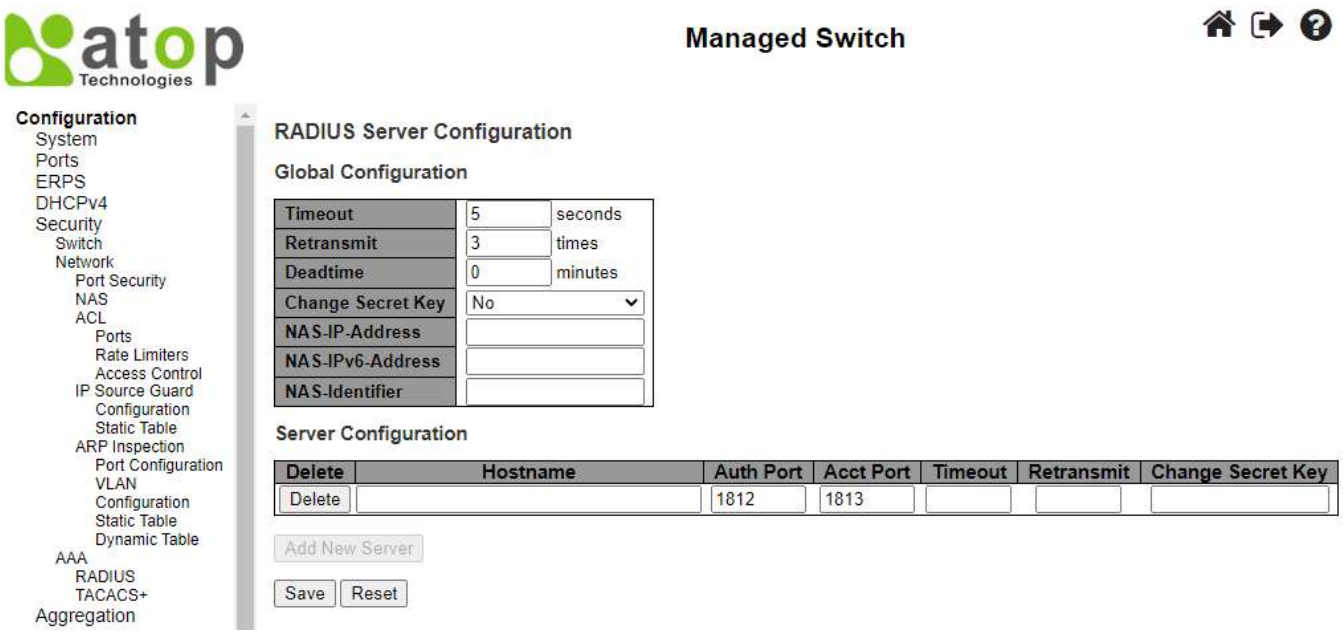


Figure 2.67 Webpage to Configure AAA RADIUS

Table 2.54 Descriptions of AAA RADIUS

Label	Description	Factory Default
Global Configuration		
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a RADIUS server before retransmitting the request.	5
Retransmit	Retransmit is the number of times, in the range 1 to 1000, a RADIUS request is retransmitted to a server that is not responding. If the server has not responded after the last retransmit it is considered to be dead.	3
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.	0
Change Secret Key	Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the RADIUS server and the switch.	No
NAS-IP-Address	The IPv4 address to be used as attribute 4 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.	Null
NAS-IPv6-Address	The IPv6 address to be used as attribute 95 in RADIUS Access-Request packets. If this field is left blank, the IP address of the outgoing interface is used.	Null
NAS-Identifier	The identifier - up to 253 characters long - to be used as attribute 32 in RADIUS Access-Request packets. If this field is left blank, the NAS-Identifier is not included in the packet.	Null
Server Configuration		
Delete	To delete a RADIUS server entry, check this box. The entry will be deleted during the next Save.	
Hostname	The IPv4/IPv6 address or hostname of the RADIUS server.	Null
Auth Port	The UDP port to use on the RADIUS server for authentication. Set to 0 to disable authentication.	1812
Acct Port	The UDP port to use on the RADIUS server for accounting. Set to 0 to disable accounting.	1813
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.	Null
Retransmit	This optional setting overrides the global retransmit value. Leaving it blank will use the global retransmit value.	Null
Change Secret Key	Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.	Null

After clicking on the **Add New Server** button to add a new RADIUS server, an empty row is added to the table, and the RADIUS server can be configured as needed. Up to 5 servers are supported. The **Delete** button can be used to undo the addition of the new server. Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.6.3.2 TACACS+

TACACS+ is an acronym for Terminal Access Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

TACACS+ (Terminal Access Controller Access-Control System Plus) TACACS+ is **a remote authentication protocol**, which allows a remote access server to communicate with an authentication server to validate user access onto the network. TACACS+ allows a client to accept a username and password, and pass a query to a TACACS+ authentication server. Table 2.55 compares the differences between the RADIUS and TACACS+.

Table 2.55 Comparison of Authentication Server Settings between RADIUS and TACACS+

	RADIUS	**TACACS+**
Transport Protocol	UDP	TCP
Authentication and Authorization	Separates AAA	Combines authentication and authorization
Multiprotocol Support	No	Yes, support AppleTalk Remote Access (ARA) and NetBIOS protocol
Confidentiality	Only password is encrypted	Entire packet is encrypted

Figure 2.68 shows the TACACS+ Server Configuration webpage. It consists of Global Configuration and Server Configuration parts. Table 2.56 summarizes descriptions of parameters for setting up the TACACS+ Server.

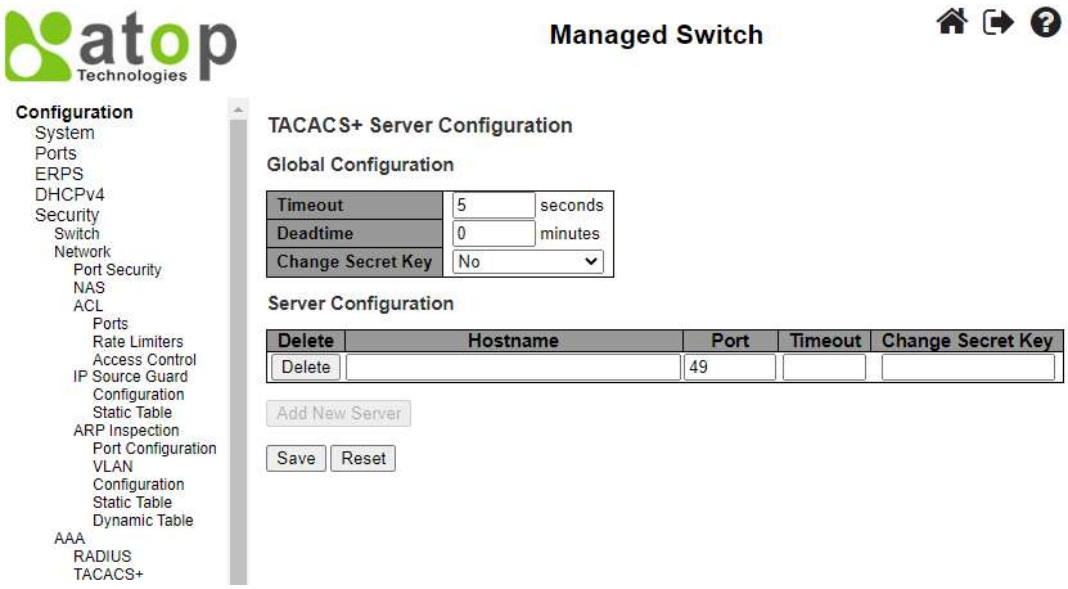


Figure 2.68 Webpage to Configure AAA TACACS+

Table 2.56 Descriptions of AAA RADIUS

Label	**Description**	**Factory Default**
Global Configuration		
Timeout	Timeout is the number of seconds, in the range 1 to 1000, to wait for a reply from a TACACS+ server before it is considered to be dead.	5
Deadtime	Deadtime, which can be set to a number between 0 to 1440 minutes, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Deadtime to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.	0
Change Secret Key	Specify to change the secret key or not. When "Yes" is selected for the option, you can change the secret key - up to 63 characters long - shared between the TACACS+ server and the switch.	No

Label	Description	Factory Default
Server Configuration		
Delete	To delete a TACACS+ server entry, check this box. The entry will be deleted during the next Save.	
Hostname	The IPv4/IPv6 address or hostname of the TACACS+ server.	Null
Port	The TCP port to use on the TACACS+ server for authentication.	49
Timeout	This optional setting overrides the global timeout value. Leaving it blank will use the global timeout value.	Null
Change Secret Key	Specify to change the secret key or not. When the checkbox is checked, you can change the setting overrides the global key. Leaving it blank will use the global key.	Null

After clicking on the **Add New Server** button to add a new TACACS+ server, an empty row is added to the table, and the TACACS+ server can be configured as needed. Up to 5 servers are supported. The **Delete** button can be used to undo the addition of the new server. Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.7 Aggregation

Aggregation is a technique to use multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability. Atop's RHG9728 allows the aggregation on its ports. Figure 2.69 lists the submenus under the **Configuration→Aggregation**.

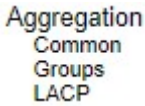


Figure 2.69 Aggregation Submenus

2.7.1 Common

The webpage in Figure 2.70 is used to configure the Aggregation hash mode. The configured mode is applied to the whole network elements. Four contributors can be selected and used to create the hash code which are Source MAC Address, Destination MAC Address, IP Address, and TCP/UDP Port Number. Table 2.57 summarizes the descriptions of hash code contributors under the Common Aggregation Configuration.

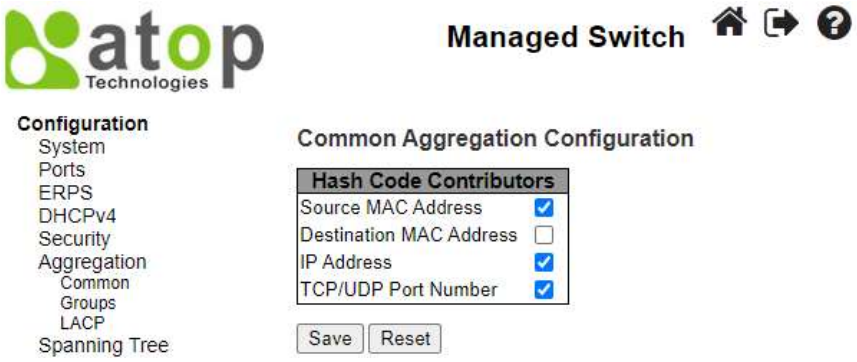


Figure 2.70 Webpage to Configure Common Aggregation

Table 2.57 Descriptions of Common Aggregation Configuration

Label	Description	Factory Default
Hash Code Contributors		

Label	Description	Factory Default
Source MAC Address	The Source MAC address can be used to calculate the destination port for the frame. Check to enable the use of the Source MAC address, or uncheck to disable. By default, Source MAC Address is enabled.	Checked
Destination MAC Address	The Destination MAC Address can be used to calculate the destination port for the frame. Check to enable the use of the Destination MAC Address, or uncheck to disable. By default, Destination MAC Address is disabled.	Unchecked
IP Address	The IP address can be used to calculate the destination port for the frame. Check to enable the use of the IP Address, or uncheck to disable. By default, IP Address is enabled.	Checked
TCP/UDP Port Number	The TCP/UDP port number can be used to calculate the destination port for the frame. Check to enable the use of the TCP/UDP Port Number, or uncheck to disable. By default, TCP/UDP Port Number is enabled.	Checked

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.7.2 Groups

This webpage allows the user to aggregate different port(s) to an aggregation group. The **Aggregation Group Configuration** is shown in Figure 2.71. After selecting which port number(s) belong to which aggregation group ID, the user can choose the mode of aggregation group from **Disabled**, **Static**, **LACP (Active)**, **LACP (Passive)**. Table 2.58 summarizes the descriptions of **Aggregation Group Configuration**.

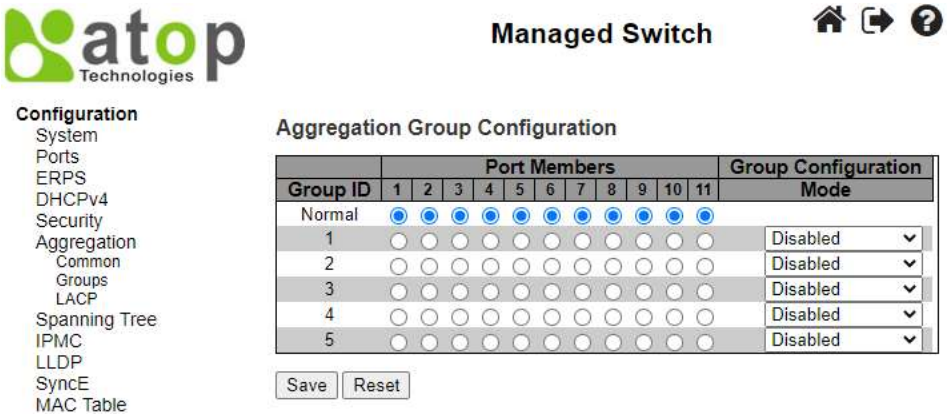


Figure 2.71 Webpage to Configure Group Aggregation

Table 2.58 Descriptions of Aggregation Group Configuration

Label	Description	Factory Default
Group ID	Indicates the aggregation group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.	-
Port Members	Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.	Unclicked
Mode	This parameter determines the mode for the aggregation group. • **Disabled:** The group is disabled. • **Static:** The group operates in static aggregation mode. • **LACP (Active):** The group operates in LACP active aggregation mode. See IEEE 801.AX-2014, Section 6.4.1 for details.	Disabled

Label	Description	Factory Default
	• **LACP (Passive):** The group operates in LACP passive aggregation mode. See IEEE 801.AX-2014, Section 6.4.1 for details.	

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.7.3 LACP

The users have an option to enable **Link Aggregation Control Protocol** (**LACP**) which is an IEEE standard (IEEE 802.3ad, IEEE 802.1AX-2008) by selecting on LACP aggregation mode in previous subsection. LACP allows the managed switch to negotiate an automatic bundling of links by sending LACP packets to the LACP partner or another device that is directly connected to the managed switch and also implements LACP. The LACP packets will be sent within a multicast group MAC address. If LACP finds a device on the other end of the link that also has LACP enabled, it will also independently send packets along the same links enabling the two units to detect multiple links between themselves and then combine them into a single logical link. During the detection period LACP packets are transmitted every second. Subsequently, keep alive mechanism for link membership will be sent periodically. Each port in the group can also operate in either LACP active or LACP passive modes. The LACP active mode means that the port will enable LACP unconditionally, while LACP passive mode means that the port will enable LACP only when an LACP partner is detected. Note that in active mode LACP port will always send LACP packets along the configured links. In passive mode however, LACP port acts as “speak when spoken to”, and therefore can be used as a way of controlling accidental loops (as long as the other device is in active mode).

Figure 2.72 shows the LACP System Configuration webpage. It allows the user to configure the System Priority and LACP System Configuration. Table 2.59 summarizes the descriptions of LACP Aggregation Configuration.

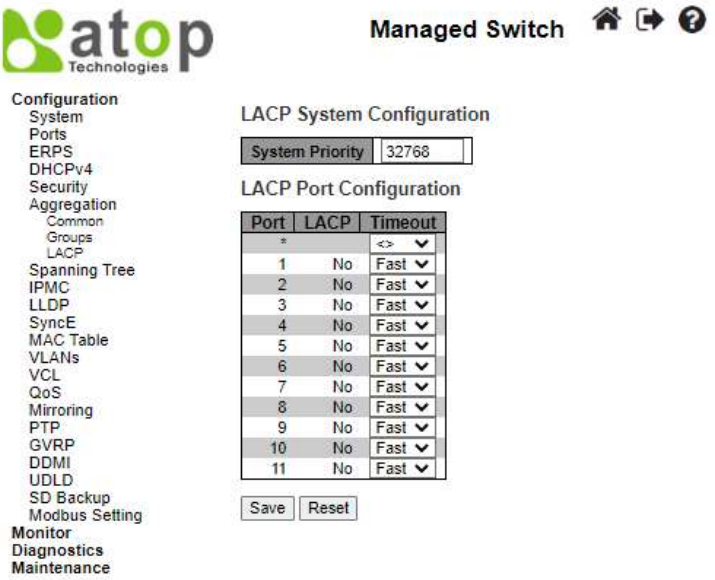


Figure 2.72 Webpage to Configure LACP Aggregation

Table 2.59 Descriptions of LACP Aggregation Configuration

Label	Description	Factory Default
Port	The switch port number.	-
LACP	Show whether LACP is currently enabled on this switch port.	No
Timeout	The **Timeout** controls the period between BPDU transmissions. **Fast** will transmit LACP packets each second, while **Slow** will wait for 30 seconds before sending a LACP packet.	Fast

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.8 Spanning Tree

IEEE 802.1D Standard spanning tree functionality is supported by Atop's RHG9728 managed switches.

Spanning Tree Protocol (STP) provides a function to prevent switching loops and broadcast radiation at the OSI layer 2. A switching loop occurs in a network when there are multiple connections or redundant paths between two network switches or at least two ports are connected on both sides of the two network switches. The switching loop can create a broadcast radiation, which is the accumulation of broadcast and multicast traffics in a computer network. As broadcast and multicast messages are forwarded by bridges/switches to every port, the bridges/switches will repeatedly rebroadcast the broadcast messages, and this accumulation of traffic can flood the network. STP creates a spanning tree topology and disables those links of the network that are not part of the spanning tree, which leaves only a single active path between two nodes. This function can avoid flooding and increase network efficiency. Therefore, Atop's managed switches deploy spanning tree as a tool when the users set up connection or port redundancy or fault-tolerance in their network.

RSTP (Rapid Spanning Tree Protocol), IEEE 802.1W, is also supported in Atop's managed switches. It is an evolution of the STP, but it is still backwards compatible with standard STP. RSTP has the advantage over the STP. When there is a topology change such as link failure in the network, the RSTP will converge significantly faster to a new spanning tree topology. RSTP improves convergence on point-to-point links by reducing the Max-Age time to 3 times Hello interval, removing the STP listening state, and exchanging a handshake between two switches to quickly transition the port to forwarding state.

MSTP (Multiple Spanning Tree Protocol) is also a standard defined by the IEEE 802.1s that allows multiple VLANs to be mapped to a single spanning tree instance called MST Instance, which will provide multiple pathways across the network. It is compatible with STP and RSTP. To support lager network, MSTP groups bridges/switches into regions that appear as a single bridge to other devices. Within each region, there can be multiple MST instances. MSTP shares common parameters as RSTP such as port path costs. MSTP also help prevent switching loop and has rapid convergence when there is a topology change. It is possible to have different forwarding paths for different MST instances. This enables load balancing of network traffic across redundant links.

The following subsections describe how to setup the **spanning tree protocol (STP)**, **rapid spanning tree protocol (RSTP)**, and **Multiple Spanning Tree Protocol (MSTP)**. The **Spanning Tree** menu consists of **Bridge Settings**, **MSTI Mapping**, **MSTI Priorities**, **CIST Ports**, and **MSTI Ports**.

2.8.1 Bridge Settings

To select a variant of Spanning Tree Protocol, the user can select the Protocol Version and set related parameters for that particular protocol version in this STP Bridge Configuration webpage as shown in Figure 2.73. The settings are grouped into Basic Settings and Advanced Settings. These settings are used by all STP Bridge instances in the managed switch. Table 2.60 summarizes the description of each parameter under the STP Bridge Configuration webpage.

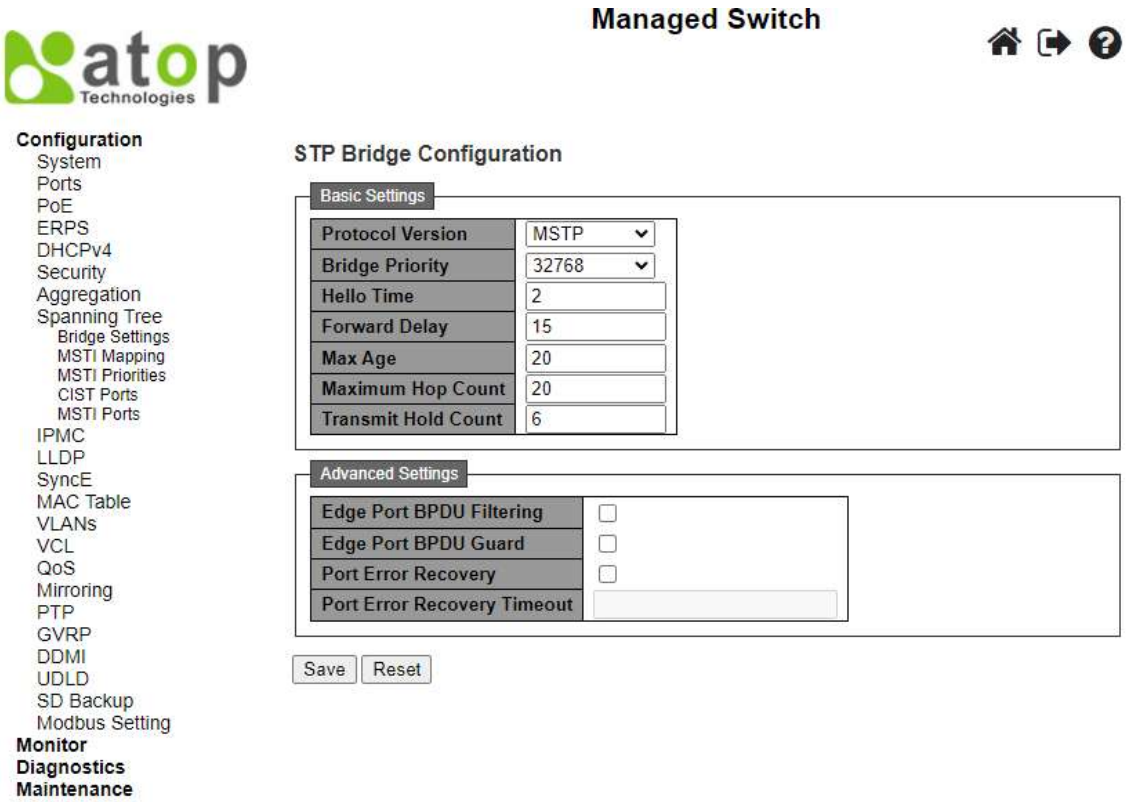


Figure 2.73 Webpage to Configure Bridge Settings of Spanning Tree

Table 2.60 Descriptions of Bridge Settings Configuration of Spanning Tree

Label	Description	Factory Default
	Basic Settings	
Protocol Version	The MSTP / RSTP / STP protocol version setting.	MSTP
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*. For **MSTP** operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.	32768
Hello Time	The interval between sending STP BPDU's. Valid values are in the range 1 to 10 seconds, default is 2 seconds. *Note: Changing this parameter from the default value is not recommended, and may have adverse effects on your network.*	2
Forward Delay	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.	15
Max Age	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, *and* MaxAge must be <= (FwdDelay-1)*2.	20
Maximum Hop Count	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information to. Valid values are in the range 6 to 40 hops.	20

Label	Description	Factory Default
Transmit Hold Count	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second.	6
Advanced Settings		
Edge Port BPDU Filtering	Control whether a port explicitly configured as Edge will transmit and receive BPDUs.	Unclicked
Edge Port BPDU Guard	Control whether a port explicitly configured as Edge will disable itself upon reception of a BPDU. The port will enter the error-disabled *state,* and will be removed from the active topology.	Unclicked
Port Error Recovery	Control whether a port in the error-disabled state automatically will be enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.	Unclicked
Port Error Recovery Timeout	The time to pass before a port in the error-disabled state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).	Null

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.8.2 MSTI Mapping

MSTI Mapping webpage is shown in Figure 2.74. This page allows the user to inspect and/or change the current STP MSTI bridge VLAN Mapping configurations. The **MSTI Configuration** consists of **Configuration Identification** part **and MSTI Mapping** part. Table 2.61 summarizes the description of parameters under MSTI Configuration.

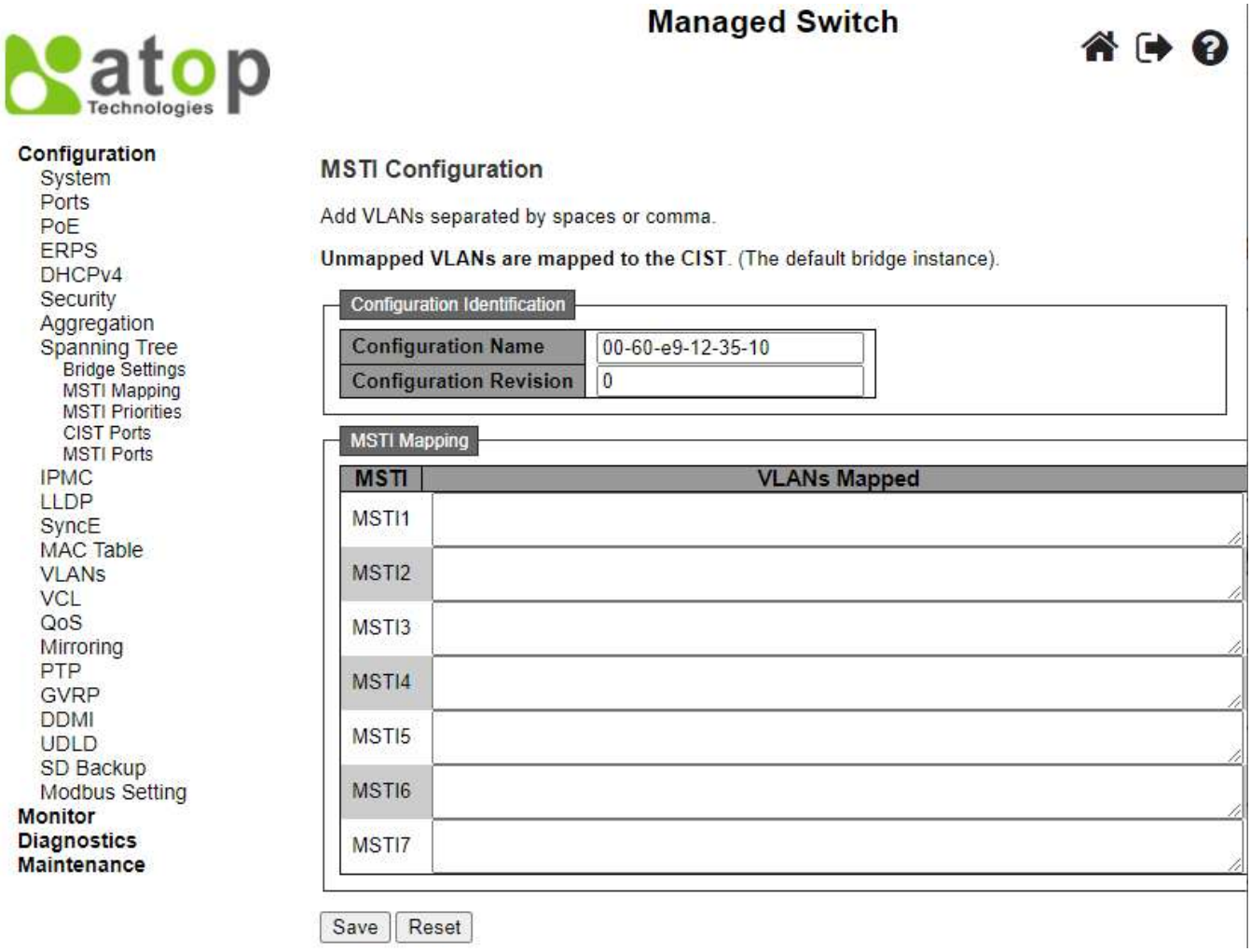


Figure 2.74 Webpage to Configure MSTI Mapping of Spanning Tree

Table 2.61 Descriptions of Bridge Priorities Configuration of Spanning Tree

Label	Description	Factory Default
Configuration Identification		
Configuration Name	The name identifying the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configuration in order to share spanning trees for MSTI's (Intra-region). The name is at most 32 characters.	DUT's MAC address
Configuration Revision	The revision of the MSTI configuration named above. This must be an integer between 0 and 65535.	0
MSTI Mapping		
MSTI	The bridge instances. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.	
VLANs Mapped	The list of VLANs mapped to the MSTI. The VLANs can be given as a single (**xx**, xx being between 1 and 4094) VLAN, or a range (**xx-yy**), each of which must be separated with comma and/or space. A VLAN can only be mapped to *one* MSTI. An unused MSTI should just be left empty. (I.e., not having any VLANs mapped to it.) Example: **2, 5, 20-40**.	Null

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.8.3 MSTI Priorities

MSTI Priorities webpage is shown in Figure 2.75. This page allows the user to inspect and/or change the current STP MSTI bridge instance priority configurations. Table 2.62 summarizes the description of parameters under MSTI Configuration.

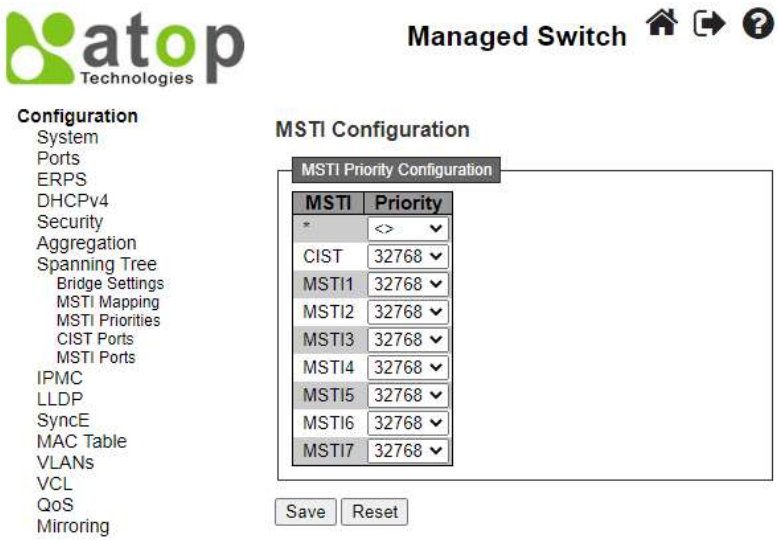


Figure 2.75 Webpage to Configure Bridge Priorities of Spanning Tree

Table 2.62 Descriptions of Bridge MSTI Priorities Configuration of Spanning Tree

Label	Description	Factory Default
MSTI	The bridge instances. The CIST is the default instance, which is always active.	-
Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a Bridge Identifier.	32768

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.8.4 CIST Ports

The **CIST Ports** webpage in Figure 2.76 allows the user to inspect and change the current STP CIST port configurations. This page contains settings for physical and aggregated ports. There are two tables: **CIST Aggregated Port Configuration** and **CIST Normal Port Configuration**. Table 2.63 provides the descriptions of all column labels of the two tables under the STP CIST Port Configuration.

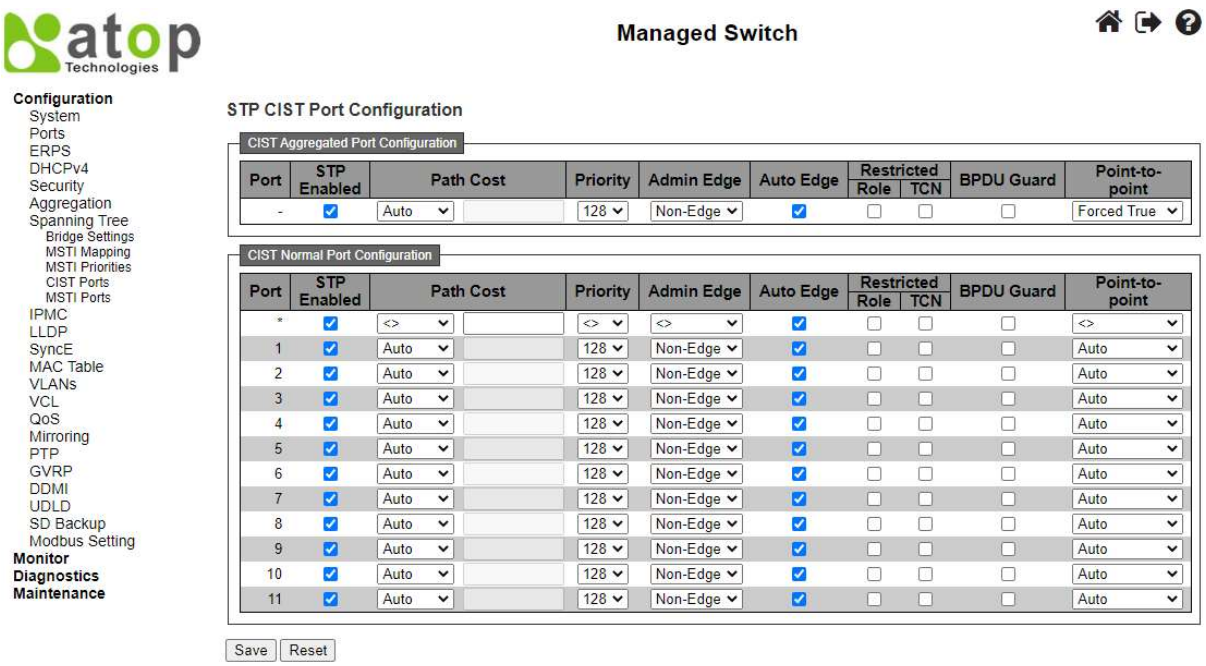


Figure 2.76 Webpage to Configure CIST Ports of Spanning Tree

Table 2.63 Descriptions of CIST Ports Configuration of Spanning Tree

Label		Description	Factory Default
CIST Aggregated Port Configuration			
Port		The switch port number of the logical STP port.	-
STP Enabled		Controls whether STP is enabled on this switch port.	Unchecked
Path Cost		Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.	Auto
Priority		Controls the port priority. This can be used to control priority of ports having identical port cost. (See above). Lower priority is better.	128
Admin Edge		Admin Edge or State Flag. Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.	Non-Edge
Auto Edge		Controls whether the bridge should enable automatic edge detection on the bridge port. This allows *operEdge* to be derived from whether BPDU's are received on the port or not.	Checked
Restricted	**Role**	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.	Unchecked
	TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active	Unchecked

Label		Description	Factory Default
		topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.	
BPDU Guard		If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not affect this setting. A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.	Unchecked
Point-to-point		Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.	Forced True
CIST Normal Port Configuration			
Port		The switch port number of the logical STP port.	-
STP Enabled		Controls whether STP is enabled on this switch port.	Unchecked
Path Cost		Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.	Auto
Priority		Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).	128
Admin Edge		Admin Edge or State Flag. Operational flag describing whether the port is connecting directly to edge devices. (No Bridges attached). Transition to the forwarding state is faster for edge ports (having operEdge true) than for other ports. The value of this flag is based on AdminEdge and AutoEdge fields. This flag is displayed as Edge in Monitor->Spanning Tree -> STP Detailed Bridge Status.	Non-Edge
Auto Edge		Controls whether the bridge should enable automatic edge detection on the bridge port. This allows operEdge to be derived from whether BPDU's are received on the port or not.	Checked
Restricted	**Role**	If enabled, causes the port not to be selected as Root Port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an Alternate Port after the Root Port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.	Unchecked
	TCN	If enabled, causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.	Unchecked
BPDU Guard		If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port **Edge** status does not affect this setting.	Unchecked

Label	Description	Factory Default
	A port entering error-disabled state due to this setting is subject to the bridge Port Error Recovery setting as well.	
Point-to-point	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media.	Auto

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.8.5 MSTI Ports

The MSTI Ports webpage as shown in Figure 2.77 allows the user to inspect and/or change the current STP MSTI port configurations. An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options. After selecting a desired MSTI and clicking on the **Get** button, the webpage is updated as shown in Figure 2.78. The updated page contains MSTI port settings for physical and aggregated ports. Table 2.64 summarizes the descriptions of MSTI Port Configuration.

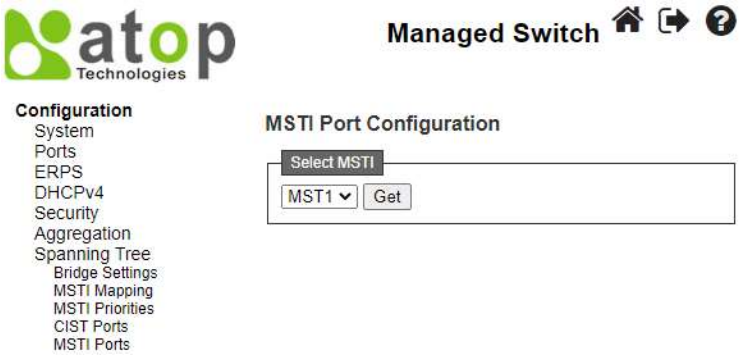


Figure 2.77 Webpage to Configure MSTI of Spanning Tree

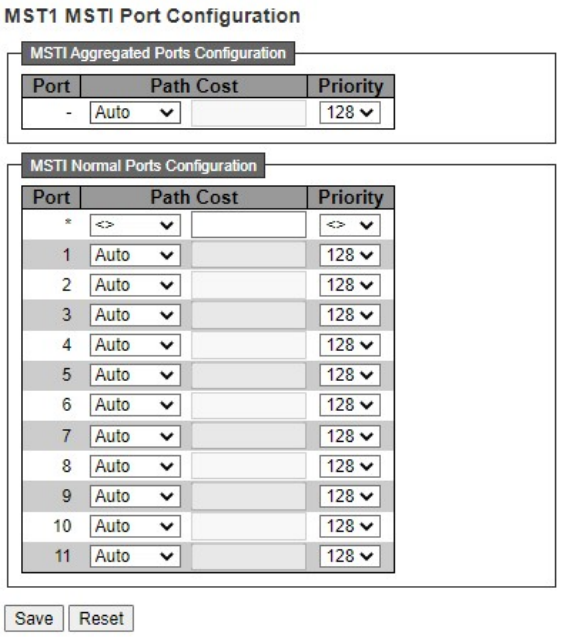


Figure 2.78 Example of MST1 MSTI Port Configuration

Table 2.64 Descriptions of MSTI Configuration of Spanning Tree

Label	Description	Factory Default
Port	The switch port number of the corresponding STP CIST (and MSTI) port.	MST1
Path Cost	Controls the path cost incurred by the port. The **Auto** setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the **Specific** setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.	Auto
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. Lower priority is better.	128

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.9 IPMC

IP MultiCast (IPMC) menu can be configured using the submenus as shown in Figure 2.79. The IGMP Snooping is used for IPv4, while the MLD Snooping is used for IPv6.

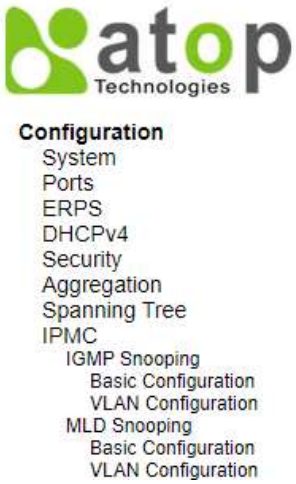


Figure 2.79 Configuration->IPMC Menu

2.9.1 IGMP Snooping

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

2.9.1.1 Basic Configuration

IGMP Snooping→Basic Configuration webpage provides IGMP Snooping related configuration as shown in Figure 2.80. The page consists of **Global Configuration** and **Port Related Configuration**. Table 2.65 summarizes the descriptions of IGMP Snooping Configuration.

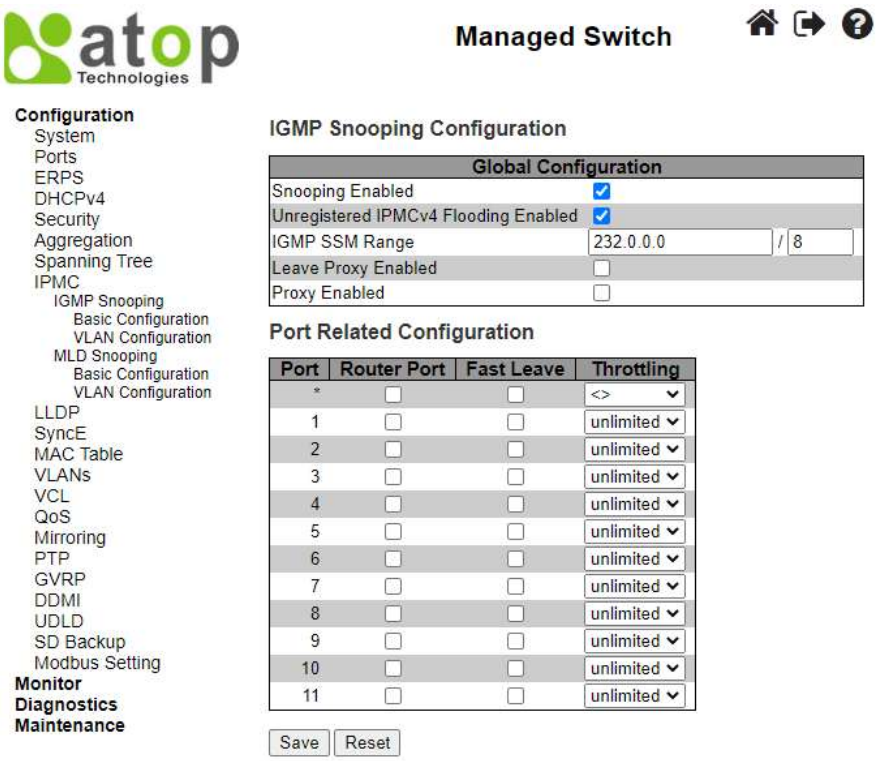


Figure 2.80 Basic Configuration Webpage to IGMP Snooping of an IPMC Profile

Table 2.65 Descriptions of IGMP Snooping of an IPMC Profile

Label	Description	Factory Default
IGMP Snooping Configuration		
Snooping Enabled	Enable the Global IGMP Snooping.	Clicked
Unregistered IPMCv4 Flooding Enabled	Enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active in spite of this setting.	Clicked
IGMP SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Assign valid IPv4 multicast address as prefix with a prefix length (from 4 to 32) for the range.	232.0.0.0 / 8
Leave Proxy Enabled	Enable IGMP Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.	Unclicked
Proxy Enabled	Enable IGMP Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.	Unclicked
Port Related Configuration		
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.	Unclicked
Fast Leave	Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the IGMPv2 leave message without sending last member query messages. It is recommended to enable this feature only when a single IGMPv2 host is connected to the specific port.	Unclicked
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.	unlimited

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.9.1.2 VLAN Configuration

IGMP Snooping VLAN Configuration is shown in Figure 2.81. Note that the user needs to enter IP configuration page (**System→IP→Add IP interface**) to setup IP interface first before the creation of IGMP VLAN interface. The IGMP Snooping VLAN table is also displayed on this webpage. Each page can show up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match. The **>>** button will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the **<<** button to start over. Table 2.66 summarizes the descriptions of the IGMP Snooping VLAN Configuration.

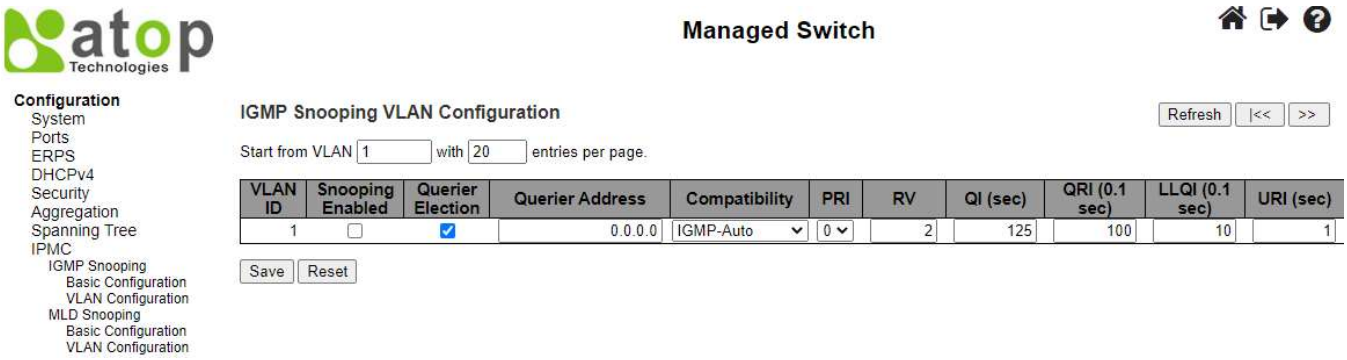


Figure 2.81 Webpage to Configure IGMP Snooping's VLAN for an IPMC Profile

Table 2.66 Descriptions of IGMP Snooping's VLAN Configuration for an IPMC Profile

Label	Description	Factory Default
VLAN ID	The VLAN ID of the entry.	1
Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 8 VLANs can be selected for IGMP Snooping.	Unchecked
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.	Checked
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 0.0.0.0.	0.0.0.0
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network. The allowed selection is **IGMP-Auto**, **Forced IGMPv1**, **Forced IGMPv2**, **Forced IGMPv3**, default compatibility value is IGMP-Auto.	IGMP-Auto
PRI	Priority of Interface. It indicates the IGMP control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is 0 (best effort) to 7 (highest), default interface priority value is 0.	0
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a network. The allowed range is 1 to 255, default robustness variable value is 2.	2

Label	Description	Factory Default
QI (sec)	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is 1 to 31744 seconds, default query interval is 125 seconds.	125
QRI (0.1 sec)	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is 0 to 31744 in tenths of seconds, default query response interval is 100 in tenths of seconds (10 seconds).	100
LLQI (0.1 sec)	Last Member Query Interval. The Last Member Query Time is the time value represented by the Last Member Query Interval, multiplied by the Last Member Query Count. The allowed range is 0 to 31744 in tenths of seconds, default last member query interval is 10 in tenths of seconds (1 second).	10
URI (sec)	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a host's initial report of membership in a group. The allowed range is 0 to 31744 seconds, default unsolicited report interval is 1 second.	1

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.9.2 MLD Snooping

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

2.9.2.1 Basic Configuration

MLD Snooping→Basic Configuration webpage provides IGMP Snooping related configuration as shown in Figure 2.82. The page consists of **Global Configuration** and **Port Related Configuration**. Table 2.67 summarizes the descriptions of MLD Snooping Configuration.

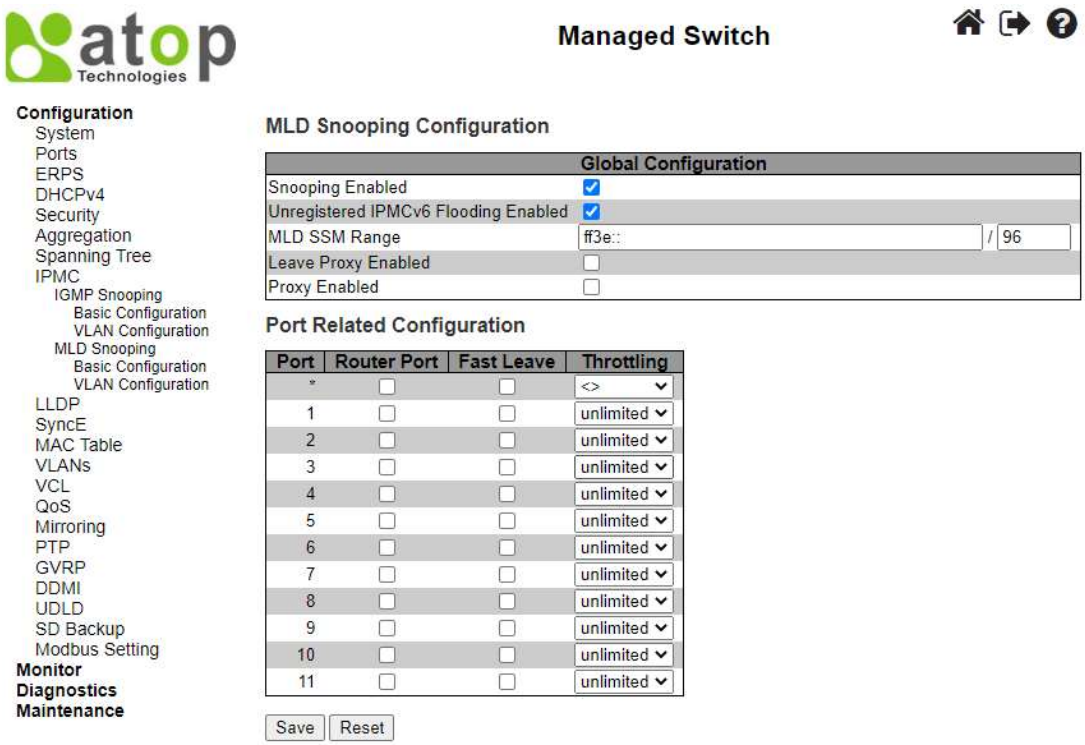


Figure 2.82 Basic Configuration Webpage to MLD Snooping of an IPMC Profile

Table 2.67 Descriptions of MLD Snooping Configuration for an IPMC Profile

Label	Description	Factory Default
MLD Snooping Configuration		
Snooping Enabled	Enable the Global MLD Snooping.	Clicked
Unregistered IPMCv6 Flooding Enabled	Enable unregistered IPMCv6 traffic flooding. The flooding control takes effect only when MLD Snooping is enabled. When MLD Snooping is disabled, unregistered IPMCv6 traffic flooding is always active in spite of this setting.	Clicked
MLD SSM Range	SSM (Source-Specific Multicast) Range allows the SSM-aware hosts and routers run the SSM service model for the groups in the address range. Assign valid IPv6 multicast address as prefix with a prefix length (from 8 to 128) for the range.	ff3e::/96
Leave Proxy Enabled	Enable MLD Leave Proxy. This feature can be used to avoid forwarding unnecessary leave messages to the router side.	Unclicked
Proxy Enabled	Enable MLD Proxy. This feature can be used to avoid forwarding unnecessary join and leave messages to the router side.	Unclicked
Port Related Configuration		
Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.	Unclicked
Fast Leave	Enable the fast leave on the port. System will remove group record and stop forwarding data upon receiving the MLDv1 leave message without sending last member query messages. It is recommended to enable this feature only when a single MLDv1 host is connected to the specific port.	Unclicked
Throttling	Enable to limit the number of multicast groups to which a switch port can belong.	unlimited

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.9.2.2 VLAN Configuration

MLD Snooping VLAN Configuration is shown in Figure 2.83. Note that the user needs to enter IP configuration page (**System→IP→Add IP interface**) to setup IP interface first before the creation of MLD VLAN interface. The MLD Snooping VLAN table is also displayed on this webpage. Each page can show up to 99 entries from the VLAN table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input fields allow the user to select the starting point in the VLAN Table. Clicking the **Refresh** button will update the displayed table starting from that or the next closest VLAN Table match. The **>>** will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the **|<<** arrow button to start over. Table 2.68 summarizes the descriptions of the MLD Snooping VLAN Configuration.

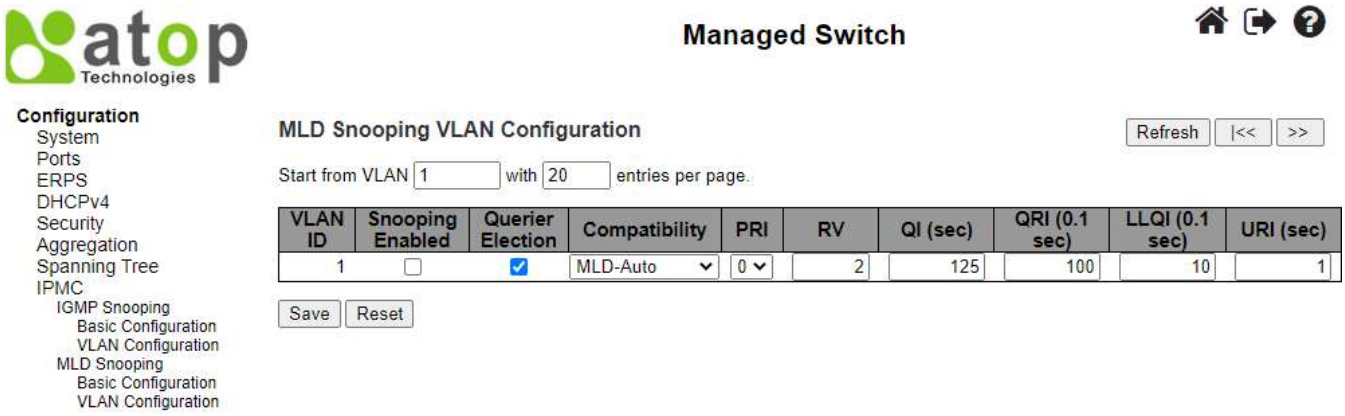


Figure 2.83 Webpage to Configure MLD Snooping's VLAN for an IPMC Profile

Table 2.68 Descriptions of MLD Snooping's VLAN Configuration for an IPMC Profile

Label	Description	Factory Default
VLAN ID	The VLAN ID of the entry.	
MLD Snooping Enabled	Enable the per-VLAN MLD Snooping. Up to **8** VLANs can be selected for MLD Snooping.	Unclicked
Querier Election	Enable to join MLD Querier election in the VLAN. Disable to act as an MLD Non-Querier.	Clicked
Compatibility	Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of MLD operating on hosts and routers within a network. The allowed selection is **MLD-Auto**, **Forced MLDv1**, **Forced MLDv2**, default compatibility value is MLD-Auto.	MLD-Auto
PRI	Priority of Interface. It indicates the MLD control frame priority level generated by the system. These values can be used to prioritize different classes of traffic. The allowed range is **0** (best effort) to **7** (highest), default interface priority value is 0.	0
RV	Robustness Variable. The Robustness Variable allows tuning for the expected packet loss on a link. The allowed range is **1** to **255**, default robustness variable value is 2.	2
QI (sec)	Query Interval. The Query Interval is the interval between General Queries sent by the Querier. The allowed range is **1** to **31744** seconds. Default query interval is 125 seconds.	125
QRI (0.1 sec)	Query Response Interval. The Maximum Response Delay used to calculate the Maximum Response Code inserted into the periodic General Queries. The allowed range is **0** to **31744** in tenths of seconds. Default query response interval is 100 in tenths of seconds (10 seconds).	100
LLQI (0.1 sec)	Last Listener Query Interval. The Last Listener Query Interval is the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address Specific Queries sent in response to Version 1 Multicast Listener Done messages. It is also the Maximum Response Delay used to calculate the Maximum Response Code inserted into Multicast Address and Source Specific Query messages. The allowed range is **0** to **31744** in tenths of seconds. Default last listener query interval is 10 in tenths of seconds (1 second).	10
URI (sec)	Unsolicited Report Interval. The Unsolicited Report Interval is the time between repetitions of a node's initial report of interest in a multicast address. The allowed range is **0** to **31744** seconds. Default unsolicited report interval is 1 second.	1

Click **Refreshes** button to refresh the displayed table starting from the "VLAN" input fields. Click **|<<** button to update the table starting from the first entry in the VLAN Table, i.e., the entry with the lowest VLAN ID. Click **>>** button to update the table, starting with the entry after the last entry currently displayed. Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.10 LLDP

Link Layer Discovery Protocol (**LLDP**) is an IEEE802.1ab standard OSI layer-2 protocol. LLDP allows Ethernet network devices to advertise details about themselves, such as device configuration, capabilities and identification. The advertise packets are periodically sent to directly connected devices on the network that are also using LLDP or so called its neighbours. LLDP is a "one hop" unidirectional protocol in an advertising mode.

LLDP information can only be sent to and received by devices, no solicit information or state changes between nodes. The device has a choice to turn on and off sending and receiving function independently. Advertised information is not forward on to other devices on the network. LLDP is designed to be managed with SNMP. Applications that use this protocol include topology discovery, inventory management, emergency services, VLAN assignment, and inline power supply.

2.10.1 LLDP

The **LLDP** webpage allows the user to inspect and configure the current LLDP interface settings as shown in Figure 2.84. The page consists of **LLDP Parameters** and **LLDP Interface Configuration**. Table 2.69 summarizes the descriptions of the **LLDP Configuration**.

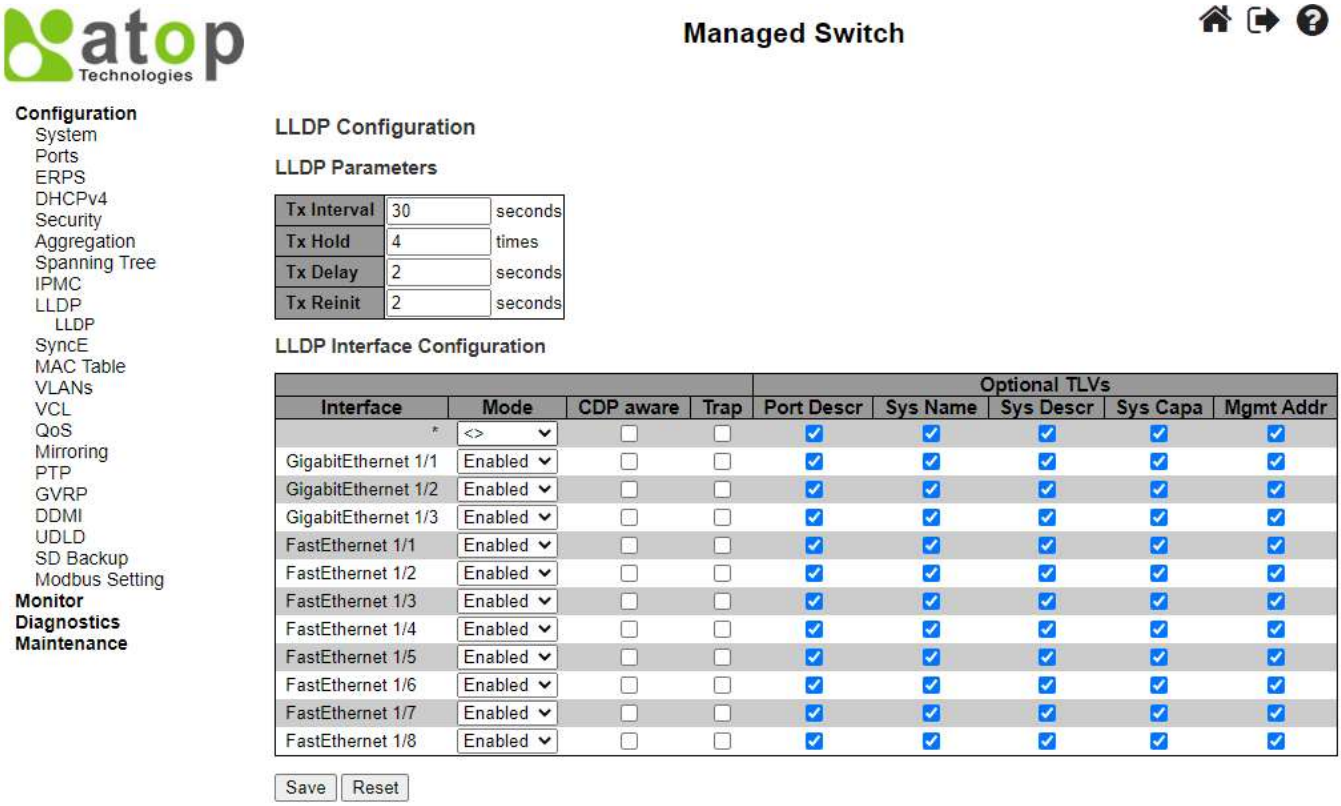


Figure 2.84 Webpage to Configure LLDP

Table 2.69 Descriptions of LLDP Configuration

Label	Description	Factory Default
LLDP Parameters		
Tx Interval	The switch periodically transmits LLDP frames to its neighbours for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. Valid values are restricted to 5 - 32768 seconds.	30
Tx Hold	Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid	4

Label	Description	Factory Default
	period is set to **Tx Hold** multiplied by **Tx Interval** seconds. Valid values are restricted to 2 - 10 times.	
Tx Delay	If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. Valid values are restricted to 1 - 8192 seconds.	2
Tx Reinit	When an interface is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighbouring units, signalling that the LLDP information isn't valid anymore. **Tx Reinit** controls the number of seconds between the shutdown frame and a new LLDP initialization. Valid values are restricted to 1 - 10 seconds.	2
LLDP Interface Configuration		
Interface	The switch interface name of the logical LLDP interface.	GigabitEthernet or FastEthernet
Mode	Select LLDP mode. **Rx only** The switch will not send out LLDP information, but LLDP information from neighbour units is analysed. **Tx only** The switch will drop LLDP information received from neighbours, but will send out LLDP information. **Disabled** The switch will not send out LLDP information, and will drop LLDP information received from neighbours. **Enabled** The switch will send out LLDP information, and will analyse LLDP information received from neighbours.	Disabled
CDP Aware	Select CDP awareness. The CDP operation is restricted to decoding incoming CDP frames (The switch doesn't transmit CDP frames). CDP frames are only decoded if LLDP on the interface is enabled. Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbours' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped onto LLDP neighbours' table as shown below. CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field. CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbours table. CDP TLV "Port ID" is mapped to the LLDP "Port ID" field. CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field. Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbours' table. If all interfaces have CDP awareness disabled the switch forwards CDP frames received from neighbour devices. If at least one interface has CDP awareness enabled all CDP frames are terminated by the switch. Note: When CDP awareness on an interface is disabled the CDP information isn't removed immediately, but gets removed when the hold time is exceeded.	Unclicked
Port Descr	Optional TLV: When checked the "port description" is included in LLDP information transmitted.	Unclicked
Sys Name	Optional TLV: When checked the "system name" is included in LLDP information transmitted.	Clicked
Sys Descr	Optional TLV: When checked the "system description" is included in LLDP information transmitted.	Clicked

Label	Description	Factory Default
Sys Capa	Optional TLV: When checked the "system capability" is included in LLDP information transmitted.	Clicked
Mgmt Addr	Optional TLV: When checked the "management address" is included in LLDP information transmitted.	Clicked

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.11 MAC Table

Unicast and Multicast MAC addresses in the memory, which is the MAC Address Table, of the managed switch can be configured in this webpage as shown in Figure 2.85. The user can set timeouts for entries (called ageing time) in the dynamic MAC Table and configure the static MAC table. The MAC Address Table Configuration webpage consists of four parts: **Aging Configuration**, **MAC Table Learning**, **VLAN Learning Configuration**, and **Static MAC Table Configuration**.

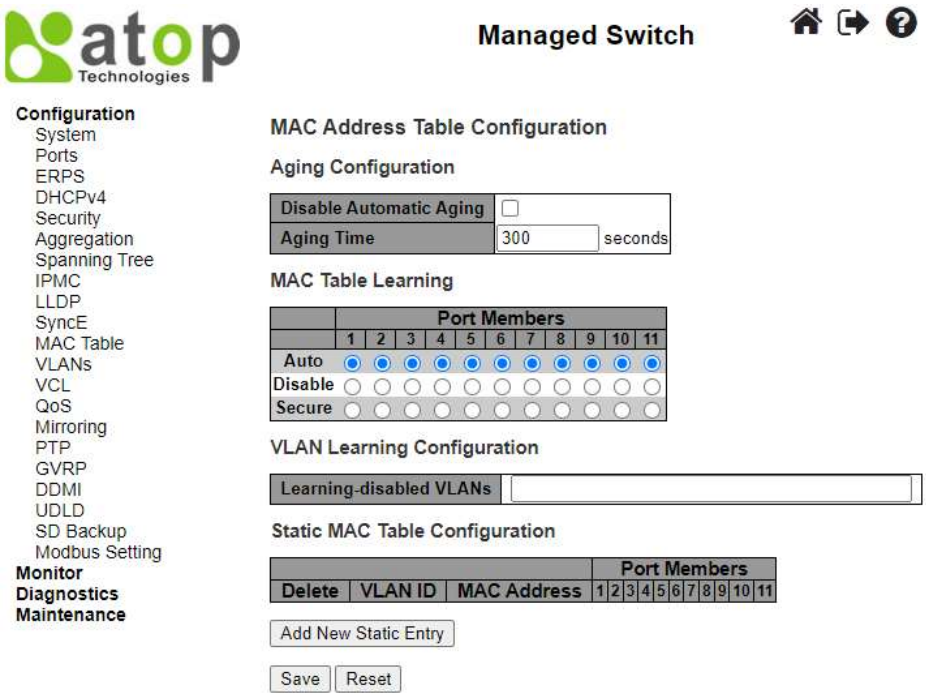


Figure 2.85 Webpage to Configure MAC Table

Table 2.70 Description of MAC Address Table Configuration

Label	Description	Factory Default
Aging Configuration		
Disable Automatic Aging	Disable the automatic aging of dynamic entries by checking the box.	Unclicked
Aging time	Configure aging time by entering a value in this field in unit of seconds. The allowed range is 10 to 1000000 seconds. By default, dynamic entries are removed from the MAC Table after 300 seconds. This removal is also called aging.	300
MAC Table Learning		

Label	Description	Factory Default
Note: If the learning mode for a given port is greyed out, another module is in control of the mode, so that it cannot be changed by the user. An example of such a module is the MAC-based Authentication under 802.1X. Each port can do learning based upon the following settings:		
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.	-
Disable	No learning is done.	-
Secure	Only static MAC entries are learned, all other frames are dropped. **Note:** Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.	-
VLAN Learning Configuration		
Learning-disabled VLANs	This field shows the Learning-disabled VLANs. When a NEW MAC arrives into a learning-disabled VLAN, the MAC won't be learnt. By the default, the field is empty. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters.	Null
Static MAC Table Configuration Note: The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The MAC table is sorted first by VLAN ID and then by MAC address.		
Delete	Check to delete the entry. It will be deleted during the next save.	-
VLAN ID	The VLAN ID of the entry.	-
MAC Address	The MAC address of the entry.	-
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry.	-
Adding a New Static Entry	Click **Add New Static Entry** button to add a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "**Save**".	-

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.12 VLANs

VLAN or Virtual LAN is a method to restrict communication between switch ports. At layer 2, the network is partitioned into multiple, distinct, mutually isolated broadcast domains. A Virtual Local Area Network (VLAN) is a group of devices that can be located anywhere on a network, but all devices in the group are logically connected together. In other words, VLAN allows end stations to be grouped together even if they are not located on the same network switch. With a traditional network, users usually spend a lot of time on devices relocations, but a VLAN reconfiguration can be performed entirely through software. Also, VLAN provides extra security because devices within a VLAN group can only communicate with other devices in the same group. For the same reason, VLAN can help to control network traffic. Traditional network broadcasts data to all devices, no matter whether they need it or not. By allowing a member to receive data only from other members in the same VLAN group, VLAN avoids broadcasting and increases traffic efficiency (see Figure 2.86).

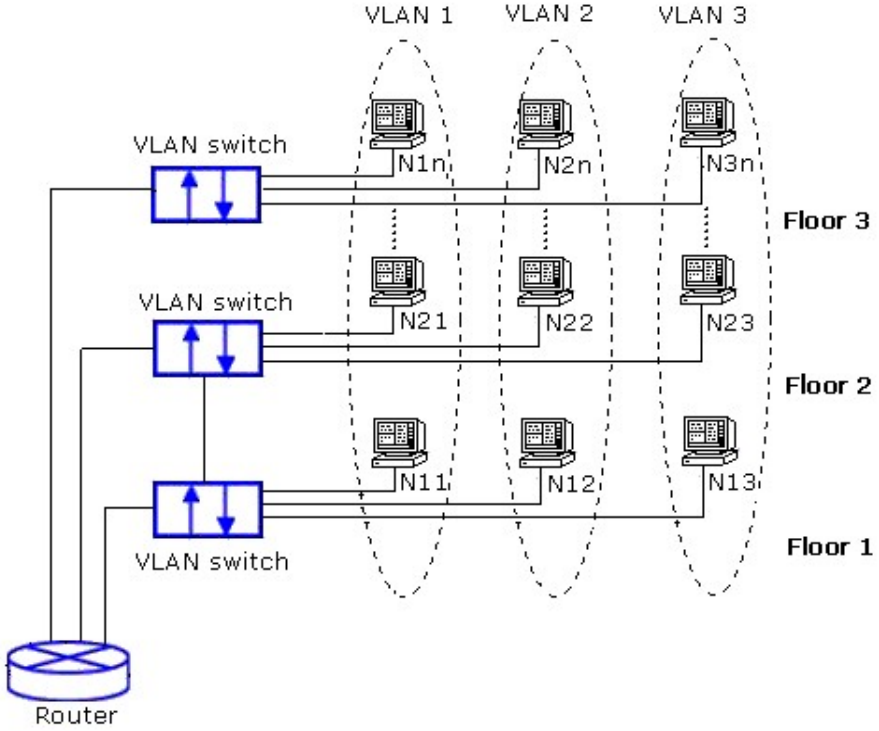


Figure 2.86 Example of VLAN Configuration

2.12.1 Configuration

VLAN→Configuration webpage allows the user to control VLAN configuration on the switch. The page is divided into a global section and a per-port configuration section as shown in

Figure 2.87. Table 2.71 and Table 2.72 provide descriptions of the options on Global VLAN Configuration and Port VLAN Configuration, respectively.

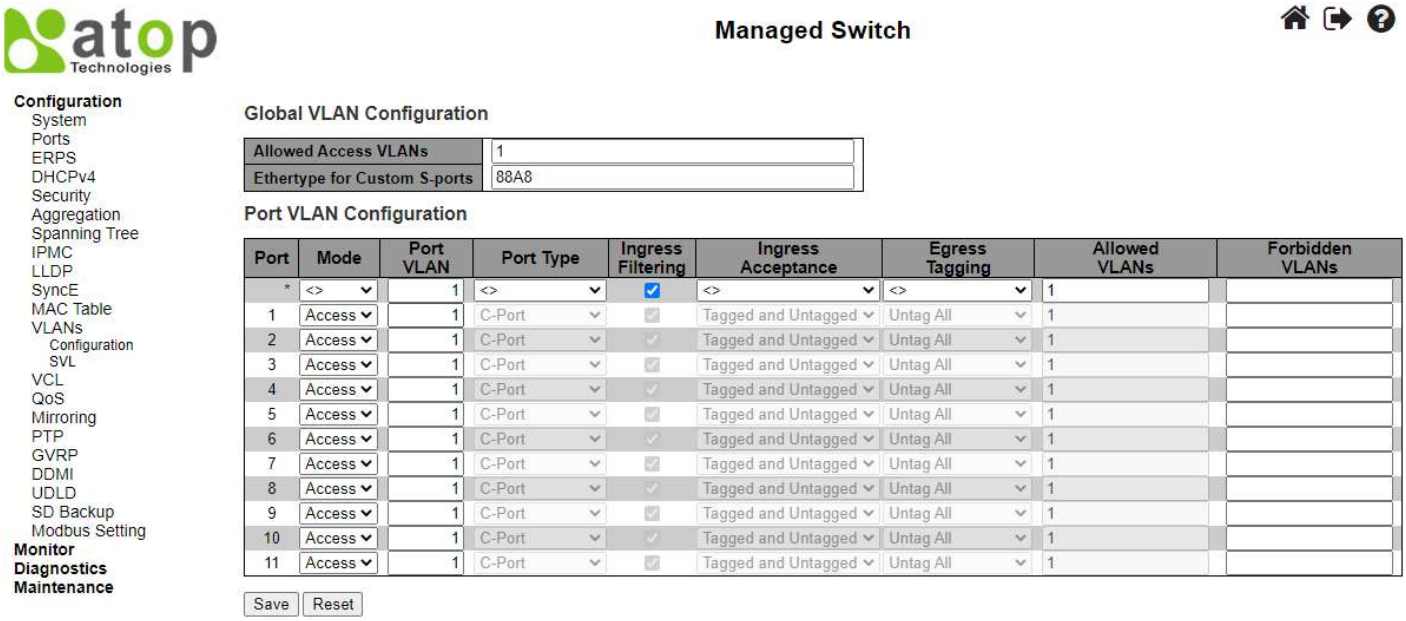


Figure 2.87 Webpage for Basic Configuration of VLANs

Table 2.71 Description of Global VLAN Configuration

Label	Description	Factory Default
Allowed Access VLANs	This field shows the allowed Access VLANs, i.e. it only affects ports configured as Access ports. Ports in other modes are members of the VLANs specified in the Allowed VLANs field. By default, only VLAN 1 is enabled. More VLANs may be created by using a list syntax where the individual elements are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will create VLANs 1, 10, 11, 12, 13, 200, and 300: **1,10-13,200,300**. Spaces are allowed in between the delimiters.	1
Ethertype for Custom S-ports	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.	88A8

Table 2.72 Description of Port VLAN Configuration

Label	Description	Factory Default
Port	This is the logical port number of this row.	-
Mode	The port mode (default is Access) determines the fundamental behaviour of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either greyed out or made changeable depending on the mode in question. Greyed out fields show the value that the port will get when the mode is applied. **Access:** Access ports are normally used to connect to end stations. Dynamic features like Voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics: • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 • Accepts untagged and C-tagged frames • Discards all frames not classified to the Access VLAN • On egress all frames are transmitted untagged **Trunk:** Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: • By default, a trunk port is member of all VLANs (1-4095) • The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Frames classified to a VLAN that the port is not a member of are discarded • By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress • Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress **Hybrid:** Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware • Ingress filtering can be controlled	Access

Label	Description	Factory Default
	• Ingress acceptance of frames and configuration of egress tagging can be configured independently	
Port VLAN	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4095, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untagged Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.	-
Port Type	Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. **Unaware:** On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. **C-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. **S-Port:** On egress, if frames must be tagged, they will be tagged with an S-tag. On ingress, frames with a VLAN tag with TPID = 0x88A8 get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept **Tagged Only** frames (see Ingress Acceptance below), frames without this TPID are dropped. ***Notice:*** If the S-port is configured to accept **Tagged and Untagged** frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with an S-tag. If the S-port is configured to accept **Untagged Only** frames, S-tagged frames will be discarded (except for priority S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID. **S-Custom-Port:** On egress, if frames must be tagged, they will be tagged with the custom S-tag. On ingress, frames with a VLAN tag with a TPID equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. Priority-tagged frames are classified to the Port VLAN. If the port is configured to accept **Tagged Only** frames (see Ingress Acceptance below), frames without this TPID are dropped. ***Notice:***	C-Port

Label	Description	Factory Default
	If the custom S-port is configured to accept **Tagged and Untagged** frames (see Ingress Acceptance below), frames with a C-tag are treated like frames with a custom S-tag. If the Custom S-port is configured to accept **Untagged Only** frames, custom S-tagged frames will be discarded (except for priority custom S-tagged frames). C-tagged frames are initially considered untagged and will therefore not be discarded. Later on, in the ingress classification process, they will get classified to the VLAN embedded in the tag instead of the port VLAN ID.	
Ingress Filtering	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.	Unclicked
Ingress Acceptance	Hybrid ports allow for changing the type of frames that are accepted on ingress. **Tagged and Untagged** Both tagged and untagged frames are accepted. See Port Type for a description of when a frame is considered tagged. **Tagged Only** Only frames tagged with the corresponding Port Type tag are accepted on ingress. **Untagged Only** Only untagged frames are accepted on ingress. See Port Type for a description of when a frame is considered untagged.	Tagged and Untagged
Egress Tagging	Ports in Trunk and Hybrid mode may control the tagging of frames on egress. **Untag Port VLAN** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. **Tag All** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. **Untag All** All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.	Untag All
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4095**. The field may be left empty, which means that the port will not become member of any VLANs.	1
Forbidden VLANs	A port may be configured to never become member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field.	Null

Label	Description	Factory Default
	By default, the field is left blank, which means that the port may become a member of all possible VLANs.	

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.12.2 SVL

SVL or Shared VLAN Learning Configuration can be set on the managed switch through this webpage as shown in Figure 2.88. In **SVL**, one or more VLANs map to a Filter ID (**FID**). By default, there is a one-to-one mapping from **VLAN** to **FID**, in which case the switch acts as an IVL (Independent VLAN Learning) bridge, but with SVL multiple VLANs may share the same MAC address table entries. Click **Add FID** button to add a new row to the SVL table. The FID will be pre-filled with the first unused FID. Table 2.73 summarizes the descriptions of Shared VLAN Learning Configuration.

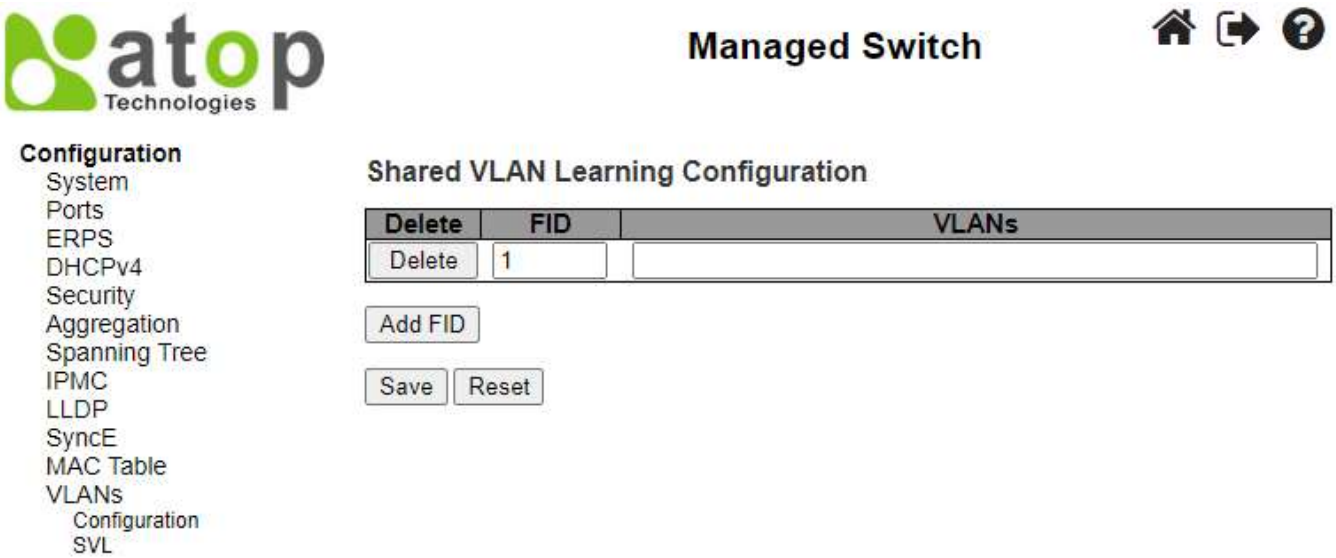


Figure 2.88 Webpage to SVL Configuration

Table 2.73 Description of Shared VLAN Learning Configuration

Label	Description	Factory Default
Delete	A previously allocated FID can be deleted by the use of this button.	-
FID	The Filter ID (FID) is the ID that VLANs get learned on in the MAC table when SVL is in effect. No two rows in the table can have the same FID and the FID must be a number between 1 and 63.	1
VLANs	List of VLANs mapped into FID. The syntax is as follows: Individual VLANs are separated by commas. Ranges are specified with a dash separating the lower and upper bound. The following example will map VLANs 1, 10, 11, 12, 13, 200, and 300: **1, 10-13, 200, 300**. Spaces are allowed in between the delimiters. The range of valid VLANs is 1 to 4095. The same VLAN can only be a member of one FID. A message will be displayed if one VLAN is grouped into two or more FIDs. All VLANs must map to a particular FID, and by default VLAN x maps to FID x. This implies that if FID x is defined, then VLAN x is implicitly a member of FID x unless it is specified for another FID. If FID x doesn't exist, a confirmation message will be displayed, asking whether to continue adding VLAN x implicitly to FID x.	-

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.13 VCL

2.13.1 MAC-based VLAN

The MAC address to VLAN ID mappings can be configured in Figure 2.89. This page allows adding and deleting MAC-based VLAN Classification List entries and assigning the entries to different ports. Figure 2.77 summarizes the descriptions of MAC-based VLAN Membership Configuration.

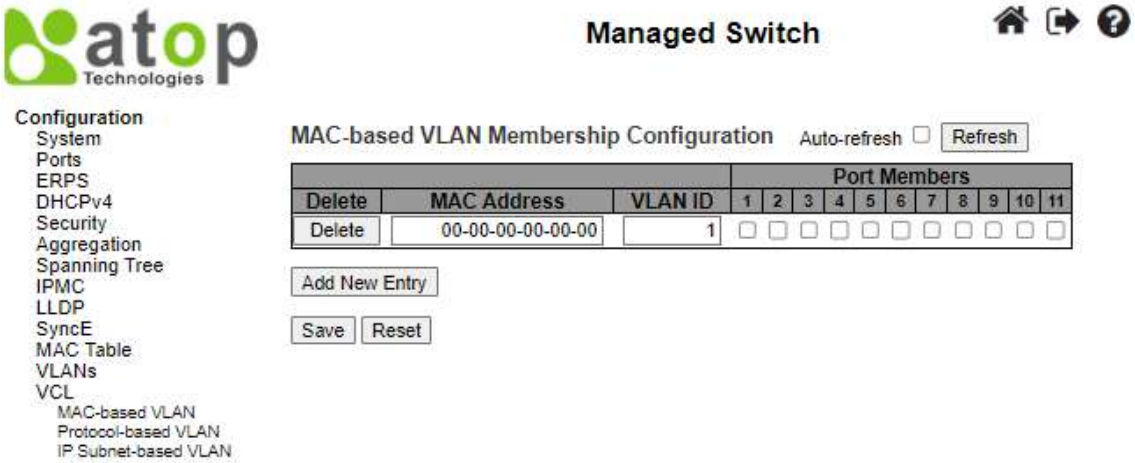


Figure 2.89 Webpage to Configure MAC-based VLAN of VCL

Table 2.74 Descriptions of MAC-based VLAN Configuration of VCL

Label	Description	Factory Default
Delete	To delete a MAC to VLAN ID mapping entry, check this box and press save. The entry will be deleted in the stack.	-
MAC Address	Indicates the MAC address of the mapping.	00-00-00-00-00-00
VLAN ID	Indicates the VLAN ID the above MAC will be mapped to.	1
Port Numbers	A row of check boxes for each port is displayed for each MAC to VLAN ID mapping entry. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.	-

Click **Add New Entry** button to add a new MAC to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any unicast MAC address can be used to configure the mapping. No broadcast or multicast MAC addresses are allowed. Legal values for a VLAN ID are 1 through 4095. The MAC to VLAN ID entry is enabled when you click on "**Save**" button. A mapping without any port members will not be added when you click "**Save**" button. The **Delete** button can be used to undo the addition of new mappings. The maximum possible MAC to VLAN ID mapping entries is limited to 256.

Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.13.2 Protocol-based VLAN

2.13.2.1 Protocol to Group

Figure 2.90 is the webpage that allows you to add new Protocol to Group Name mapping entries. Note that each protocol can be part of only one Group. It also allows you to see and delete current mapped entries for the switch. Table 2.75 provides the descriptions of the Protocol to Group Mapping Table.

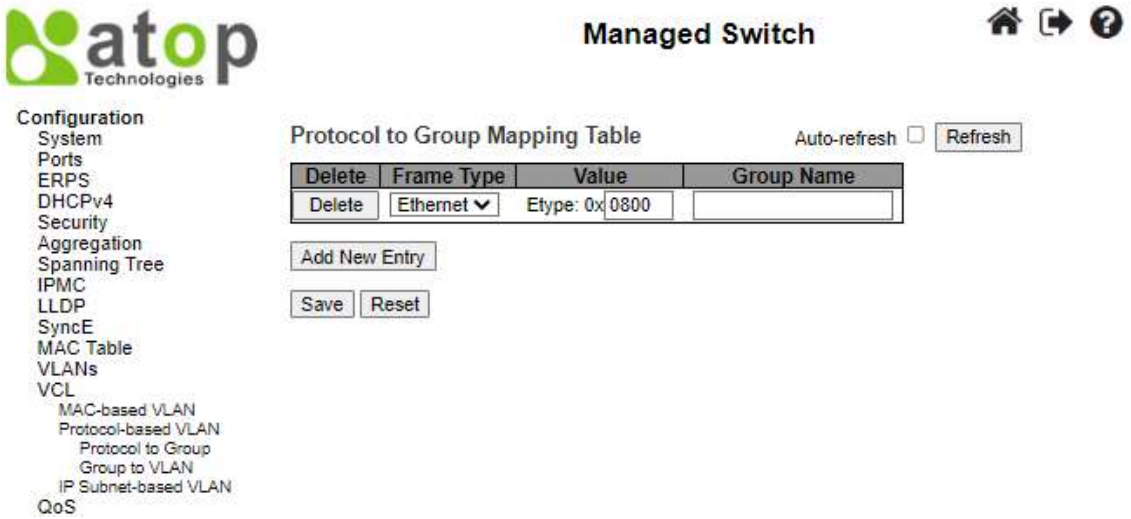


Figure 2.90 Webpage to Configure Protocol to Group Mapping Table

Table 2.75 Descriptions of Protocol to Group Mapping Table Configuration

Label	Description	Factory Default
Delete	To delete a Protocol to Group Name map entry, check this box. The entry will be deleted from the switch during the next Save.	-
Frame Type	Frame Type can have one of the following values: 1. **Ethernet** 2. **LLC** 3. **SNAP** Note: When changing the Frame type field, the valid value of the following text field will vary depending on the new frame type you selected.	Ethernet
Value	Valid value that can be entered in this text field depends on the option selected from the preceding Frame Type selection menu. Below are the criteria for the three different Frame Types: 1. **Ethernet**: Value in the text field when Ethernet is selected as a Frame Type is called etype. Valid values for etype range between 0x0600 and 0xffff 2. **LLC**: Valid value in this case is comprised of two different sub-values. a. DSAP: 1-byte long string (0x00-0xff) b. SSAP: 1-byte long string (0x00-0xff) 3. **SNAP**: Valid value in this case is also comprised of two different sub-values. a. **OUI**: OUI (Organizationally Unique Identifier) is a parameter in the format of xx-xxxx where each pair (xx) in the string is a hexadecimal value ranging between 0x00 and 0xff. b. **PID**: PID (Protocol ID). If OUI is hexadecimal 000000, then the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP; if OUI is an OUI for a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP. In other words, if the value of OUI field is 00-00-00 then the value of PID will be etype (0x0600-0xffff) and if the value of OUI is other than 00-00-00 then valid values of PID will be any value between 0x0000 and 0xffff.	0x0800
Group Name	A valid Group Name is a 16-character long string, unique for every entry, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9). Note: Special characters and underscores (_) are not allowed.	-

Click **Add New Entry** button to add a new entry in the mapping table. An empty row is added to the table, where Frame Type, Value and the Group Name can be configured as needed. The **Delete** button can be used to undo the

addition of new entry. The maximum possible Protocol to Group mappings is limited to 128. Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.13.2.2 Group to VLAN

This page allows the user to map a Group Name, which is already configured or going to be configured in the future, to a VLAN for the managed switch. Figure 2.91 shows the Group Name to VLAN mapping Table. Description of each column's label can be found in Table 2.76.

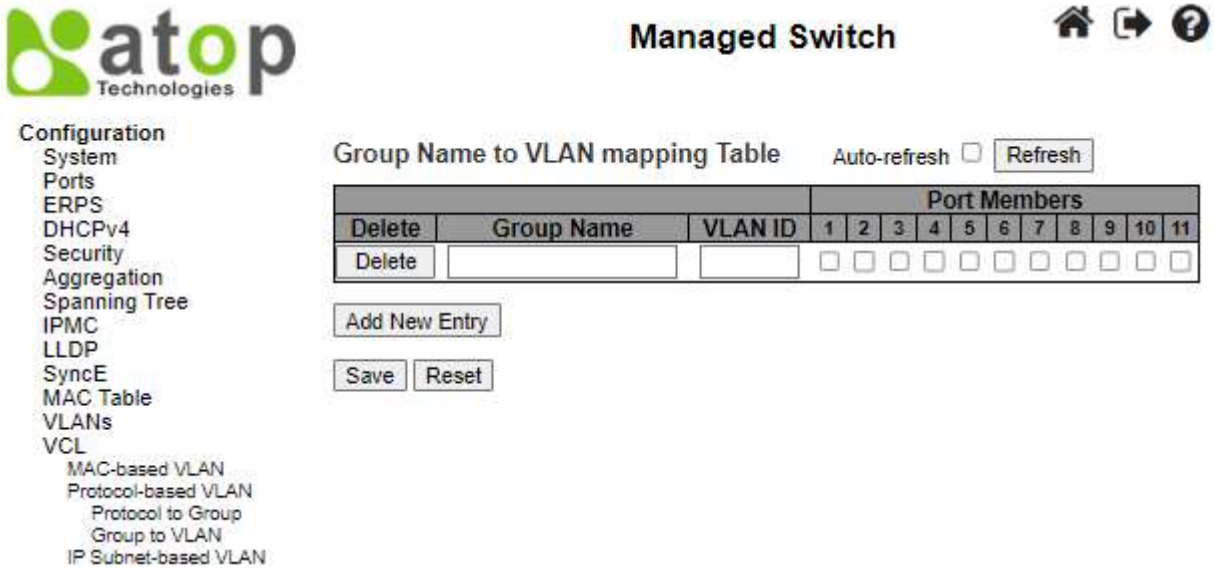


Figure 2.91 Webpage to Configure Group name to VLAN Mapping Table

Table 2.76 Descriptions of Group name to VLAN Mapping Table Configuration

Label	Description	Factory Default
Delete	To delete a Group Name to VLAN mapping, check this box. The entry will be deleted from the switch during the next Save.	-
Group Name	A valid Group Name is a string, at the most 16 characters long, which consists of a combination of alphabets (a-z or A-Z) and integers (0-9) with no special characters allowed. You may either use a Group that already includes one or more protocols (see Protocol to Group mappings), or create a Group to VLAN ID mapping that will become active the moment you add one or more protocols inside that Group. Furthermore, the Group to VLAN ID mapping is not unique, as long as the port lists of these mappings are mutually exclusive (e.g., Group1 can be mapped to VID 1 on port#1 and to VID 2 on port#2).	Null
VLAN ID	Indicates the VLAN ID to which the Group Name will be mapped. A valid VLAN ID ranges from 1 to 4095.	Null
Port Members	A row of check boxes for each port is displayed for each Group Name to VLAN ID mapping. To include a port in the mapping, check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.	Unclicked

Click **Add New Entry** button to add a new entry in the mapping table. An empty row is added to the table and the Group Name, VLAN ID and port members can be configured as needed. Legal values for a VLAN ID are 1 through 4095. The **Delete** button can be used to undo the addition of new entry. The maximum possible Groups to VLAN mappings are limited to 256. Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.13.3 IP Subnet-based VLAN

The IP subnet to VLAN ID mappings can be configured on the webpage as shown in Figure 2.92. This page allows adding, updating and deleting IP subnet to VLAN ID mapping entries and assigning them to different ports. Table 2.77 describes the column's label in the IP Subnet-based VLAN membership configuration.

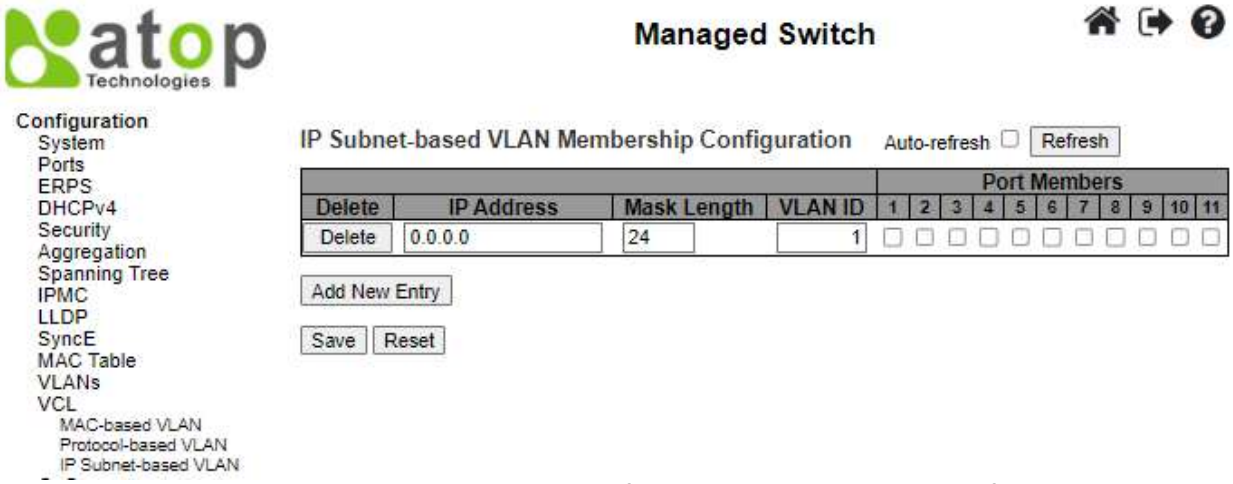


Figure 2.92 Webpage to Configure IP Subnet-based VLAN of VCL

Table 2.77 Descriptions of IP Subnet-based VLAN Configuration

Label	Description	Factory Default
Delete	To delete a mapping, check this box and press save. The entry will be deleted in the stack.	-
IP Address	Indicates the subnet's IP address (Any of the subnet's host addresses can be also provided here, the application will convert it automatically).	0.0.0.0
Mask Length	Indicates the subnet's mask length.	24
VLAN ID	Indicates the VLAN ID the subnet will be mapped to. IP Subnet to VLAN ID is a unique matching.	1
Port Members	A row of check boxes for each port is displayed for each IP subnet to VLAN ID mapping entry. To include a port in a mapping, simply check the box. To remove or exclude the port from the mapping, make sure the box is unchecked. By default, no ports are members and all boxes are unchecked.	Unclicked

Click **Add New Entry** to add a new IP subnet to VLAN ID mapping entry. An empty row is added to the table, and the mapping can be configured as needed. Any IP address/mask can be configured for the mapping. Valid values for the VLAN ID are 1 to 4095. The IP subnet to VLAN ID mapping entry is enabled when you click on "**Save**" button. The **Delete** button can be used to undo the addition of new mappings. The maximum possible IP subnet to VLAN ID mappings is limited to 128.

Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting. Check the **Auto-refresh** box to refresh the page automatically. The automatic refresh occurs every 3 seconds. Otherwise, click **Refresh** box to refresh the page immediately.

2.14 Voice VLAN

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI.

Table 2.78 Descriptions of Voice VLAN Configuration

Label	Description	Factory Default
Mode	Indicates the Voice VLAN mode operation. We must disable MSTP feature before we enable Voice VLAN. It can avoid the conflict of ingress filtering.	Disable
VLAN ID	Indicates the Voice VLAN ID. It should be a unique VLAN ID in the system and cannot equal each port PVID. It is a conflict in configuration if the value equals management VID, MVR VID, PVID etc. The allowed range is 1 to 4095.	1000
Aging Time	Indicates the Voice VLAN secure learning aging time. The allowed range is **10** to **10000000** seconds. It is used when security mode or auto detect mode is enabled. In other cases, it will be based on hardware aging time. The actual aging time will be situated between the [age_time; 2 * age_time] interval.	86400
Traffic Class	Indicates the Voice VLAN traffic class. All traffic on the Voice VLAN will apply this class.	7(High)
Port Mode	Indicates the Voice VLAN port mode. Possible port modes are: **Disabled**: Disjoin from Voice VLAN. **Auto**: Enable auto detect mode. It detects whether there is VoIP phone attached to the specific port and configures the Voice VLAN members automatically. **Forced**: Force join to Voice VLAN.	Disabled
Security	Indicates the Voice VLAN port security mode. When the function is enabled, all non-telephonic MAC addresses in the Voice VLAN will be blocked for 10 seconds. Possible port modes are: **Enabled**: Enable Voice VLAN security mode operation. **Disabled**: Disable Voice VLAN security mode operation.	Disabled
Discovery Protocol	Indicates the Voice VLAN port discovery protocol. It will only work when auto detect mode is enabled. We should enable LLDP feature before configuring discovery protocol to "LLDP" or "Both". Changing the discovery protocol to "OUI" or "LLDP" will restart auto detect process. Possible discovery protocols are: **OUI**: Detect telephony device by OUI address. **LLDP**: Detect telephony device by LLDP. **Both**: Both OUI and LLDP.	OUI

2.15 QoS

Quality of Service (QoS) is the ability to provide different priority to different applications, users, or data flows. QoS guarantees a certain level of performance to a data flow by using the following metrics: transmitted bit rate, bit error rate, delay, jitter, and probability of packet dropping. QoS guarantees are important if the network capacity is insufficient, especially for application that requires certain bit rate and is delay sensitive. For any network that is best effort, QoS cannot be guaranteed, except that resource is more than sufficient to serve users.

Controlling network traffic needs a set of rules to help classify different types of traffic and define how each of them should be treated as they are being transmitted. This managed switch can inspect both 802.1p Class of Service (CoS) tags and DiffServ tags called Differentiated Services Code Point (DSCP) to provide consistent classification.

2.15.1 Port Classification

The Port Classification webpage shown in Figure 2.93 allows the user to configure the basic QoS Ingress Classification settings for all of managed switch ports. Table 2.79 provides the descriptions of the setting parameters of QoS Port Classification.

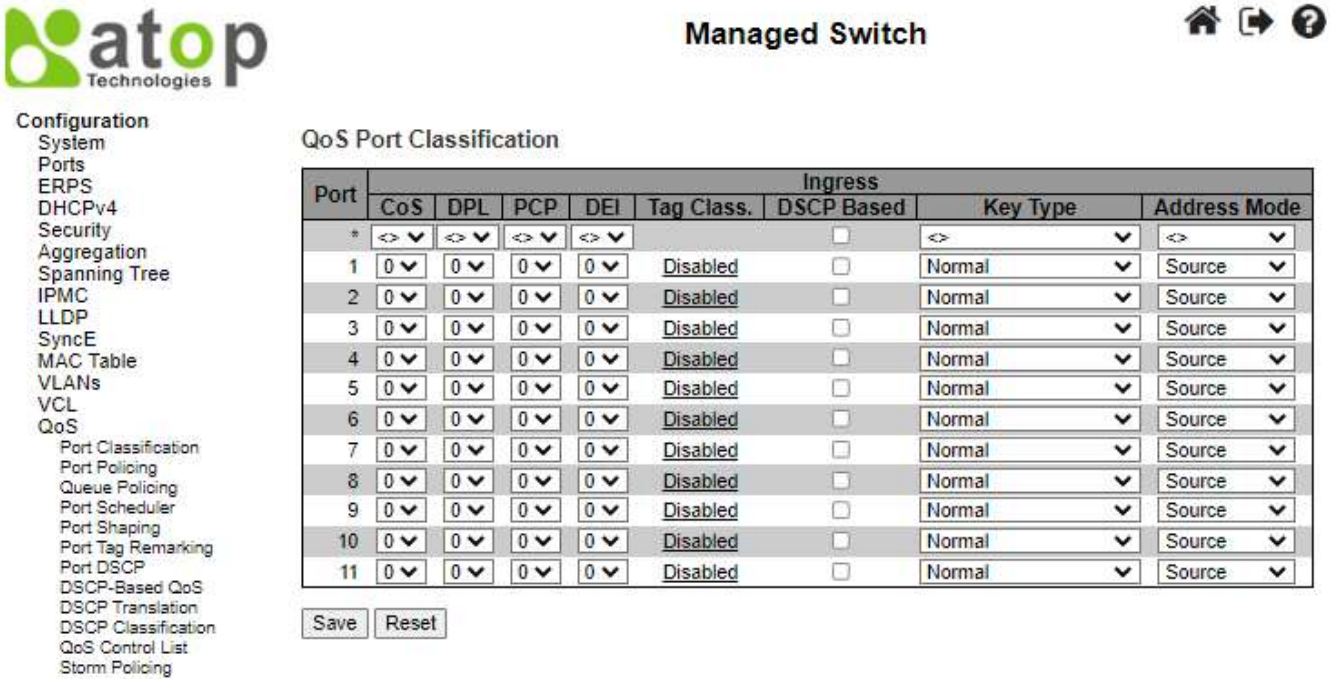


Figure 2.93 Webpage to Configure Port Classification of QoS

Table 2.79 Descriptions of Port Classification Configuration of QoS

Label	Description	Factory Default
Port	The port number for which the configuration below applies.	-
CoS	Controls the default class of service (CoS) value. All frames are classified to a CoS. There is a one-to-one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a CoS that is mapped from the PCP and DEI value in the tag. Otherwise, the frame is classified to the default CoS. The classified CoS can be overruled by a QCL entry. Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.	0
DPL	Controls the default Drop Precedence Level (DPL) value. All frames are classified to a Drop Precedence Level. If the port is VLAN aware, the frame is tagged and Tag Class. is enabled, then the frame is classified to a DPL that is mapped from the PCP and DEI value in the tag. Otherwise, the frame is classified to the default DPL. The classified DPL can be overruled by a QCL entry.	0
PCP	Controls the default Priority Code Point (PCP) value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise, the frame is classified to the default PCP value. Note: PCP is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.	0
DEI	Controls the default Drop Eligible Indicator (DEI) value. It is a 1-bit field in the VLAN tag. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise, the frame is classified to the default DEI value.	0
Tag Class.	Shows the classification mode for tagged frames on this port. **Disabled**: Use default CoS and DPL for tagged frames. **Enabled**: Use mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping.	Disabled

Label	Description	Factory Default
	Note: This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default CoS and DPL.	
DSCP Based	Click to Enable Differentiated Services Code Point (DSCP) Based QoS Ingress Port Classification. It is a field in the header of IP packets for packet classification purposes.	Unclicked
Key Type	The key type specifying the key generated for frames received on the port. The allowed values are: **Normal**: Half key, match outer tag, SIP/DIP and SMAC/DMAC. **Double Tag**: Quarter key, match inner and outer tag. **IP Address**: Half key, match inner and outer tag, SIP and DIP. For non-IP frames, match outer tag only. **MAC and IP Address**: Full key, match inner and outer tag, SMAC, DMAC, SIP and DIP. Filtering on DMAC type (unicast/multicast/broadcast) is supported for any key type.	Normal
Address Mode	The IP/MAC address mode specifying whether the QoS Control List (QCL) classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. This parameter is only used when the key type is **Normal**. The allowed values are: **Source**: Enable SMAC/SIP matching. **Destination**: Enable DMAC/DIP matching.	Source

Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.15.2 Port Policing

Port Policing webpage allows the user to configure the Policer settings for all switch ports. Note that a policer can limit the bandwidth of received frames. It is located in front of the ingress queue. QoS Ingress Port Policer Table is shown in Figure 2.94. The descriptions of QoS Ingress Port Policers are explained in Table 2.80.

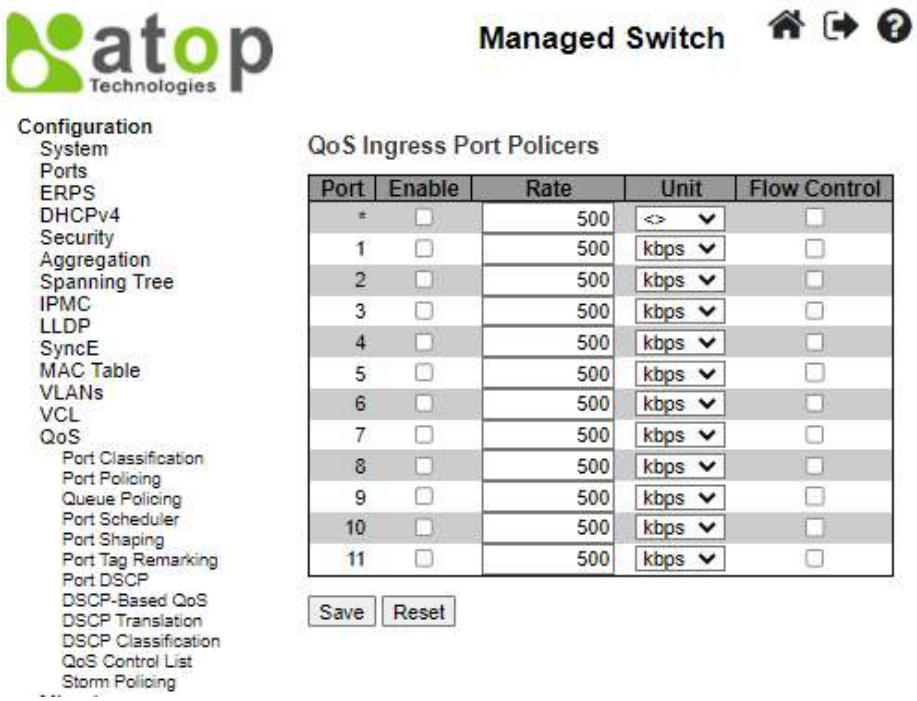


Figure 2.94 Webpage to Configure Port Policing of QoS

Table 2.80 Descriptions of Port Policing Configuration of QoS

Label	Description	Factory Default
Port	The port number for which the configuration below applies.	-
Enable	Enable or disable the port policer for this switch port.	Unchecked
Rate	Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps or fps, and 1-3276 when "Unit" is Mbps or kfps. The rate is internally rounded up to the nearest value supported by the port policer.	500
Unit	Controls the unit of measure for the port policer rate as kbps, Mbps, fps or kfps.	kbps
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.	Unchecked

Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.15.3 Queue Policing

To configure the Queue Policer settings for all switch ports, the user can check the corresponding boxes in the table in Figure 2.95. Table 2.81 describes the labels in QoS Ingress Queue Policer Table.

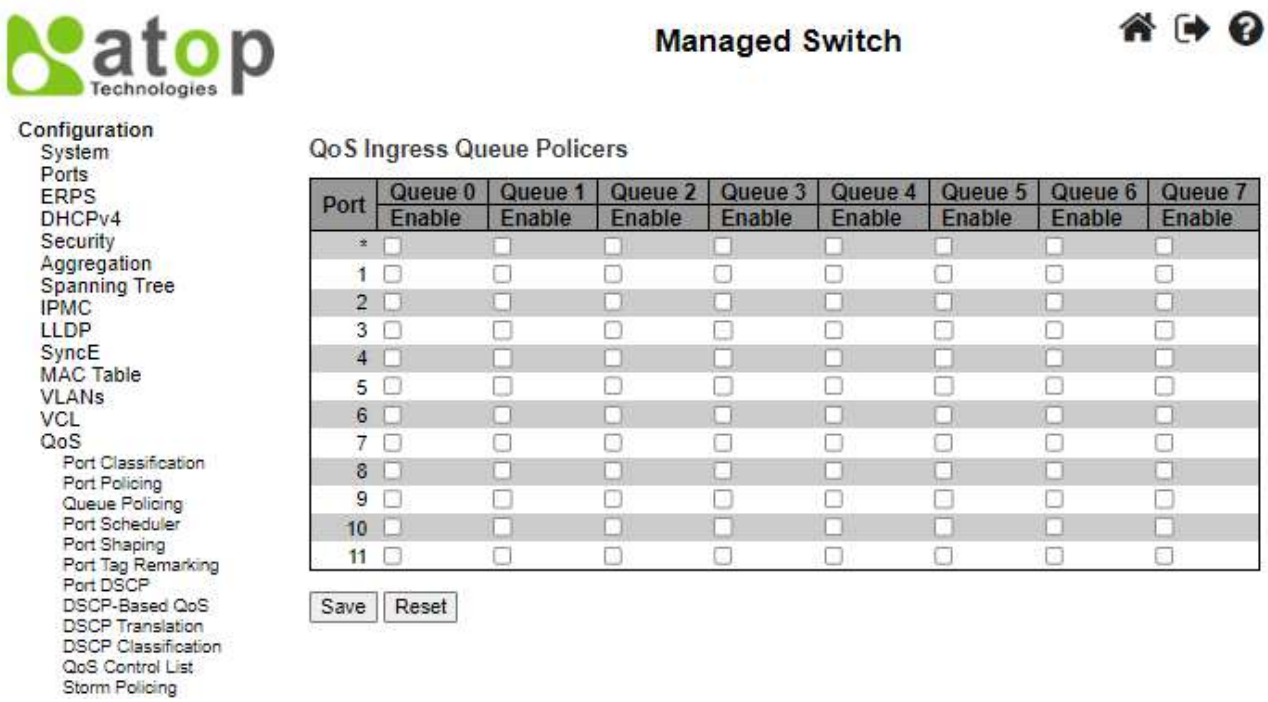


Figure 2.95 Webpage to Configure Queue Policing of QoS

Table 2.81 Descriptions of Queue Policing Configuration of QoS

Label	Description	Factory Default
Port	The port number for which the configuration below applies.	-
Enable (E)	Enable or disable the port policer for this switch port.	unchecked
Rate	Controls the rate for the port policer. This value is restricted to 100-3276700 when "Unit" is kbps, and 1-3276 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port policer. This field is only shown if at least one of the queue policers are enabled.	500

Unit	Controls the unit of measure for the queue policer rate as kbps or Mbps. This field is only shown if at least one of the queue policers are enabled.	kbps

Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.15.4 Port Scheduler

This webpage provides an overview of QoS Egress Port Schedulers for all switch ports as shown in Figure 2.96. Table 2.82 describes the labels in the QoS Egress Port Schedulers.

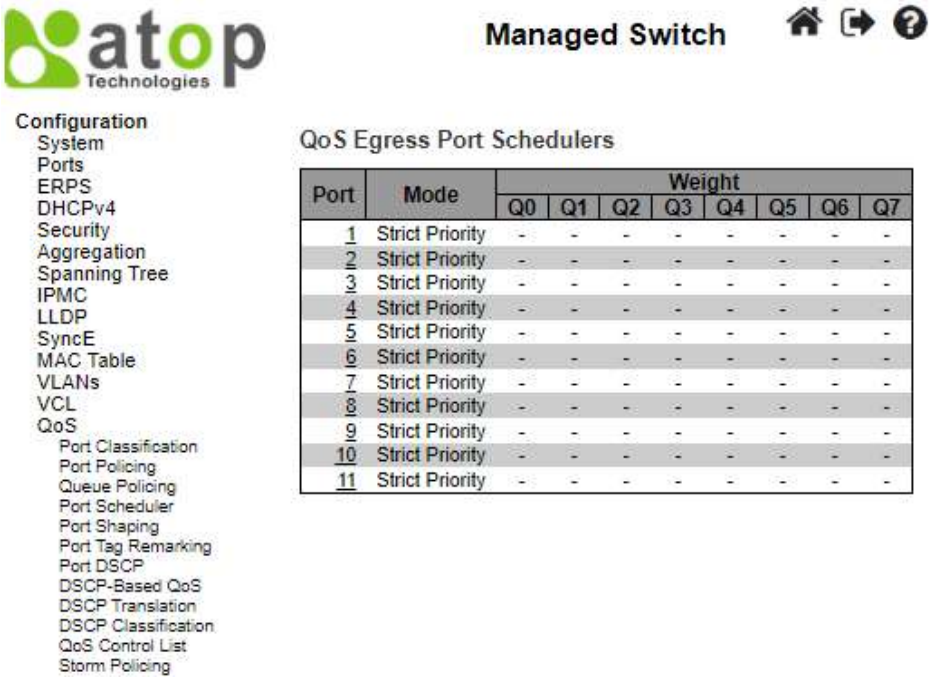


Figure 2.96 Webpage to Configure Port Scheduler of QoS

Table 2.82 Descriptions of Port Scheduler Configuration of QoS

Label	Description	Factory Default
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the schedulers.	-
Mode	Shows the scheduling mode for this port.	Strict Priority
Qn	Shows the weight for this queue and port.	-

After Clicking hyperlink on any port, another webpage configuration will be launched, as shown in Figure 2.97. Table 2.83 describes the QoS Egress Port Scheduler and Shapers Port Configuration.

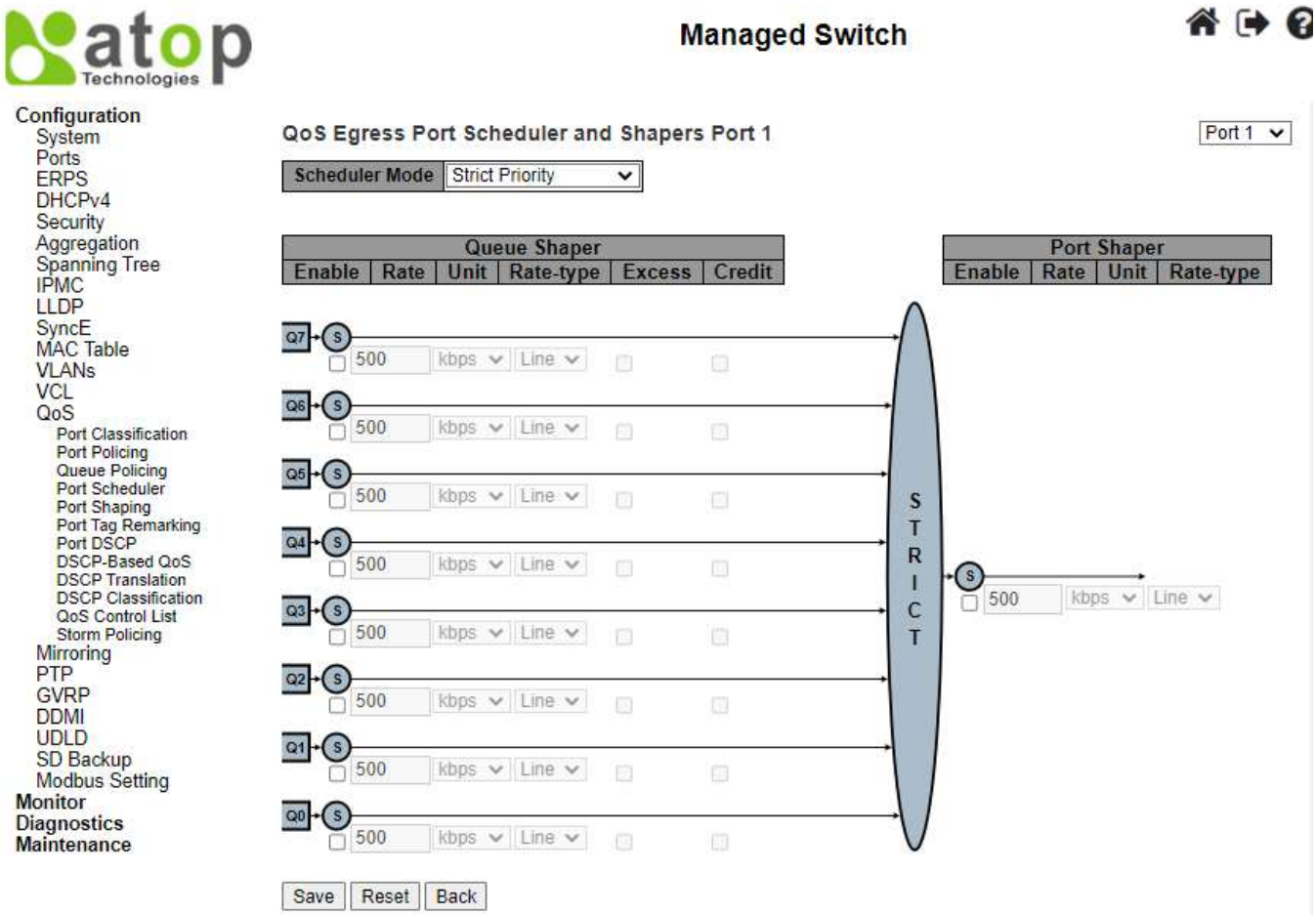


Figure 2.97 Webpage to Configure QoS Egress Port Scheduler and Shapers Port

Table 2.83 Descriptions of QoS Egress Port Scheduler and Shapers Port Configuration

Label	Description	Factory Default
Scheduler Mode	Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port.	Strict Priority
Queue Shaper		
Enable	Controls whether the queue shaper is enabled for this queue on this switch port.	Unclicked
Rate	Controls the rate for the queue shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.	500
Unit	Controls the unit of measure for the queue shaper rate as kbps or Mbps.	Kbps
Rate-type	The rate type of the queue shaper. The allowed values are: Line: Specify that this shaper operates on line rate. Data: Specify that this shaper operates on data rate.	Line
Excess	Controls whether the queue is allowed to use excess bandwidth.	Unclicked
Credit	Controls whether the queue has credit-based shaper enabled.	Unclicked
Queue Scheduler		
Weight	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".	
Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".	

Port Shaper		
Enable	Controls whether the port shaper is enabled for this switch port.	Unclicked
Rate	Controls the rate for the port shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.	500
Unit	Controls the unit of measure for the port shaper rate as kbps or Mbps.	Kbps
Rate-type	The rate type of the port shaper. The allowed values are: Line: Specify that this shaper operates on line rate. Data: Specify that this shaper operates on data rate.	Line

Click Save button to save changes. Click Reset button to undo any changes made locally and revert to previously saved values. Click Back button to undo any changes made locally and return to the previous page.

2.15.5 Port Shaping

This webpage provides an overview of QoS Egress Port Shapers for all switch ports as shown in Figure 2.98. Table 2.84 describes the labels in QoS Egress Port Shapers.

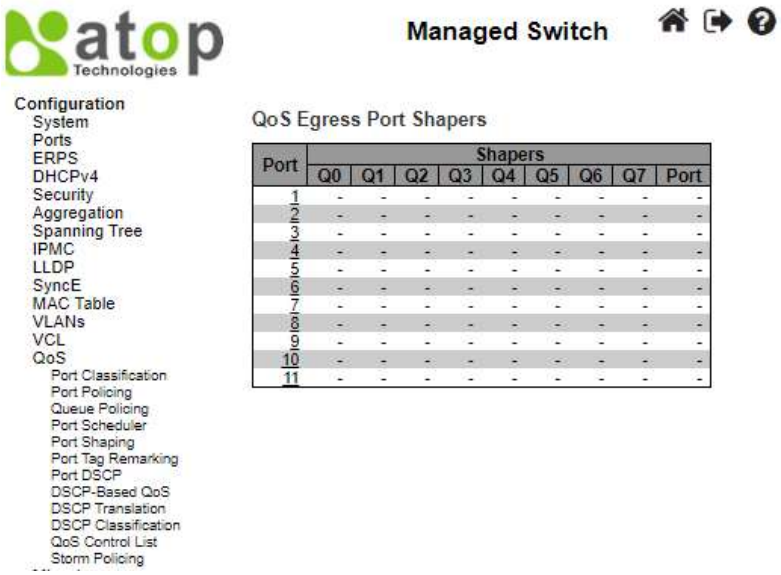


Figure 2.98 Webpage to Configure Port Shaping of QoS

Table 2.84 Descriptions of Port Shaping Configuration of QoS

Label	Description	Factory Default
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure the shapers.	-
Qn	Shows "-" for disabled or actual queue shaper rate - e.g., "800 Mbps".	-
Port	Shows "-" for disabled or actual port shaper rate - e.g., "800 Mbps".	-

After Clicking hyperlink on any port, another webpage configuration will be launched, as shown in Figure 2.99. Table 2.85 describes the detaled QoS Egress Port Scheduler and Shapers Port Configuration.

This page allows you to configure the Scheduler and Shapers for a specific port.

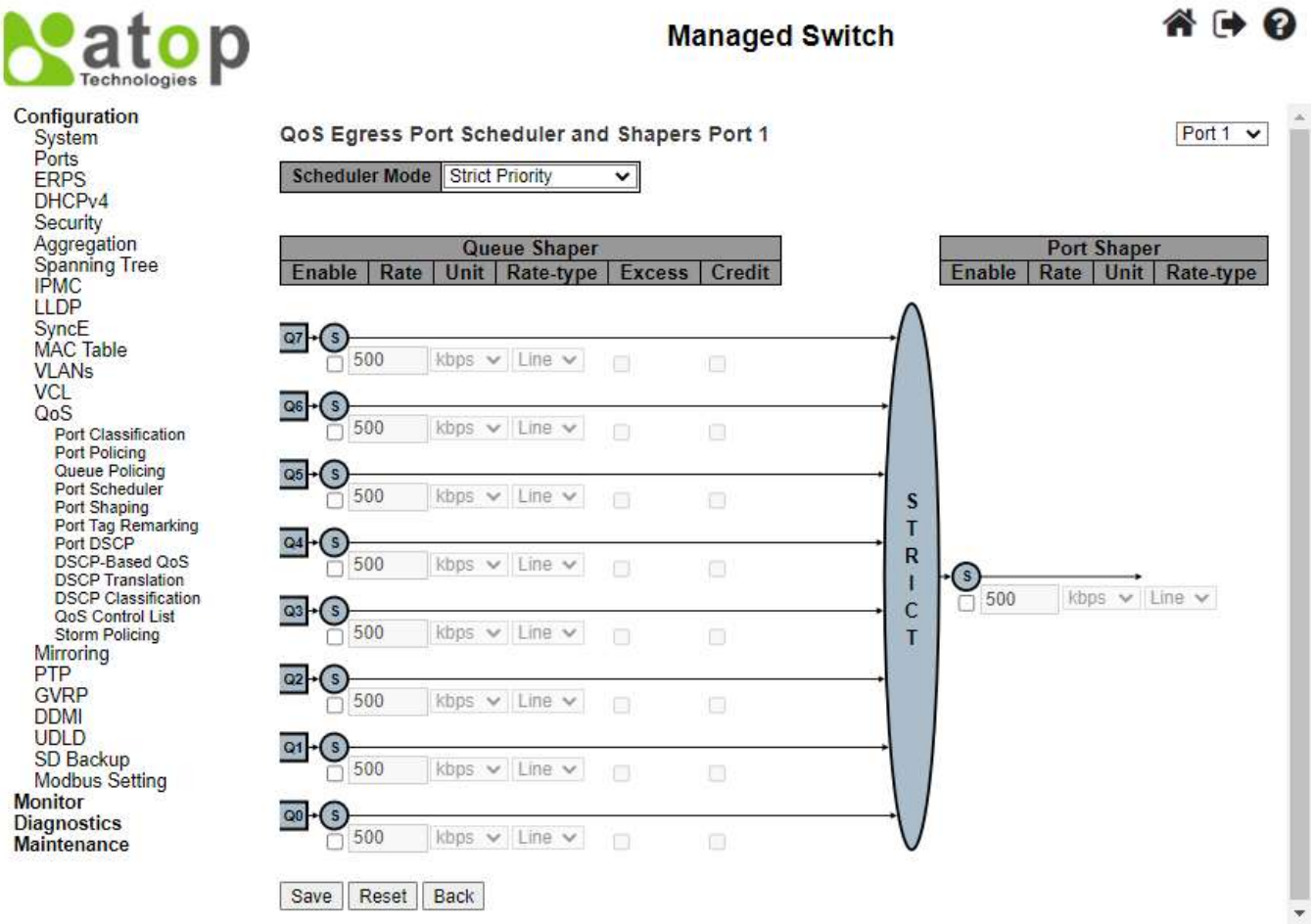


Figure 2.99 Webpage to Detailed Configure QoS Egress Port Scheduler and Shapers Port

Table 2.85 Descriptions of Detaled QoS Egress Port Scheduler and Shapers Port Configuration

Label	Description	Factory Default
Scheduler Mode	Controls how many of the queues are scheduled as strict and how many are scheduled as weighted on this switch port.	Strict Priority
Queue Shaper		
Enable	Controls whether the queue shaper is enabled for this queue on this switch port.	Unclicked
Rate	Controls the rate for the queue shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the queue shaper.	500
Unit	Controls the unit of measure for the queue shaper rate as kbps or Mbps.	Kbps
Rate-type	The rate type of the queue shaper. The allowed values are: Line: Specify that this shaper operates on line rate. Data: Specify that this shaper operates on data rate.	Line
Excess	Controls whether the queue is allowed to use excess bandwidth.	Unclicked
Credit	Controls whether the queue has credit-based shaper enabled.	Unclicked
Queue Scheduler		
Weight	Controls the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted".	

Percent	Shows the weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted".	
Port Shaper		
Enable	Controls whether the port shaper is enabled for this switch port.	Unclicked
Rate	Controls the rate for the port shaper. This value is restricted to 100-3281943 when "Unit" is kbps, and 1-3281 when "Unit" is Mbps. The rate is internally rounded up to the nearest value supported by the port shaper.	500
Unit	Controls the unit of measure for the port shaper rate as kbps or Mbps.	Kbps
Rate-type	The rate type of the port shaper. The allowed values are: Line: Specify that this shaper operates on line rate. Data: Specify that this shaper operates on data rate.	Line

Click Save button to save changes. Click Reset button to undo any changes made locally and revert to previously saved values. Click Back button to undo any changes made locally and return to the previous page.

2.15.6 Port Tag Remarking

This webpage provides an overview of QoS Egress Port Tag Remarking for all switch ports as shown in Figure 2.100. Table 2.86 describes the labels in QoS Egress Port Tag Remarking.

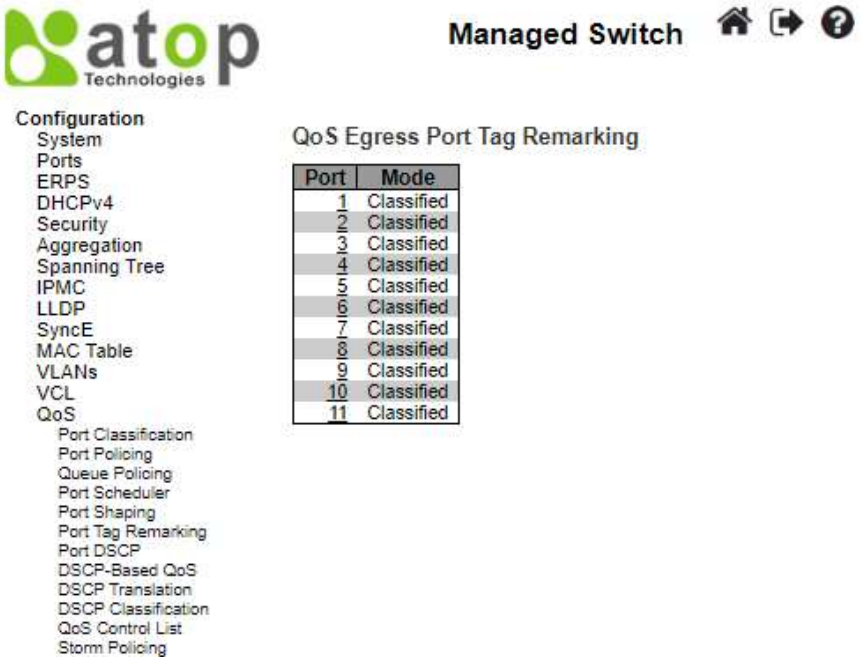


Figure 2.100 Webpage to Configure Port Tag Remarking of QoS

Table 2.86 Descriptions of Port Tag Remarking Configuration of QoS

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number in order to configure tag remarking.
Mode	Shows the tag remarking mode for this port. Classified: Use classified PCP/DEI values. Default: Use default PCP/DEI values. Mapped: Use mapped versions of QoS class and DP level.

After clicking into any port, the following webpage will be launched as shown in Figure 2.101. Table 2.861 describes the labels in Each Port Tag Remarking Mode of QoS.

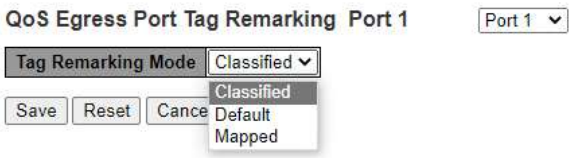


Figure 2.101 Webpage to Configure Each Port Tag Remarking of QoS

Table 2.87 Descriptions for Port Tag Remarking Configuration of Mode

Label	Description
Mode Controls the tag remarking mode for this port.	
Classified	Use classified PCP/DEI values.
Default	Use default PCP/DEI values
Mapped	Use mapped versions of CoS and DPL.
PCP/DEI Configuration	Controls the default PCP and DEI values used when the mode is set to **Default**.
(CoS, DPL) to (PCP, DEI) Mapping	Controls the mapping of the classified (CoS, DPL) to (PCP, DEI) values when the mode is set to **Mapped**.

2.15.7 Port DSCP

The Port DSCP webpage allows the user to configure the basic Quality of Server (QoS) Port Differentiated Service Code Point (DSCP) Configuration settings for all switch ports. The QoS Port DSCP Configuration table is shown in Figure 2.102. The user can change the setting of either or both ingress or egress traffic. Table 2.88 explains the options for each port in QoS Port DSCP Configuration.

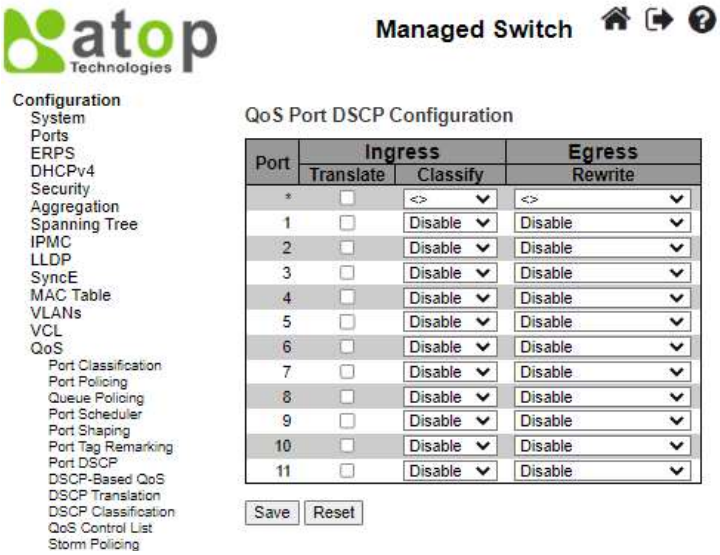


Figure 2.102 Webpage to Configure Port DSCP of QoS

Table 2.88 Descriptions of Port DSCP Configuration of QoS

Label		**Description**	**Factory Default**
Port		The Port column shows the list of ports for which you can configure DSCP ingress and egress settings.	-
Ingress	**Translate**	In Ingress settings you can change ingress translation and classification settings for individual ports. There are two configuration parameters available in Ingress: 1. Translate: To Enable the Ingress Translation click the checkbox.	Unchecked

Label		Description	Factory Default
	Classify	2. Classify: Classification for a port have 4 different values. • **Disable**: No Ingress DSCP Classification. • **DSCP=0**: Classify if incoming (or translated if enabled) DSCP is 0. • **Selected**: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP. • **All**: Classify all DSCP.	Disable
Egress Rewrite		Port Egress Rewriting can be one of – • **Disable**: No Egress rewrite. • **Enable**: Rewrite enabled without remapping. • **Remap DP Unaware**: DSCP from analyser is remapped and frame is remarked with remapped DSCP value. DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table. • **Remap DP Aware**: DSCP from analyser is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table.	Disable

Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.15.8 DSCP-Based QoS

This page as shown in Figure 2.103 allows the user to configure the basic QoS DSCP based QoS Ingress Classification settings for the managed switch. The maximum number of supported DSCP (Differentiated Services Code Point) is 64 as shown in the table. Table 2.89 describes the options for each DSCP.

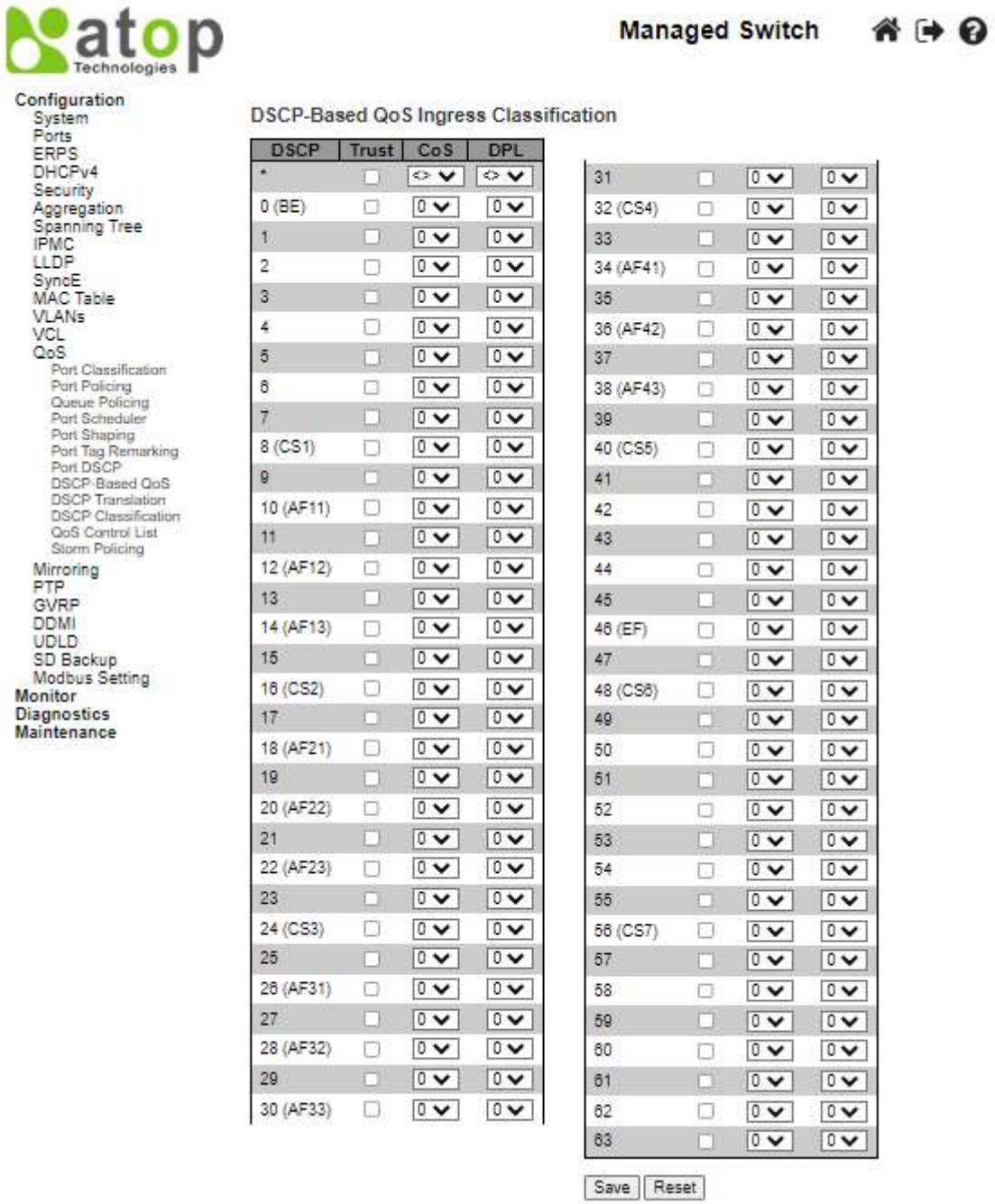


Figure 2.103 Webpage to Configure DSCP-Based of QoS

Table 2.89 Descriptions of DSCP-Based Configuration of QoS

Label	Description	Factory Default
DSCP	Maximum number of supported DSCP values is 64.	-
Trust	Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and Drop Precedence Level (DPL). Frames with untrusted DSCP values are treated as a non-IP frame.	Unchecked
CoS	CoS class value can be any of (0-7)	0
DPL	Drop Precedence Level (0-1)	0

Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.15.9 DSCP Translation

DSCP Translation webpage as shown in Figure 2.104 allows you to configure the basic QoS DSCP Translation settings for the managed switch. DSCP translation can be done in Ingress or Egress. Table 2.90 describes the setting options for DSCP Translation.

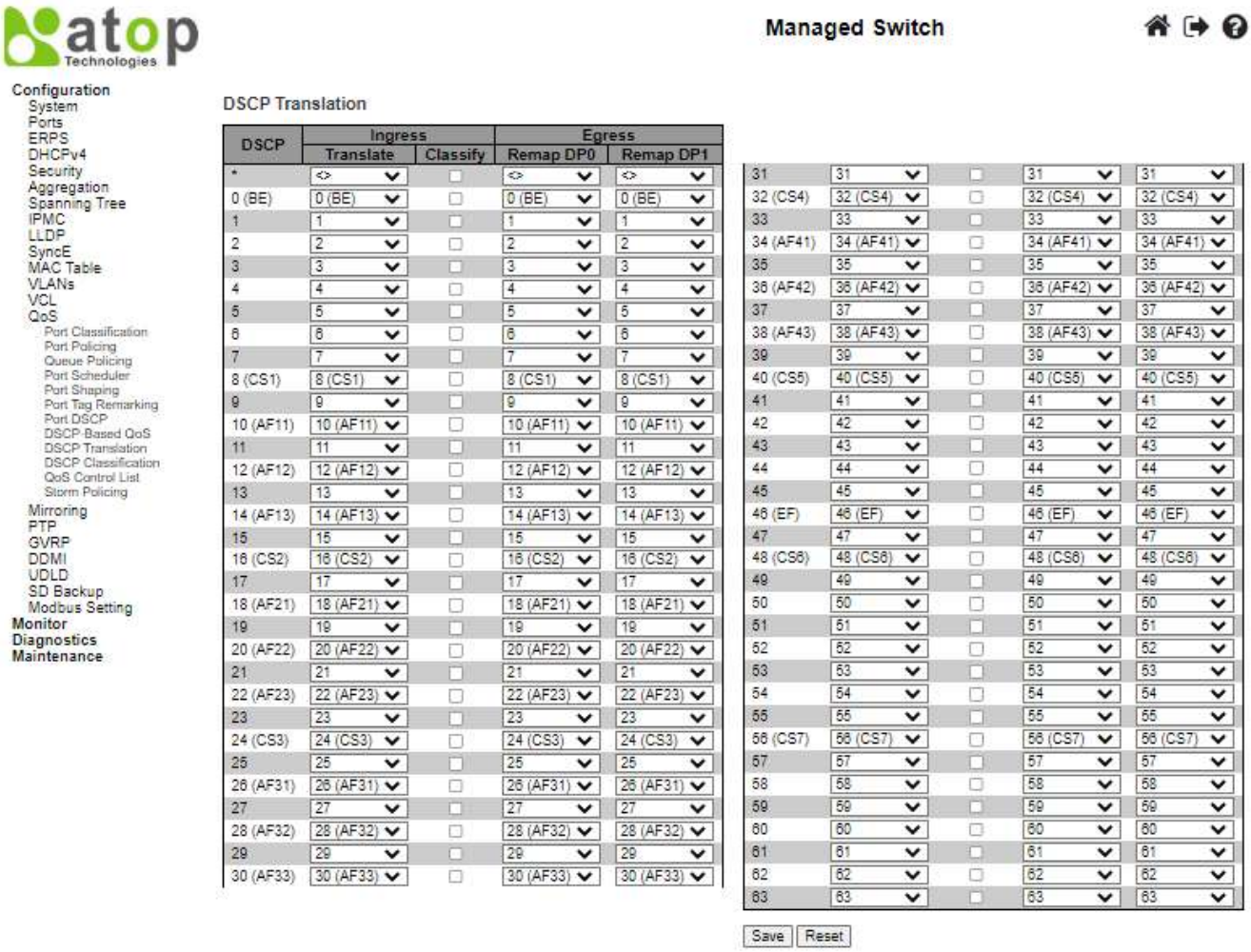


Figure 2.104 Webpage to Configure DSCP Translation of QoS

Table 2.90 Descriptions of DSCP Translation Configuration of QoS

Label		Description	Factory Default
DSCP		Maximum number of supported DSCP values are 64 and valid DSCP value ranges from 0 to 63.	-
Ingress	**Translate**	Ingress side DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. Translate: DSCP at Ingress side can be translated to any of (0-63) DSCP values.	-
	Classify	Click to enable Classification at Ingress side.	Unchecked
Egress		There are the following configurable parameters for Egress side – 1. Remap DP0 Controls the remapping for frames with DP level 0. 2. Remap DP1 Controls the remapping for frames with DP level 1.	-
DP0 /DP1		Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63.	-

Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.15.10 DSCP Classification

The DSCP Classification webpage as shown in Figure 2.105 allows you to configure the mapping of Class of Service (CoS) or QoS Class and Drop Precedence Level (DPL) to DSCP value. Table 2.91 explains the options for DSCP Classification.

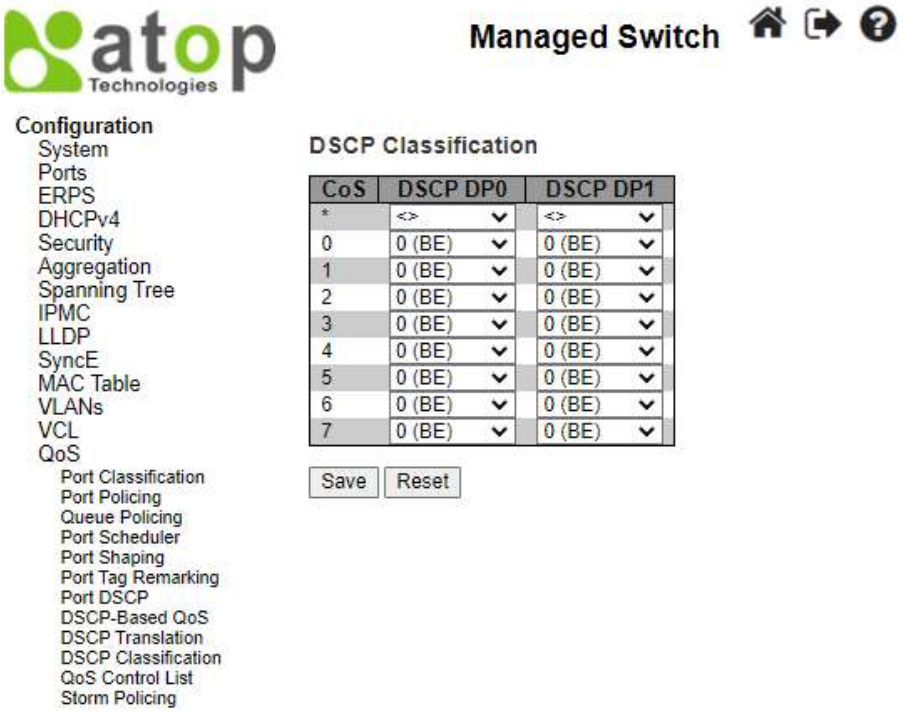


Figure 2.105 Webpage to Configure DSCP Classification of QoS

Table 2.91 Descriptions of DSCP Classification Configuration of QoS

Label	Description	Factory Default
QoS Class	Actual QoS class.	-
DSCP DP0	Select the classified DSCP value (0-63) for Drop Precedence Level 0.	0
DSCP DP1	Select the classified DSCP value (0-63) for Drop Precedence Level 1.	0

Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.15.11 QoS Control List

The QoS Control List webpage as shown in Figure 2.106 shows the QoS Control List (QCL), which is made up of the QCEs (QoS Control Entries). Each row describes a QCE that is defined. Table 2.92 describes the definition of each column in the list. The maximum number of QCEs is 256 on each switch. To add a new entry, click on the ⊕ plus sign to add a new QCE to the list and the webpage is updated as shown in Figure 2.107. This updated webpage allows the user to edit or insert one single QoS Control Entry at a time. A QCE consists of several parameters as described in Table 2.93. These parameters vary according to the frame type that the user selected.

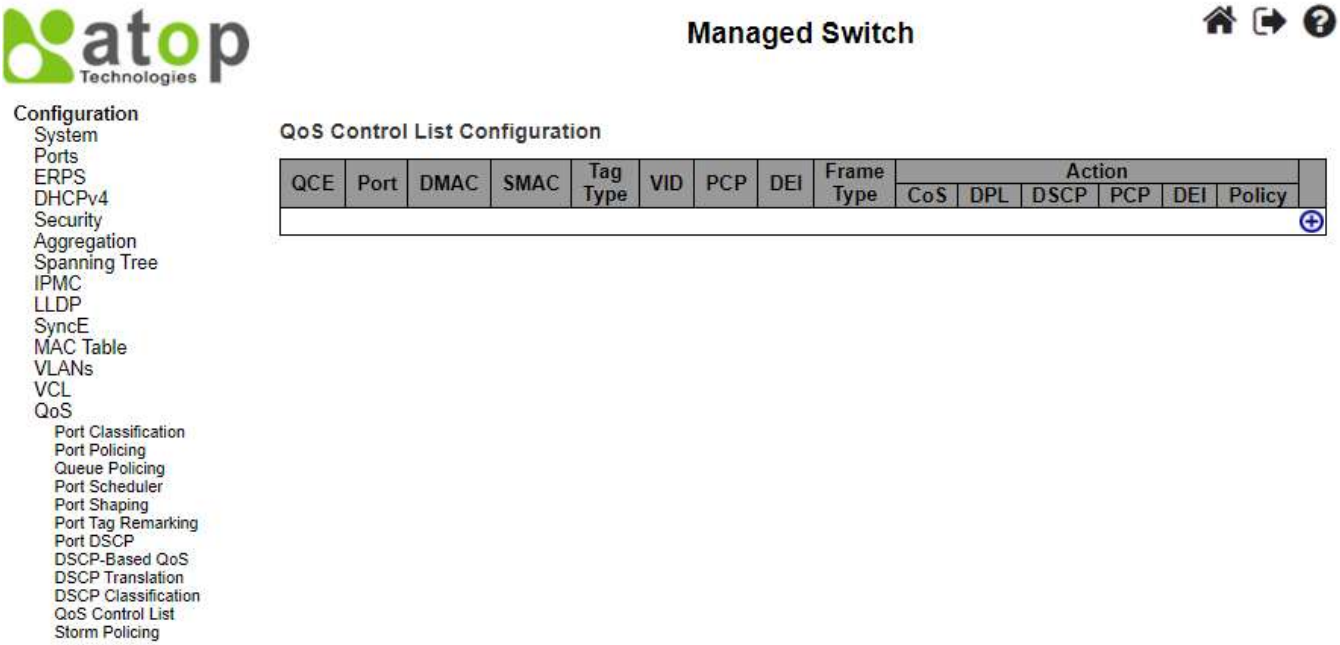


Figure 2.106 Webpage to Configure QoS Control List

Table 2.92 Descriptions of QoS Control List Configuration

Label	Description	Factory Default
QCE	Indicates the QCE id.	-
Port	Indicates the list of ports configured with the QCE or 'Any'.	-
DMAC	Indicates the destination MAC address. Possible values are: **Any**: Match any DMAC. **Unicast**: Match unicast DMAC. **Multicast**: Match multicast DMAC. **Broadcast**: Match broadcast DMAC. **<MAC>**: Match specific DMAC. The default value is 'Any'.	-
SMAC	Match specific source MAC address or 'Any'. If a port is configured to match on destination addresses, this field indicates the DMAC.	-
Tag	Indicates tag type. Possible values are: **Any**: Match tagged and untagged frames. **Untagged**: Match untagged frames. **Tagged**: Match tagged frames. **C-Tagged**: Match C-tagged frames. **S-Tagged**: Match S-tagged frames. The default value is 'Any'.	-
VID	Indicates (VLAN ID), either a specific VID or range of VIDs. VID can be in the range 1-4095 or 'Any'	-
PCP	Priority Code Point: Valid values of PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'.	-
DEI	Drop Eligible Indicator: Valid value of DEI are 0, 1 or 'Any'.	-
Frame Type	Indicates the type of frame. Possible values are: **Any**: Match any frame type. **Ethernet**: Match EtherType frames. **LLC**: Match (LLC) frames. **SNAP**: Match (SNAP) frames. **IPv4**: Match IPv4 frames. **IPv6**: Match IPv6 frames.	-

Label	Description	Factory Default
Action Parameters	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: **CoS**: Classify Class of Service. **DPL**: Classify Drop Precedence Level. **DSCP**: Classify DSCP value. **PCP**: Classify PCP value. **DEI**: Classify DEI value. **Policy**: Classify ACL Policy number.	-

The user can modify each QCE (QoS Control Entry) in the table using the following buttons:

⊕: Inserts a new QCE before the current row.

ⓔ: Edits the QCE.

⬆: Moves the QCE up the list.

⬇: Moves the QCE down the list.

⊗: Deletes the QCE.

⊕: The lowest plus sign adds a new entry at the bottom of the QCE listings.

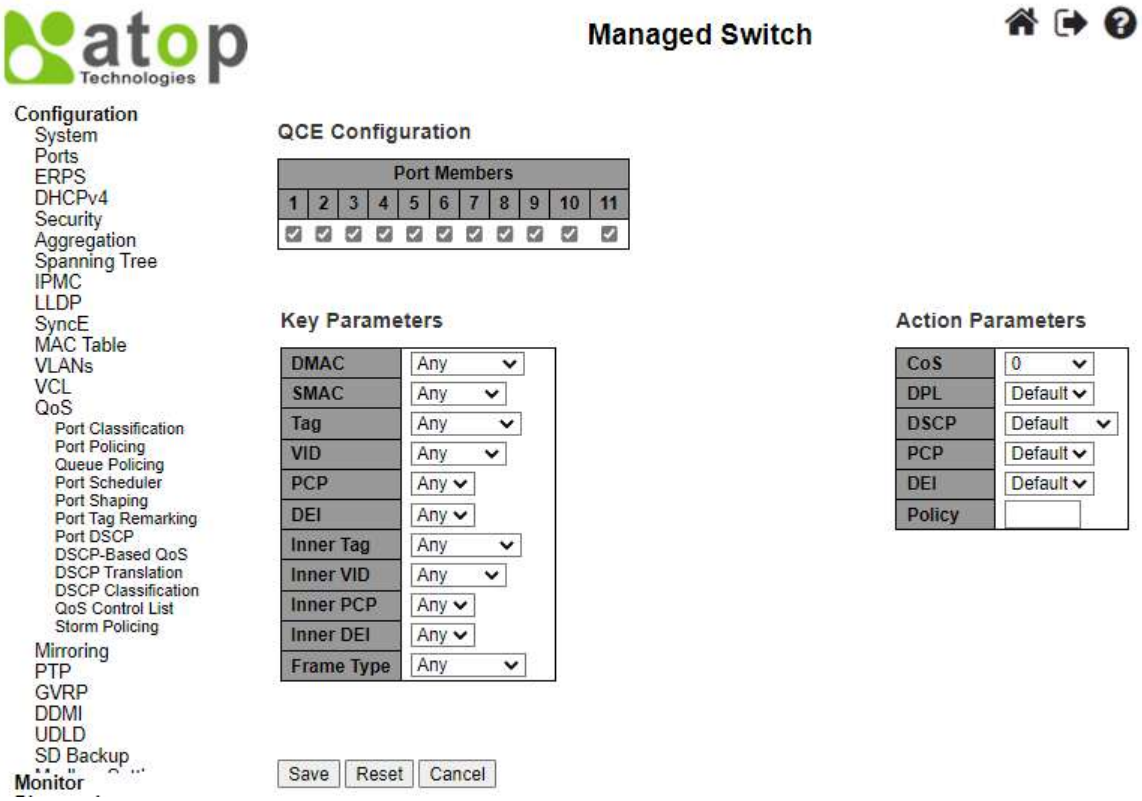


Figure 2.107 Adding New QCE Configuration

Table 2.93 Descriptions of QoS Control Entry's Parameters

Label	Description	Factory Default
Port Members	Check the checkbox button to include the port in the QCL entry. By default, all ports are included.	All ports

Label	Description	Factory Default
Key Parameters	Key configuration is described as below: **DMAC** Destination MAC address: Possible values are 'Unicast', 'Multicast', 'Broadcast', 'Specific' (xx-xx-xx-xx-xx-xx) or 'Any'. **SMAC** Source MAC address: xx-xx-xx-xx-xx-xx or 'Any'. **Tag** Value of Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'. **VID** Valid value of VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs. **PCP** Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. **DEI** Valid value of DEI can be '0', '1' or 'Any'. **Inner Tag** Value of Inner Tag field can be 'Untagged', 'Tagged', 'C-Tagged', 'S-Tagged' or 'Any'. All inner tag parameters depend on the Key Type configuration in QoS Ingress Port Classification Help. **Inner VID** Valid value of Inner VLAN ID can be any value in the range 1-4095 or 'Any'; user can enter either a specific value or a range of VIDs. **Inner PCP** Valid value of Inner PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. **Inner DEI** Valid value of Inner DEI can be '0', '1' or 'Any'. **Frame Type** Frame Type can have any of the following values: 1. **Any** 2. **EtherType** 3. **LLC** 4. **SNAP** 5. **IPv4** 6. **IPv6** Note: All frame types are explained in the next Table.	Any
Action Parameters	**CoS** Class of Service: (0-7) or 'Default'. **DPL** Drop Precedence Level: (0-1) or 'Default'. **DSCP** DSCP: (0-63, BE, CS1-CS7, EF or AF11-AF43) or 'Default'. **PCP** PCP: (0-7) or 'Default'. Note: PCP and DEI cannot be set individually. **DEI** DEI: (0-1) or 'Default'. **Policy** ACL Policy number: (0-63) or 'Default' (empty field). 'Default' means that the default classified value is not modified by this QCE.	Default

Table 2.94 Description of Frame Type

Frame Type	Description
Any	Allow all types of frames.
EtherType	**Ether Type** Valid Ether Type can be 0x600-0xFFFF excluding 0x800(IPv4) and 0x86DD(IPv6) or 'Any'.
LLC	**DSAP Address** Valid DSAP (Destination Service Access Point) can vary from 0x00 to 0xFF or 'Any'. **SSAP Address** Valid SSAP(Source Service Access Point) can vary from 0x00 to 0xFF or 'Any'. **Control** Valid Control field can vary from 0x00 to 0xFF or 'Any'.
SNAP	**PID** Valid PID (a.k.a Ether Type) can be 0x0000-0xFFFF or 'Any'.
IPv4	**Protocol** IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'. **Source IP** Specific Source IP address in value/mask format or 'Any'. IP and Mask are in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When Mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero. **Destination IP** Specific Destination IP address in value/mask format or 'Any'. **IP Fragment** IPv4 frame fragmented option: 'Yes', 'No' or 'Any'. **DSCP** Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. **Sport** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol

Frame Type	Description
	UDP/TCP. **Dport** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.
IPv6	**Protocol** IP protocol number: (0-255, 'TCP' or 'UDP') or 'Any'. **Source IP** 32 LS bits of IPv6 source address in value/mask format or 'Any'. **Destination IP** Specific Destination IP address in value/mask format or 'Any'. **DSCP** Diffserv Code Point value (DSCP): It can be a specific value, range of values or 'Any'. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43. **Sport** Source TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP. **Dport** Destination TCP/UDP port:(0-65535) or 'Any', specific or port range applicable for IP protocol UDP/TCP.

Click **Save** button to save the configuration and move to main QCL page. Click **Reset** button to undo any changes made locally and revert to previously saved values. Click **Cancel** button to return to the previous page without saving the configuration change.

2.15.12 Storm Policing

Global storm policers for the managed switch are configured on this webpage as shown in Figure 2.108. There are unicast storm policer, multicast storm policer, and broadcast storm policer. These only affect flooded frames, i.e., frames with a (VLAN ID, DMAC) pair not present in the MAC Address table. The settings are described in Table 2.95.

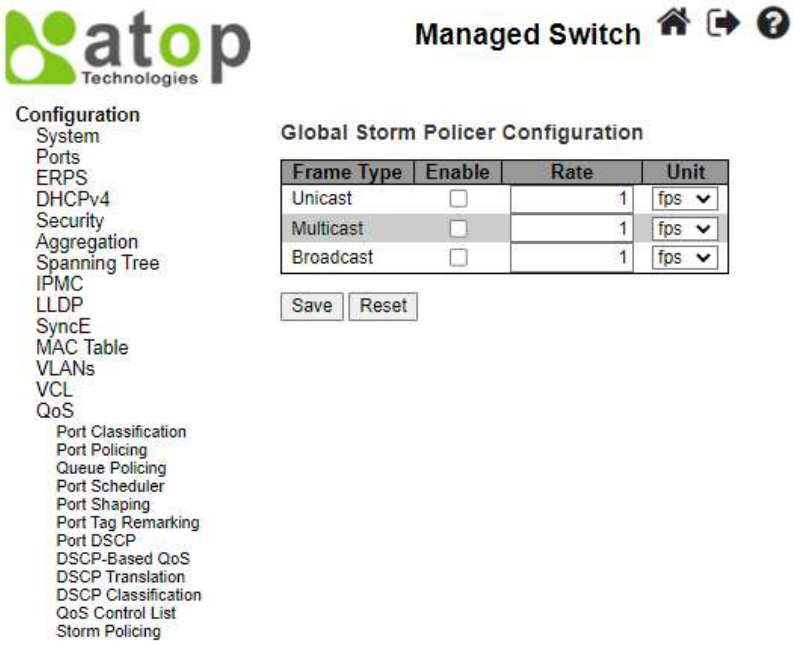


Figure 2.108 Webpage to Configure Storm Policing of QoS

Table 2.95 Descriptions of Storm Policing Configuration of QoS

Label	Description	Factory Default
Frame Type	The frame type for which the configuration below applies.	-
Enable	Enable or disable the global storm policer for the given frame type.	Unchecked
Rate	Controls the rate for the global storm policer. This value is restricted to 1-1024000 when "Unit" is fps, and 1-1024 when "Unit" is kfps. The rate is internally rounded up to the nearest value supported by the global storm policer. Supported	1

	rates are 1, 2, 4, 8, 16, 32, 64, 128, 256 and 512 fps for rates <= 512 fps and 1, 2, 4, 8, 16, 32, 64, 128, 256, 512 and 1024 kfps for rates > 512 fps.	
Unit	Controls the unit of measure for the global storm policer rate as fps or kfps.	fps

Click **Save** button to save the setting configuration. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.16 Mirroring

In order to help the network administrator keeps track of network activities, the managed switch supports port mirroring, which allows incoming and/or outgoing traffic to be monitored by a single port that is defined as a **mirror port**. Note that the mirrored network traffic can be analysed by a network analyser or a sniffer for network performance or security monitoring purposes. Figure 2.110 shows the Mirror Port webpage. The descriptions of port mirroring options are summarized in Table 2.96.

Port mirroring or traffic mirroring enables users to monitor network traffic passing in, or out of, a set of ports. can then pass this traffic to a destination port on the same router. Traffic mirroring copies traffic from one or more source ports and sends the copied traffic to one or more destinations for analysis by a network analyser or other monitoring device. However, traffic from one source port can be copied to only one destination port. Traffic mirroring does not affect the flow of traffic on the source ports, and allows the mirrored traffic to be sent to a destination port. For example, you need to attach a traffic analyser to the router if you want to capture Ethernet traffic that is sent by host A to host B. Traffic between host A and host B is also seen on the destination port.

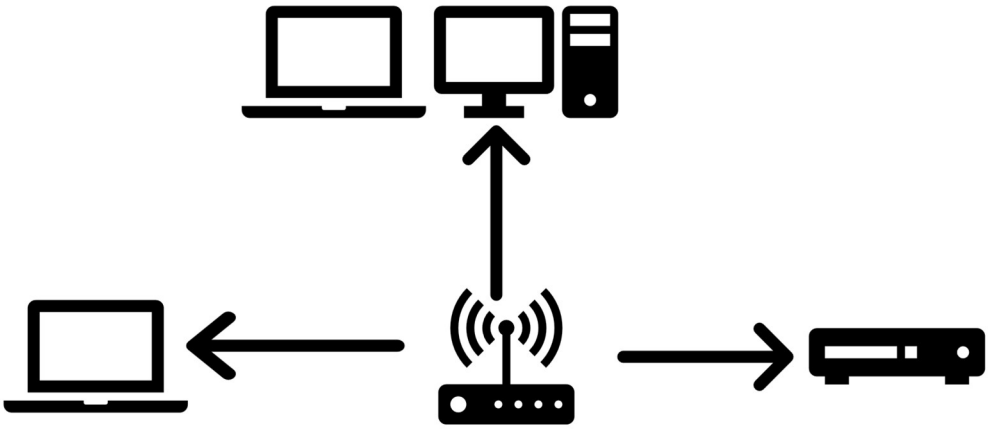


Figure 2.109 Traffic Mirroring Operation

When local traffic mirroring is enabled, the traffic analyser is attached directly to the port of the same router that is configured to receive a copy of every packet that host A sends. This port is called a traffic mirroring port. The other sections of this document describe how you can fine tune this feature.

The following types of traffic mirroring are supported:

- Local traffic mirroring: This is the most basic form of traffic mirroring. The network analyzer orsniffer is directly attached to the destination interface. In other words, all monitored ports are all located on the same router as the destination port.
- Layer 2 or Layer 3 traffic mirroring: Both Layer 2 and Layer 3 source ports can be mirrored.

Mirroring is a feature for switched port analyzer. The administrator can use the Mirroring to debug network problems. The selected traffic can be mirrored or copied on a destination port where a network analyzer can be attached to analyze the network traffic. Remote Mirroring is an extend function of Mirroring. It can extend the destination port in other switch so that the administrator can analyze the network traffic on the other switches. If you want to get the tagged mirrored traffic, you have to set VLAN egress tagging as "Tag All" on the reflector port. On the other hand, if you want to get untagged mirrored traffic, you have to set VLAN egress tagging as "Untag ALL" on the reflector port.

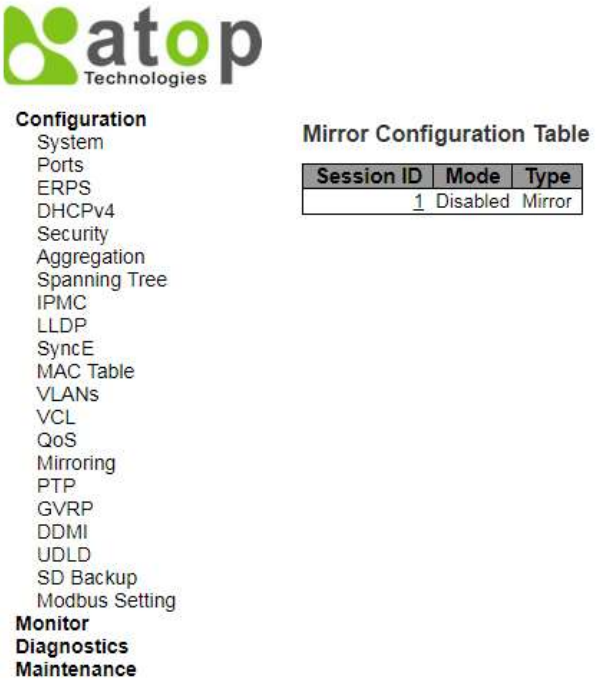


Figure 2.110 Webpage to Configure Mirroring

Table 2.96 Descriptions of Mirroring Webpage

Label	Description	Factory Default
Session ID	Display Mirror feature session id.	1
Mode	To Enabled/Disabled the Mirroring function.	Disabled
Type	Display switch mirroring type. **Mirror**: The switch is running on mirror mode. The source port(s) and destination port are located on this switch.	Mirror
VLAN ID	The VLAN ID points out where the monitor packet will copy to. The default VLAN ID is 200.	-
Port Configuration	**Port:** The logical port for the settings contained in the same row. **Source:** select mirror mode **Disabled** : Neither frames transmitted nor frames received are mirrored. **Both** : Frames received and frames transmitted are mirrored on the **Destination port**. **Rx only** : Frames received on this port are mirrored on the **Destination port**. Frames transmitted are not mirrored. **Tx only** : Frames transmitted on this port are mirrored on the **Destination port**. Frames received are not mirrored. **Destination:** select destination port This checkbox is designed for mirror Mirroring. The **destination port** is a switched port that you receive a copy of traffic from the source port. Note1: On mirror mode, the device only supports one destination port. Note2: The destination port needs to disable MAC Table learning.	-

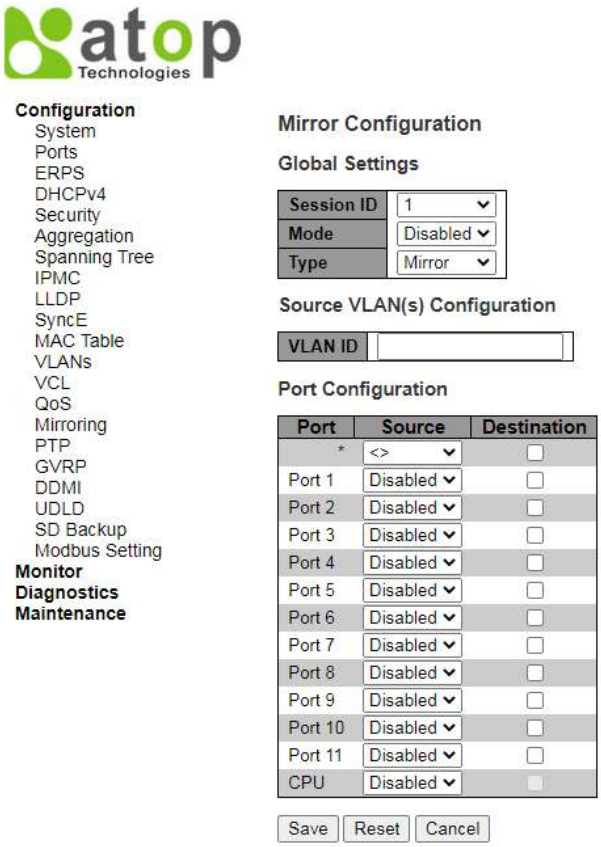


Figure 2.111 Webpage to Detailed Configure Mirroring for Session ID

2.17 PTP

Precision Time Protocol (PTP) is defined in IEEE 1588 as Precision Clock Synchronization for Networked Measurements and Control Systems, and was developed to synchronize the clocks in packet-based networks that include distributed device clocks of varying precision and stability. PTP, which is a high-precision time protocol, can be used with measurement and control systems in local area network that require precise time synchronization. PTP is designed specifically for industrial, networked measurement and control systems, and is optimal for use in distributed systems because it requires minimal bandwidth and little processing overhead.

Smart grid power automation applications such as peak-hour billing, virtual power generators, and outage monitoring and management, require extremely precise time accuracy and stability. Timing precision improves network monitoring accuracy and troubleshooting ability.

In addition to providing time accuracy and synchronization, the PTP message-based protocol can be implemented on packet-based networks, such as Ethernet networks. The benefits of using PTP in an Ethernet network include:

- Low cost and easy setup in existing Ethernet networks
- Limited bandwidth is required for PTP data packets

In an Ethernet network, switches provide a full-duplex communication path between network devices. Switches send data packets to packet destinations using address information contained in the packets. When the switch attempts to send multiple packets simultaneously, some of the packets are buffered by the switch so that they are not lost before they are sent. When the buffer is full, the switch delays sending packets. This delay can cause device clocks on the network to lose synchronization with one another.

Additional delays can occur when packets entering a switch are stored in local memory while the switch searches the MAC address table to verify packet CRC fields. This process causes variations in packet forwarding time latency, and these variations can result in asymmetrical packet delay times.

Adding PTP to a network can compensate for these latency and delay problems by correctly adjusting device clocks so that they stay synchronized with one another. PTP enables network switches to function as PTP devices, including boundary clocks (BCs) and transparent clocks (TCs).

To ensure clock synchronization, PTP requires an accurate measurement of the communication path delay between the time source or *primary clock* and the client clock. The system clocks can be categorized based on the role of the node in the network. They are broadly categorized into ordinary clocks and boundary clocks. The primary clock and the client clock are known as ordinary clocks. The boundary clock can operate as either a primary clock or a client clock. The following list explains these clocks in detail:

- Primary clock—The primary clock transmits the messages to the PTP clients (also called client node or boundary node). This allows the clients to establish their relative time distance and offset from the primary clock (which is the reference point) for phase synchronization. Delivery mechanism to the clients is either unicast or multicast packets over Ethernet or UDP.
- Member clock—located in the PTP client (also called client node), the client clock performs clock and time recovery operations based on the received and requested timestamps from the primary clock.
- Boundary clock—The boundary clock operates as a combination of the primary and client clocks. The boundary clock endpoint acts as a client clock to the primary clock, and also acts as the primary to all the slaves reporting to the boundary endpoint.

PTP sends messages between the primary clock and client clock device to determine the delay measurement. Then, PTP measures the exact message transmit and receive times and uses these times to calculate the communication path delay. PTP then adjusts current time information contained in network data for the calculated delay, resulting in more accurate time information.
This delay measurement principle determines path delay between devices on the network, and the local clocks are adjusted for this delay using a series of messages sent between masters and slaves. The one-way delay time is calculated by averaging the path delay of the transmit and receive messages. This calculation assumes a symmetrical communication path; however, switched networks do not necessarily have symmetrical communication paths, due to the buffering process.
PTP provides a method, using transparent clocks, to measure and account for the delay in a time-interval field in network timing packets, making the switches temporarily transparent to the master and slave nodes on the network. An end-to-end transparent clock forwards all messages on the network in the same way that a switch does.

The PTP webpage as shown in Figure 2.112 allows the user to configure and inspect the current PTP clock settings. Table 2.97 summarizes the parameters for PTP Clock Configuration.

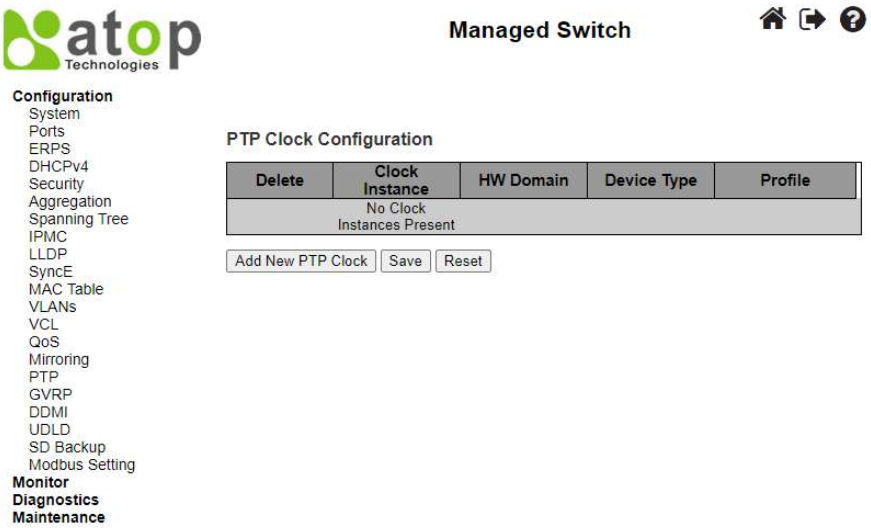


Figure 2.112 Webpage to Configure PTP

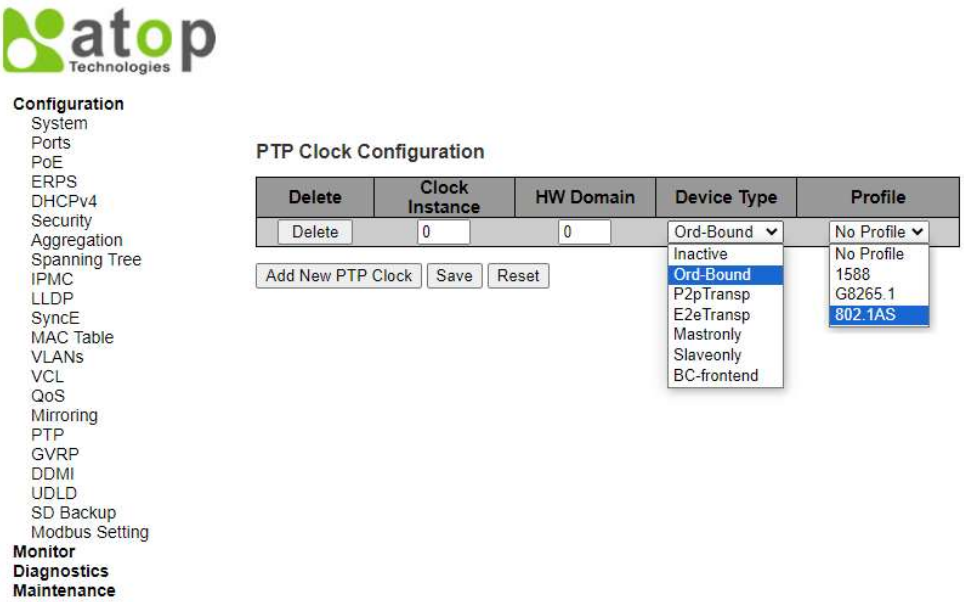


Figure 2.113 Webpage to Add New PTP Clock

Table 2.97 Descriptions of PTP Clock Configuration

Label	Description	Factory Default
Delete	Check this box and click on '**Save**' button to delete the clock instance.	-
Clock Instance	Indicates the Instance of a particular Clock Instance [0…3]. Click on the Clock Instance number to edit the Clock details.	
HW Domain	Indicates the HW clock domain used by the clock.	
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - clock's Device Type is End to End Transparent Clock. 4. Master Only - clock's Device Type is Master Only. 5. Slave Only - clock's Device Type is Slave Only.	
Profile	Indicates the profile used by the clock.	

After Clicking Add NEW PTP Clock button, another webpage will be launched, as shown in Figure 2.113. Table 2.98 summarizes the parameters for new PTP Clock Configuration.

Table 2.98 Descriptions of New PTP Clock Configuration

Label	Description	Factory Default
Delete	Check this box and click on 'Save' to delete the clock instance.	-
Clock Instance	Indicates the instance number of a particular Clock Instance [0..3]. Click on the Clock Instance number to edit the Clock details.	0
HW Domain	Indicates the HW clock domain used by the clock.	0
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound - clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - clock's Device Type is End to End Transparent Clock. 4. Master Only - clock's Device Type is Master Only. 5. Slave Only - clock's Device Type is Slave Only.	Ord-bound
Profile	Indicates the profile used by the clock.	No Profile

Click **Add New PTP Clock** button to create a new clock instance. Click **Save** button to save the setting configuration. Click **Reset** button to keep to the original setting.

2.18 GVRP

GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a standard-based protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.1Q specification, which defines a method of tagging frames with VLAN configuration data over networ trunk interconnects. GVRP is based on Generic Attribute Registration Protocol (GARP) and IEEE 802.1r, which defines procedures for end stations and switches in a VLAN to register and deregister attributes, such as identifiers or addresses, with each other. It provides every end station and switch with a current record of all the other end stations and switches that can be reached on the network. GVRP is similar to GARP, as both eliminate unnecessary network traffic by preventing attempts to transmit information to unregistered users. In addition, it is necessary to manually configure only one switch with all the other switches then being updated automatically.

Becoming part of a formal IEEE 802.1ak standard amendment in 2007, Multiple VLAN Registration Protocol replaced GVRP, as it was found to be prone to performance issues that could potentially cause prolonged network convergence. This delay was found to create bandwidth degradation on the network at the point where the delayed convergence appeared. Technically, GVRP is still included as part of the IEEE standard, as the amendment did not completely remove it. It is expected to be removed in the future, but until that happens, GVRP is still being used.

GVRP can be used to keep VLAN configurations on trunk interfaces organized across the network on large networks that consist of dozens or even hundreds of VLAN segments. There are three benefits for administrators that enable GVRP on a network:

- It enables switches to automatically delete unused VLANs so that only the VLANs that are in use are transported across 802.1Q trunk links.
- It enables admins to configure a new VLAN on one switch and then have it propagate the configuration across all network switches participating in the GVRP process.
- GVRP can eliminate some unnecessary broadcast traffic on the network, reducing bandwidth overhead used for network management.

GVRP works as follows. When two or more switches are connected via 802.1Q trunk ports with GVRP enabled in a network, these switches will begin to communicate statically or dynamically through VLAN information. Switches with statically configured VLANs will advertise them to connected switches using GVRP data units. Those units are specifically designed management packets used to share VLAN information. If a switch learns of a new VLAN from its neighbor, this VLAN is added to the list of VLAN tags that can be transported across the link The VLAN that learned the new information can then pass along its own statically configured VLANs, in addition to ones learned from its neighbor. For loop avoidance, switch cannot send dynamically learned VLAN information out the same interface that it was learned on.
All the dynamically learned VLAN information is stored in switch memory. So, if power is lost or the switch is rebooted, the dynamically learned VLAN information is lost, and the VLANs are pruned from the trunk interface. But, once the switches begin communication again, they will relearn the shared VLAN information to bring the network and all VLANs back into a fully informed state.

2.18.1 Global config

This GVRP→Global config webpage shown in Figure 2.114 allows the user to configure the global GVRP configuration settings that are commonly applied to all GVRP enabled ports.

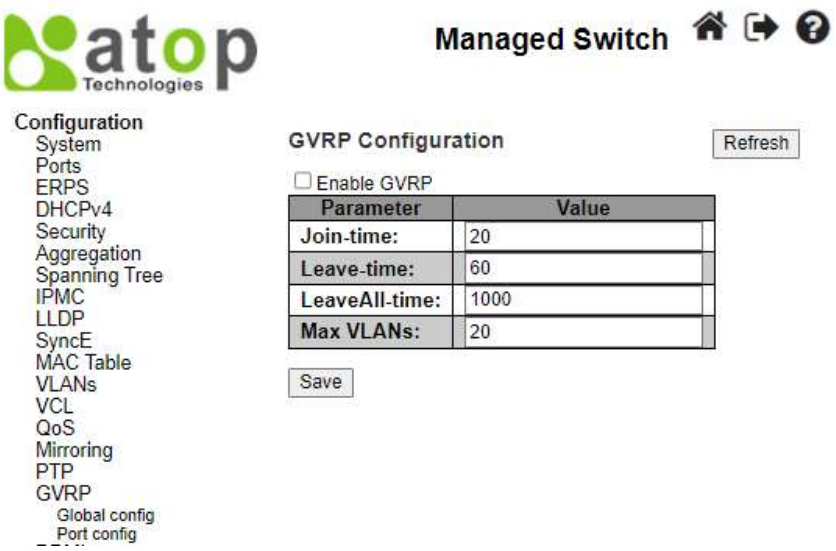


Figure 2.114 Webpage to Configure GVRP Globally

Table 2.99 Descriptions of GVRP Globally Configuration

Label	Description	Factory Default
Join-time	Join-time is a value in the range of 1-20cs, i.e. in units of one hundredth of a second. The default value is 20cs	20
Leave-time	Leave-time is a value in the range of 60-300cs, i.e. in units of one hundredth of a second. The default is 60cs.	60
LeaveAll-time	LeaveAll-time is a value in the range of 1000-5000cs, i.e. in units of one hundredth of a second. The default is 1000cs.	1000
Max VLANs	When GVRP is enabled, a maximum number of VLANs supported by GVRP is specified. By default, this number is 20. This number can only be changed when GVRP is turned off.	20

Click **Save** button to save the setting configuration. Click **Refresh** box to refresh the page immediately. Note that unsaved changes will be lost.

2.18.2 Port config

The GVRP Port Config webpage shown in Figure 2.115 allows the user to enable or disable a port for GVRP operation. This configuration can be performed either before or after GVRP is configured globally; however, the protocol operation will remain the same. Table 2.100 describes the labels on GVRP Port Configuration.

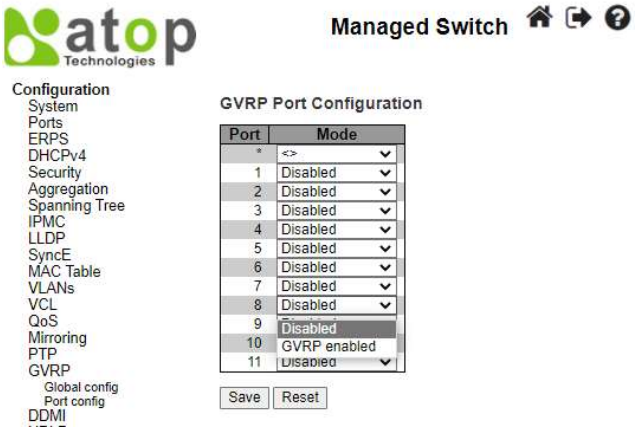


Figure 2.115 Webpage to Configure Port for GVRP

Table 2.100 Descriptions of GVRP PortConfiguration

Label	Description	Factory Default
Port	The logical port that is to be configured.	-
Mode	Mode can be either 'Disabled' or 'GVRP enabled'. These values turn the GVRP feature off or on respectively for the port in question.	Disabled

Click **Save** button to save the setting configuration. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.19 sFlow

This page allows for configuring sFlow. The configuration is divided into two parts: Configuration of the sFlow receiver (a.k.a. sFlow collector) and configuration of per-port flow and counter samplers.
sFlow configuration is not persisted to non-volatile memory, which means that a reboot will disable sFlow sampling.

Table 2.101 Descriptions of sFlow PortConfiguration

Label	Description	Factory Default
IP Adress	The IP address used as Agent IP address in sFlow datagrams. It serves as a unique key that will identify this agent over extended periods of time. Both IPv4 and IPv6 addresses are supported.	127.0.0.1
IP Address/ Hostnam e	The IP address or hostname of the sFlow receiver. Both IPv4 and IPv6 addresses are supported.	0.0.0.0
UDP port	The UDP port on which the sFlow receiver listens to sFlow datagrams. If set to 0 (zero), the default port (6343) is used.	6343
Timeout	The number of seconds remaining before sampling stops and the current sFlow owner is released. While active, the current time left can be updated with a click on the Refresh-button. If locally managed, the timeout can be changed on the fly without affecting any other settings. Valid range is 0 to 2147483647 seconds.	0
Max. Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. This should be set to a value that avoids fragmentation of the sFlow datagrams. Valid range is 200 to 1468 bytes with default being 1400 bytes.	1400Flow
Flow Sampler Enabled	Enables/disables flow sampling on this port.	Unchecke d
Flow Sampler Samplein g Rate	The statistical sampling rate for packet sampling. Set to N to sample on average 1/Nth of the packets transmitted/received on the port. Not all sampling rates are achievable. If an unsupported sampling rate is requested, the switch will automatically adjust it to the closest achievable. This will be reported back in this field. Valid range is 1 to 32767.	0
Flow Sampler , Max. Header	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram. Valid range is 14 to 200 bytes with default being 128 bytes. To have room for any frame, the maximum datagram size should be roughly 100 bytes larger than the maximum header size. If the maximum datagram size does not take into account the maximum header size, samples may be dropped.	128

Counter Poller Enabled	Enables/disables counter polling on this port.	Unchecked
Counter Poller Interval	With counter polling enabled, this specifies the interval - in seconds - between counter poller samples. Valid range is 1 to 3600 seconds.	0

2.20 DDMI

Digital Diagnostics Monitoring Interface (DDMI) allows users to perform diagnostic tests on transceiver modules such as small form-factor pluggable (SFP). Click Enabled this feature to view the various parameters of the transceiver module, such as temperature, voltage, transmission power, and so on. Figure 2.116 shows the DDMI configuration webpage. Table 2.102 describes the option on DDMI Configuration webpage.

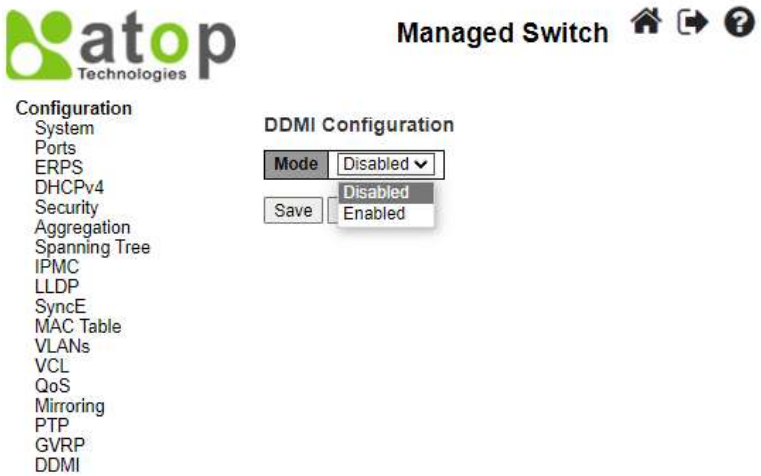


Figure 2.116 Webpage to Configure DDMI

Table 2.102 Descriptions of DDMI Configuration

Label	Description	Factory Default
Mode	Indicates the DDMI mode operation. Possible modes are: Enabled: Enable DDMI mode operation. Disabled: Disable DDMI mode operation.	Disabled

Click **Save button** to save changes. Click **Reset button** to undo any changes made locally and revert to previously saved values.

2.21 UDLD

Unidirectional Link Detection (UDLD) is a layer 2 protocol used to determine the physical status of a link. The purpose of UDL) is to detect and deter issues that arise from Unidirectional Links. UDLD helps to prevent forwarding loops and blackholding of traffic by identifying and acting on logical one-way links that would otherwise go undetected. UDLD works with the Layer 1 mechanisms to determine the physical status of a link. At Layer 1, auto-negotiation takes care of physical signaling and fault detection. UDLD performs tasks that auto-negotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected ports. When users enable both auto-negotiation and UDLD, Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

UDLD works by exchanging **UDLD** protocol packets that include information about the port's **device and port ID** between the neighboring devices. In order for UDLD to work, both devices on the link must support UDLD and have

it enabled on respective ports. Each switch port configured for UDLD sends UDLD protocol packets that contain the port's own device/port ID, and the neighbor's device/port IDs seen by UDLD on that port. Neighboring ports should see their own device/port ID (echo) in the packets received from the other side.

Because of this, a port should receive its own device and port ID information from its neighbor if the link is bi-directional. If a port does not receive information about its own device and port ID from its neighbor for a specific duration of time, the link is considered to be unidirectional. This can also occur when the link is up on both sides, but one side is not receiving packets, or when wiring mistakes occur, causing the transmit and receive wires to not be connected to the same ports on both ends of a link.

This echo-algorithm allows detection of these issues:

- Link is up on both sides; however, packets are only received by one side.
- Wiring mistakes when receive and transmit fibers are not connected to the same port on the remote side.

Once the unidirectional link is detected by UDLD, the respective port is disabled. Port shutdown by UDLD remains disabled until it is manually reenabled, or until errdisable timeout expires (if configured).

UDLD can operate in two modes: normal and aggressive. In normal mode, if the link state of the port was determined to be bi-directional and the UDLD information times out, no action is taken by UDLD. The port state for UDLD is marked as undetermined. The port behaves according to its STP state. In aggressive mode, if the link state of the port is determined to be bi-directional and the UDLD information times out while the link on the port is still up, UDLD tries to re-establish the state of the port. If not successful, the port is put into the **errdisable** state.

Aging of UDLD information happens when the port that runs UDLD does not receive UDLD packets from the neighbor port for duration of hold time. The hold time for the port is dictated by the remote port and depends on the message interval at the remote side. The shorter the message interval, the shorter the hold time and the faster the detection. Recent implementations of UDLD allow configuration of message interval.

UDLD information can age out due to the high error rate on the port caused by some physical issue or duplex mismatch. Such packet drop does not mean that the link is unidirectional and UDLD in normal mode will not disable such link.

It is important to be able to choose the right message interval in order to ensure proper detection time. The message interval should be fast enough to detect the unidirectional link before the forwarding loop is created, however, it should not overload the switch CPU. The default message interval is 7 seconds, and is fast enough to detect the unidirectional link before the forwarding loop is created with default STP timers. The detection time is approximately equal to three times the message interval.

For example: $T_{detection}$ ~ message_interval x 3

This is 21 seconds for the default message interval of 7 seconds.

It takes $T_{reconvergence}$=max_age + 2x forward_delay for the STP to reconverge in case of unidirectional link failure. With the default timers, it takes 20+2x7=34 seconds.

It is recommended to keep $T_{detection} < T_{reconvergence}$ by choosing an appropriate message interval.

In aggressive mode, once the information is aged, UDLD will attempt to re-establish the link state by sending packets every second for eight seconds. If the link state is still not determined, the link is disabled.

Aggressive mode adds additional detection of these situations:

- The port is stuck (on one side the port neither transmits nor receives, however, the link is up on both sides).
- The link is up on one side and down on the other side. This is issue might be seen on fiber ports. When transmit fiber is unplugged on the local port, the link remains up on the local side. However, it is down on the remote side.

Most recently, fiber FastEthernet hardware implementations have Far End Fault Indication (FEFI) functions in order to bring the link down on both sides in these situations. On Gigabit Ethernet, a similar function is provided by link negotiation. Copper ports are normally not susceptible to this type of issue, as they use Ethernet link pulses to monitor the link. It is important to mention that, in both cases, no forwarding loop occurs because there is no connectivity between the ports. If the link is up on one side and down on the other, however, blackholing of traffic might occur. Aggressive UDLD is designed to prevent this.

This UDLD webpage shown Figure 2.117 allows the user to inspect the current UDLD configurations, and possibly change them as well. Table 2.103 provides the descriptions of UDLD Port Configuration.

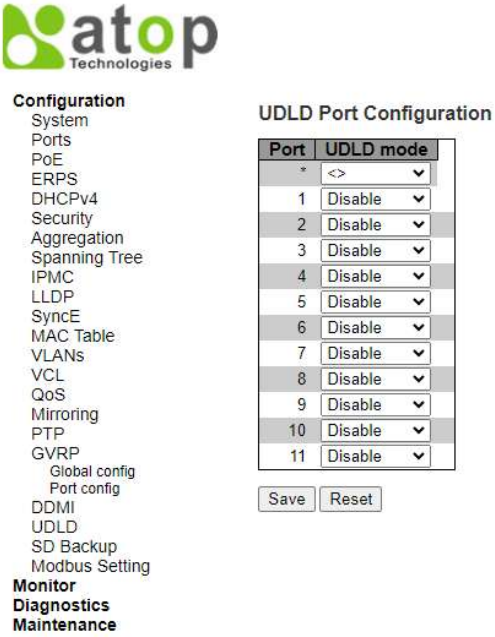


Figure 2.117 Webpage to Configure UDLD

Table 2.103 Descriptions of UDLD Port Configuration

Label	Description	Factory Default
Port	Port number of the switch.	1-11
UDLD Mode	Configures the UDLD mode on a port. Valid values are Disable, Normal and Aggressive. Default mode is Disable. • Disable in disabled mode, UDLD functionality doesn't exists on port. • Normal in normal mode, if the link state of the port was determined to be unidirectional, it will not affect the port state. Aggressive in aggressive mode, unidirectional detected ports will get shutdown. To bring back the ports up, need to disable UDLD on that port.	Disable

Click **Save** button to save the setting configuration. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.22 SD Backup

The SD card can be used instead of the internal flash memory of the switch to update or restore configuration settings. In addition, the SD card can be used to boot the switch. User can also copy IOS software and switch configuration settings from a PC or from the switch to the SD card, and then use the SD card to copy this software and settings to other switches.

SD Backup can be configured on this page as shown in Figure 2.118. Options for SD Backup can be set according to the descriptions in Table 2.104.

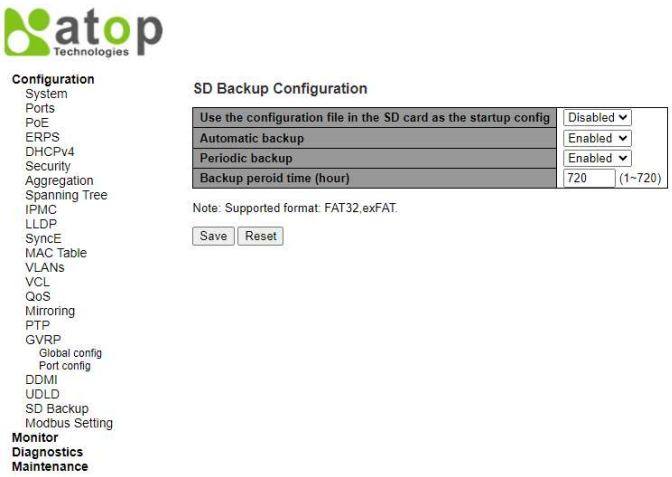


Figure 2.118 Webpage to Configure SD Backup

Table 2.104 Descriptions of SD Backup Configuration

Label	Description	Factory Default
Use the configuration file form sd	The startup-config file will be replaced from the newest config file in sd card when booting switch.	Disabled
Automatic backup	Backup the starup-config into sd card folder "Automatic_backup" when saving startup-config. Only have one file be saved.	Enabled
Periodic backup	Backup the starup-config into sd card folder "Period_backup" when saving startup-config. Multiple files can be saved which depend on "Backup period time".	Enabled
Backup period time (Hr)	The backup Periodic time setting.	720

Click **Save** button to save the setting configuration. Click **Reset** button to undo any changes made locally and revert to previously saved values.

2.23 Modbus Setting

Atop's managed switch can be connected to a Modbus network using Modbus TCP/IP protocol which is an industrial network protocol for controlling automation equipment. The managed switch's status and settings can be read and written through Modbus TCP/IP protocol which operates similar to a Management Information Base (MIB) browser. The managed switch will be a Modbus slave which can be remotely configured by a Modbus master. The Modbus slave address must be set to match the setting inside the Modbus master. In order to access the managed switch, a **Modbus Address** must be assigned as described in this subsection. Figure 2.119 shows the Modbus Setting webpage.

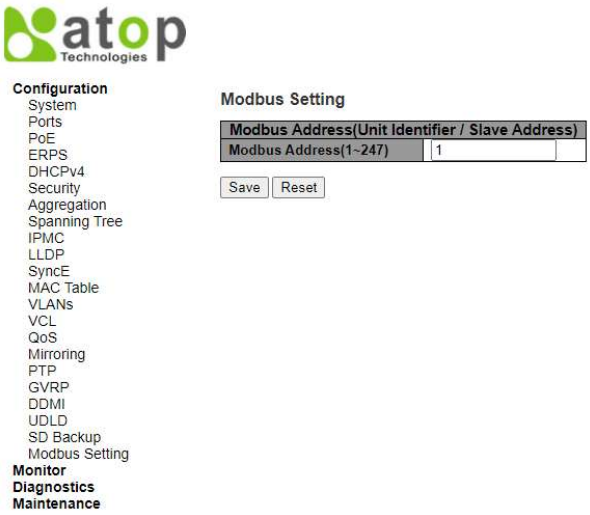


Figure 2.119 Webpage to Configure Modbus Setting

Table 2.105 Descriptions of Modbus Setting PortConfiguration

Label	Description	Factory Default
Modbus Address	Identifier for modbus slave device, range from 1 to 247	1

Click **Save** button to save the setting configuration. Click **Reset** button to undo any changes made locally and revert to previously saved values.

Users can use Modbus TCP/IP compatible applications such as **Modbus Poll** to configure the switch. Note that Modbus Poll can be download from http://www.modbustools.com/download.html. The Modbus Poll 64-bit version 9.2.2, Build 1343 was used in this document. Atop does not provide this software to the users. Tutorial of Modbus read and write examples are illustrated below. **Note***:* The switch only supports Modbus function code 03, 04 *(*for Read*)* and 06 *(*for Write*)*.

Read Registers (This example shows how to read the switch's IP address.)

Address	Data Type	Read/Write	Description
0x0051 (81)	2 words	R	IP Address of switch Ex: IP = 10.0.50.1 Word 0 Hi byte = 0x0A Word 0 Lo byte = 0x00 Word 1 Hi byte = 0x32 Word 1 Lo byte = 0x01

Figure 2.120 Mapping Table of Modbus Address for Switch's IP Address

1. Make sure that a supervising computer (Modbus Master) is connected to your target switch (Modbus Slave) over Ethernet network.
2. Launch **Modbus Poll** in the supervising computer. Note a registration key may be required for a long-term use of Modbus Poll after 30-day evaluation period. Additionally, there is a 10-minute trial limitation for the connection to the managed switch.
3. Click **Connect** button on the top toolbar to enter Connection Setup dialog by selecting **Connect…** menu as shown in Figure 2.121 Entering Connection Setup Menu of the Modbus Poll

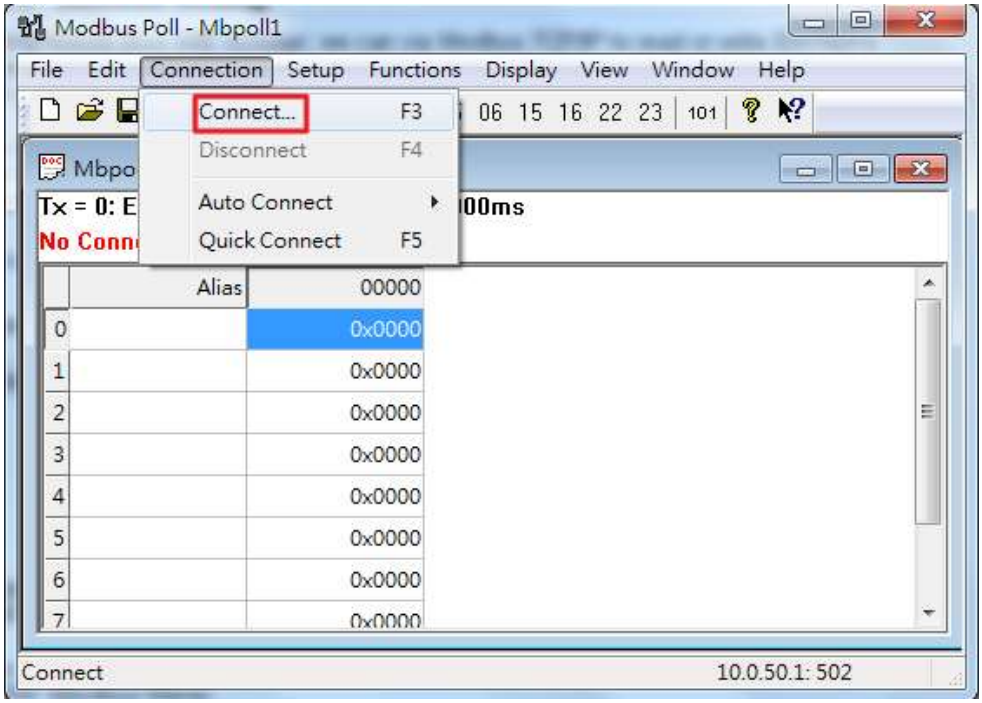


Figure 2.121 Entering Connection Setup Menu of the Modbus Poll

4. Select **Modbus TCP/IP** as the **Connection** mode and enter the switch's IP address inside the **Remote Modbus Server**'s **IP Address or Node Name** field at the bottom as shown in Figure 2.122 Modbus Poll Connection Setup. The **Port** number should be set to 502. Then click **OK** button.

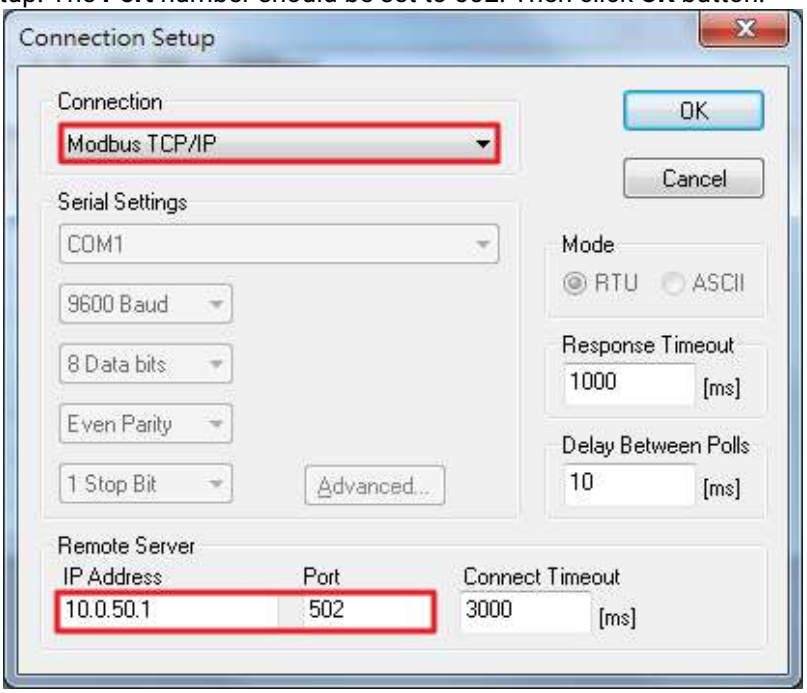


Figure 2.122 Modbus Poll Connection Setup

5. On the window Mbpoll1, select multiple cells from row 0 to row 2 by clicking on cells in second column of row 0 and row 2 while holding the shift key as shown in Figure 2.123 Multiple Cell Section in Modbus Poll.

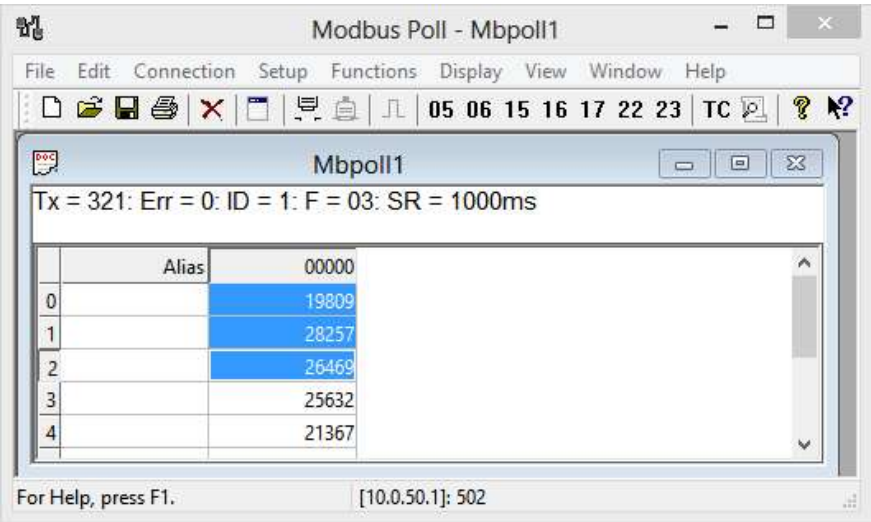


Figure 2.123 Multiple Cell Section in Modbus Poll

6. Set **Display** mode of the selected cells in previous step to HEX (hexadecimal) by selecting **Display** pull-down menu and choosing the **Hex** as shown in Figure 2.124 Set Display Mode to Hex in Modbus Poll.

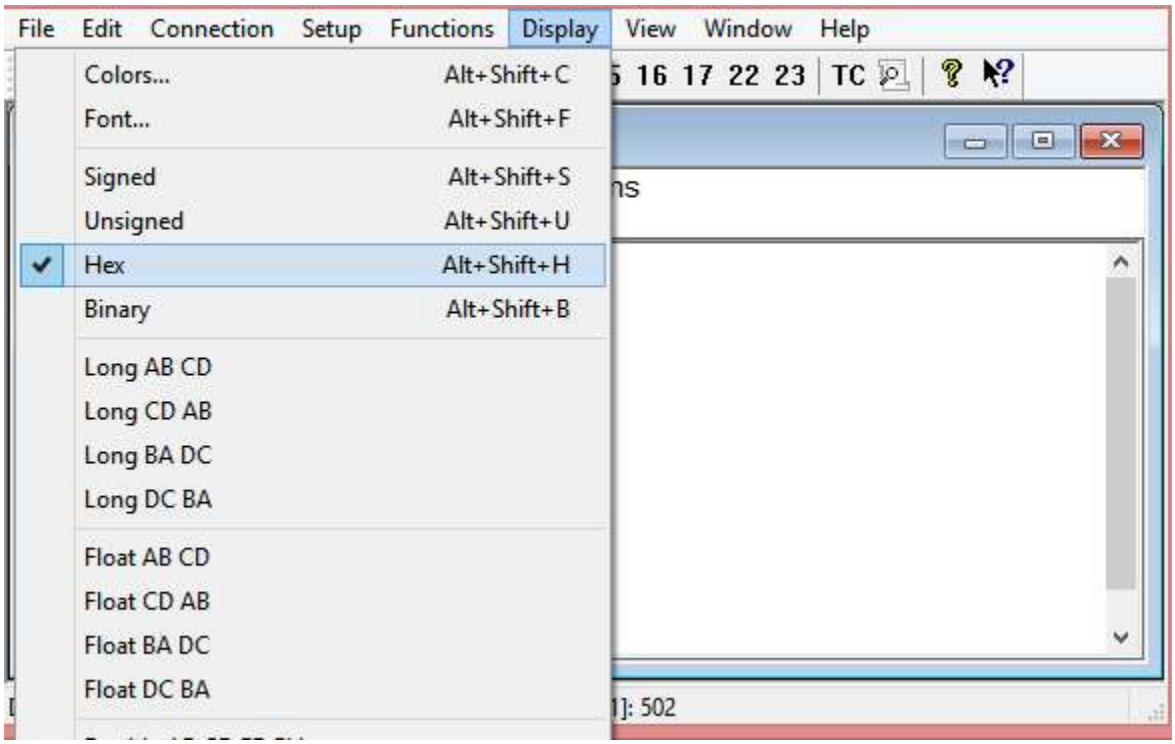


Figure 2.124 Set Display Mode to Hex in Modbus Poll

7. Click on the **Setup** pull-down menu and choose **Read/Write Definition…** as shown in Figure 2.125 Modbus Poll Setup Read/Write Definition.

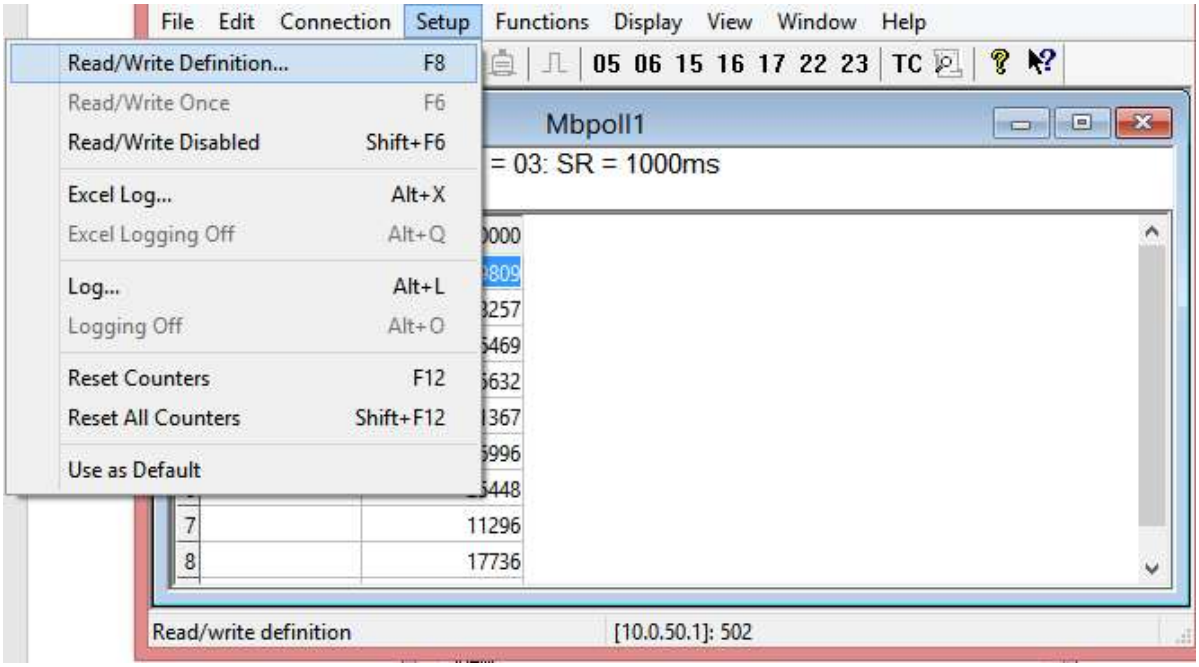


Figure 2.125 Modbus Poll Setup Read/Write Definition

8. Enter the **Slave ID** in the Modbus Poll function as shown in Figure 2.122 Modbus Poll Connection Setup, which should match the Modbus Address = 1 entered in Figure 2.126.

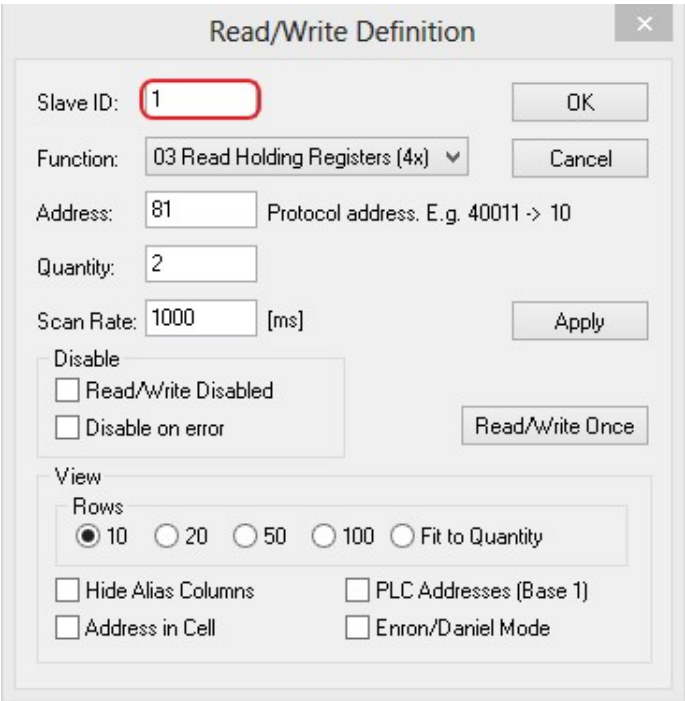


Figure 2.126 Slave ID in the Modbus Poll Function is set to 1

9. Select **Function 03** or **04** because the managed switch supports function code 03 and 04 as shown in Figure 2.127.

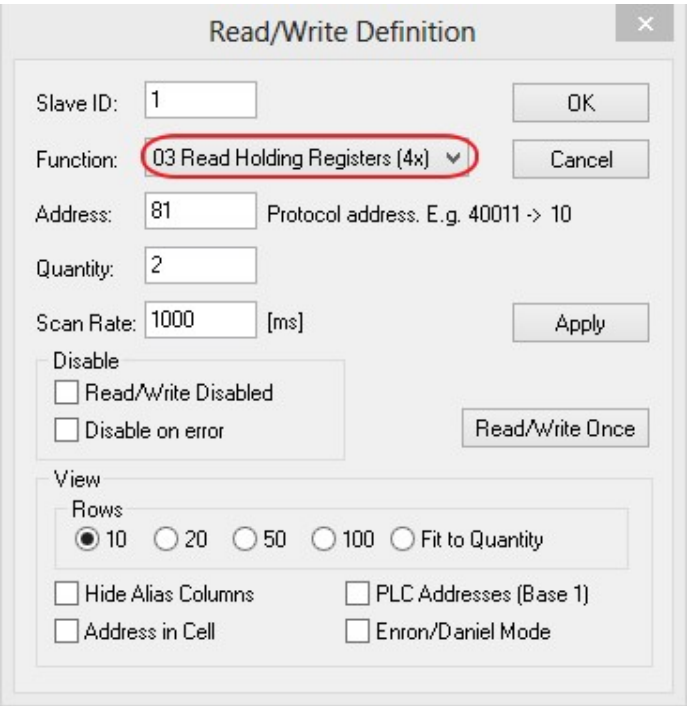


Figure 2.127 Set Code 03 in the Modbus Poll Function

10. Set starting **Address** to 81 and **Quantity** to 2 as shown in Figure 2.128.

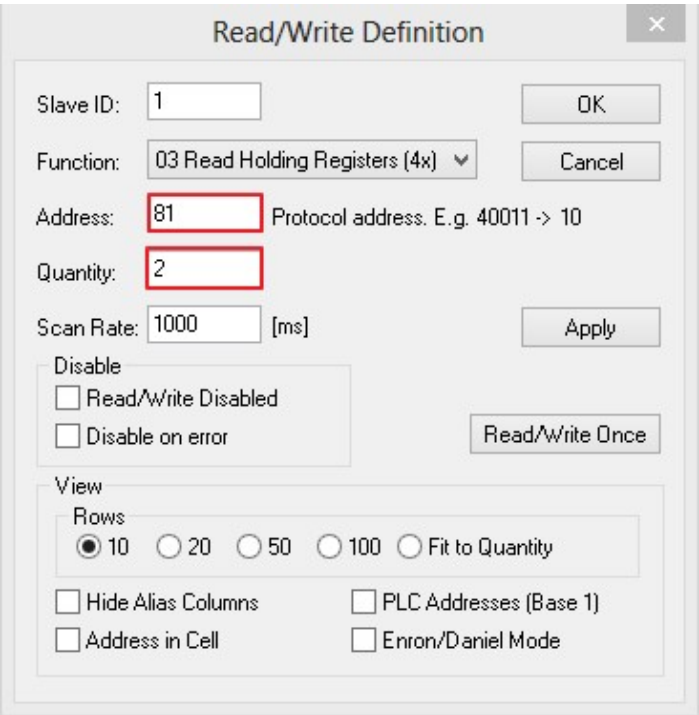


Figure 2.128 Setup Starting Address and Quantity in Modbus Poll

11. Click **OK** button to read the IP address of the switch.

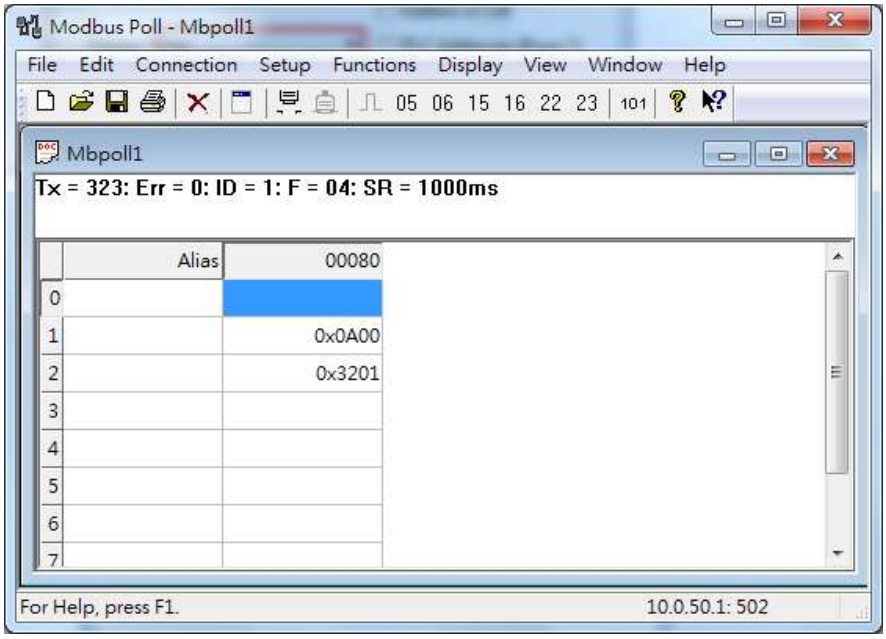


Figure 2.132 Modbus Memory Address 81 and 82 are the location of RHG9728's IP Address

12. Modbus Poll will get the values 0x0A, 0x00, 0x32, 0x01, which means that the switch's IP is 10.0.50.1 as shown in Figure 2.129.

Write Registers (This example shows how to clear the switch's Port Count (Statistics).)

Address	Data Type	Read/Write	Description
0x0100 (256)	1 word	W	Clear Port Statistics 0x0001: Do clear action

Figure 2.129 Mapping Table of Modbus Address for Clearing Port Statistics

13. Check the switch's Port TX/RX counts in **Port Statistics** page as shown in Figure 2.130.

Port Statistics Overview Auto-refresh ☐

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	7561	6791	1480609	2256480	5	0	0	0	2425
11	0	0	0	0	0	0	0	0	0

Figure 2.130 Port Count in Port Statistics Webpage

14. Click function **06** on the toolbar as shown in Figure 2.131.

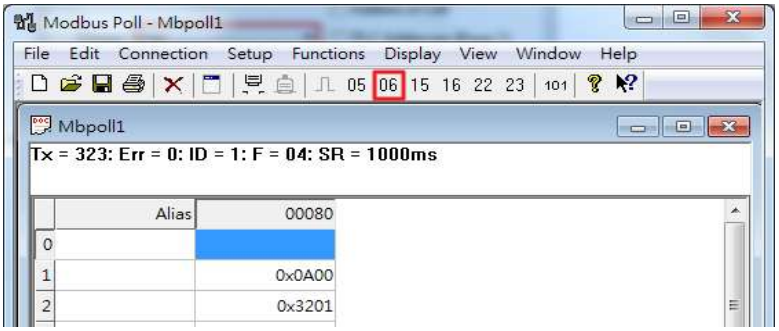


Figure 2.131 Click on Function 06 in the Modbus Poll

15. Set **Address** to 256 and **Value (HEX)** to 1 as shown in Figure 2.132, then click "**Send**" button.

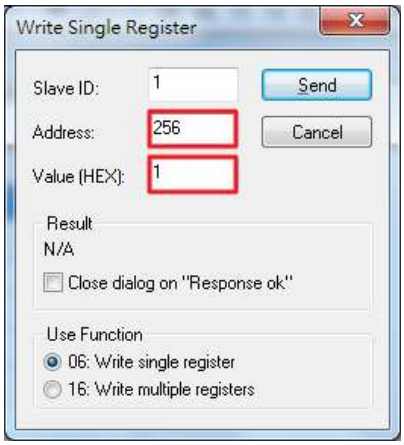


Figure 2.132 Use Modbus Poll to Clear Switch's Port Count

16. Check **Port Statistics** in the managed switch's Web UI as shown in Figure 2.133. The packet count is now cleared.

Port Statistics Overview

Auto-refresh

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0

Figure 2.133 Cleared Port Statistics

2.22 Modbus Memory Map

1. Read Registers (Support Function Code 3, 4).
2. Write Register (Support Function Code 6).
3. 1 Word = 2 Bytes.

Address	Data Type	Read/Write	Description

System Information			
0x0000 (0)	32 words	R	System Description = "Managed Switch RHG9728" Word 0 Hi byte = 'M' Word 0 Lo byte = 'a' Word 1 Hi byte = 'n' Word 1 Lo byte = 'a' Word 2 Hi byte = 'g' Word 2 Lo byte = 'e' Word 3 Hi byte = 'd' Word 3 Lo byte = ' ' Word 4 Hi byte = 'S' Word 4 Lo byte = 'w' Word 5 Hi byte = 'i' Word 5 Lo byte = 't' Word 6 Hi byte = 'c' Word 6 Lo byte = 'h' Word 7 Hi byte = ' ' Word 7 Lo byte = 'E' Word 8 Hi byte = 'H' Word 8 Lo byte = '9' Word 9 Hi byte = '7' Word 9 Lo byte = '1' Word 10 Hi byte = '1' Word 10 Lo byte = '\0'
0x0020 (32)	1 word	R	Firmware Version = Ex: Version = 1.02 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x02
0x0021 (33)	3 words	R	Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0x00 Word 0 Lo byte = 0x01 Word 1 Hi byte = 0x02 Word 1 Lo byte = 0x03 Word 2 Hi byte = 0x04 Word 2 Lo byte = 0x05
0x0024 (36)	1 word	R	Kernel Version Ex: Version = 1.03 Word 0 Hi byte = 0x01 Word 0 Lo byte = 0x03
Console Information			

0x0030 (48)	1 word	R	Baud Rate 0x0000: 4800 0x0001: 9600 0x0002: 14400 0x0003: 19200 0x0004: 28800 0x0005: 38400 0x0006: 57600 0x0007: 144000 0x0008: 115200
0x0031 (49)	1 word	R	Data Bits 0x0007: 7 0x0008: 8
0x0032 (50)	1 word	R	Parity 0x0000: None 0x0001: Odd 0x0002: Even
0x0033 (51)	1 word	R	Stop Bit 0x0001: 1 0x0002: 2
0x0034 (52)	1 word	R	Flow Control 0x0000: None
Power Information			
0x0040 (64)	1 word	R	Power Status Power 1 OK, Hi byte = 0x01 Power 1 Fail, Hi byte = 0x00 Power 2 OK, Low byte = 0x01 Power 2 Fail, Low byte = 0x00
IP Information			
0x0050 (80)	1 word	R	DHCP Status 0x0000: Disabled 0x0001: Enabled
0x0051 (81)	2 words	R	IP Address of switch Ex: IP = 192.168.1.1 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x01 Word 1 Lo byte = 0x01
0x0053 (83)	2 words	R	Subnet Mask of switch Ex: IP = 255.255.255.0 Word 0 Hi byte = 0xFF Word 0 Lo byte = 0xFF Word 1 Hi byte = 0xFF Word 1 Lo byte = 0x00

0x0055 (85)	2 words	R	Gateway Address of switch Ex: IP = 192.168.1.254 Word 0 Hi byte = 0xC0 Word 0 Lo byte = 0xA8 Word 1 Hi byte = 0x01 Word 1 Lo byte = 0xFE
0x0057 (87)	2 words	R	DNS1 of switch Ex: IP = 168.95.1.1 Word 0 Hi byte = 0xA8 Word 0 Lo byte = 0x5F Word 1 Hi byte = 0x01 Word 1 Lo byte = 0x01
0x0059 (89)	2 words	R	DNS2 of switch Ex: IP = 168.95.1.1 Word 0 Hi byte = 0xA8 Word 0 Lo byte = 0x5F Word 1 Hi byte = 0x01 Word 1 Lo byte = 0x01
System Status Clear			
0x0100 (256)	1 word	W	Clear Port Statistics 0x0001: Do clear action
0x0101 (257)	1 word	W	Clear Relay Alarm 0x0001: Do clear action
Port Status			
0x1000 (4096)	5 words	R	Port Status 0x0000: Disabled 0x0001: Enabled Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status

0x1020 (4128)	5 words	R	Port Negotiation Status, force = 0x00 Status, auto = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1040 (4160)	5 words	R	Port Speed Status, 10M = 0x01 Status, 100M = 0x02 Status, 1000M = 0x03 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1060 (4192)	5 words	R	Port Duplex Status, half-duplex = 0x00 Status, full-duplex = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1080 (4224)	5 words	R	Port Flow Control Status, disabled = 0x00 Status, enabled = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status

0x10A0 (4256)	5 words	R	Port Link Status Status, down = 0x00 Status, up = 0x01 Word 0 Hi byte = Port 1 Status Word 0 Lo byte = Port 2 Status Word 1 Hi byte = Port 3 Status Word 1 Lo byte = Port 4 Status Word 2 Hi byte = Port 5 Status Word 2 Lo byte = Port 6 Status Word 3 Hi byte = Port 7 Status Word 3 Lo byte = Port 8 Status Word 4 Hi byte = Port 9 Status Word 4 Lo byte = Port 10 Status
0x1300 (4864)	40 words	R	Count of Good Packets of TX Ex. Port 1 gets 0x2EEEE1FFFF good packets of TX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets
0x1400 (5120)	40 words	R	Count of Bad Packets of TX Ex. Port 1 gets 0x2EEEE1FFFF bad packets of TX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets

0x1500 (5376)	40 words	R	Count of Good Packets of RX Ex. Port 1 gets 0x2EEEE1FFFF good packets of RX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets
0x1600 (5632)	40 words	R	Count of Bad Packets of RX Ex. Port 1 gets 0x2EEEE1FFFF bad packets of RX. Word 0 of Port 1 = 0x0000 Word 1 of Port 1 = 0x002E Word 2 of Port 1 = 0xEEE1 Word 3 of Port 1 = 0xFFFF Word 0,1,2,3 = Port 1 good packets Word 4,5,6,7 = Port 2 good packets Word 8,9,10,11 = Port 3 good packets Word 12,13,14,15 = Port 4 good packets Word 16,17,18,19 = Port 5 good packets Word 20,21,22,23 = Port 6 good packets Word 24,25,26,27 = Port 7 good packets Word 28,29,30,31 = Port 8 good packets Word 32,33,34,35 = Port 9 good packets Word 36,37,38,39 = Port 10 good packets

2.23 RedBox

A **RedBox** is a device designed to connect **PRP**, **HSR**, or single-threaded networks. **PRP** (**P**arallel **R**edudancy **P**rotocol) and **HSR** (**H**igh-availability **S**eamless **R**edundancy) are defined by International Electrotechnical Commission (IEC) in the 62439-3 standard, edition 4, 2021-12. A corrigendum (IEC 62439-3:2021/COR1:2023) was issued in 2023, primarily detailing the translation of supervision frames in HSR-PRP RedBoxes.
A RedBox can function in one of the following four modes:

- PRP-SAN
- HSR-SAN
- HSR-PRP
- HSR-HSR

The standard refers to several optional HSR sub-modes. However, Atop only supports **Mode H** and **Mode U**, which will be further explained in the subsequent HSR sections of this section.

1. PRP-SAN
PRP is designed to offer fail-safe redundancy in Ethernet networks, ensuring immediate recovery post any failures. Other redundancy protocols like STP, MRP, and ERPS require network reconfiguration (typically to unblock a blocked port) upon failure and recovery from failure before traffic flows again. Depending on protocol, recovery may take from a few milliseconds to several seconds.

PRP introduces redundancy at the node level by connecting two network interfaces (ports) to two separate and disjoint parallel networks, LAN A and LAN B. These two ports are referred to as **L**ink **R**edundancy **E**ntity (**LRE**) ports. The LRE port connected to LAN A is known as **Port A**, while the one connected to LAN B is termed **Port B**.

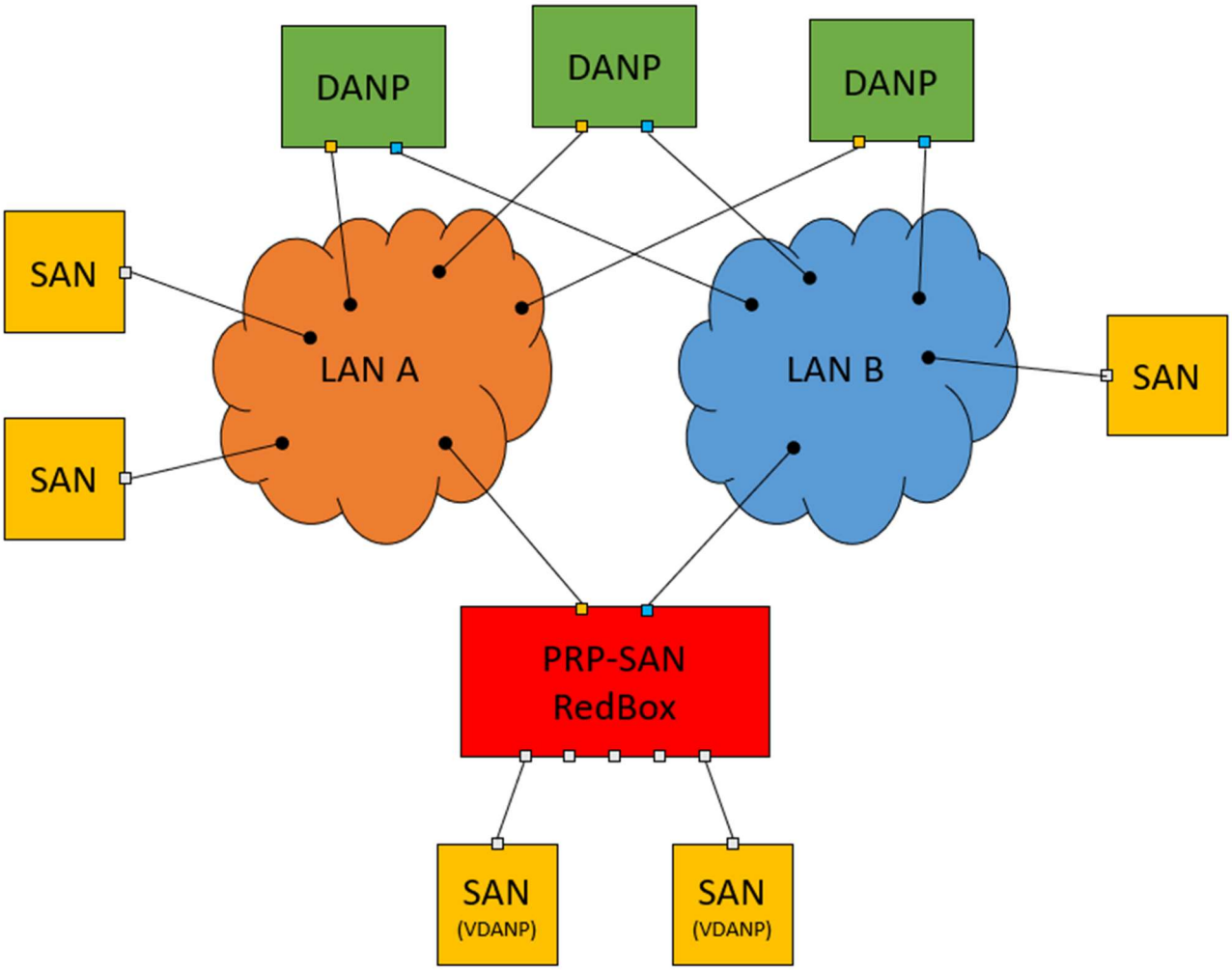


Figure 2.134 A PRP-SAN RedBox connected to a PRP network

Nodes that are connected to both LAN A and LAN B are termed **D**oubly **A**ttached **N**odes (**DANs**), and within a PRP network, these DANs are referred to as **DANPs**.

Singly **A**ttached **N**odes (**SANs**) are standard Ethernet devices with only one port connected to either LAN A or LAN B - or to the RedBox. When utilized as depicted in the Figure 2.134, the RedBox is configured as a RedBox in PRP-SAN mode.

A PRP-SAN RedBox is also a DANP that connects to both LAN A and LAN B. In addition to this, it has one or more ports - on its bridge-side - that are simple network ports that may connect other SANs to the PRP network. The interface that connects Port A and Port B with the bridge-side is referred to as the interlink port or Port C.
All DANPs and all RedBoxes in the network can communicate, and will not lose connection if either of their LRE ports goes down.

SANs connected directly to LAN A or LAN B can only communicate with other nodes connected to the respective LAN. SANs connected to the RedBox' bridge-side are known as **V**irtual **DANs** (**VDANs**) and in the PRP-case, they are called **VDANPs**. VDANPs can communicate with all SANs and all DANs in both LAN A and LAN B via the PRP-SAN RedBox.

A DANP sends the same frame simultaneously through its two LRE ports towards the destination node. A **R**edundancy **C**ontrol **T**railer (also known as **R**edundancy **C**heck **T**railer; **RCT**) containing a sequence number (**RCT.SeqNr**) is added to each frame copy to help the destination node distinguish between duplicate frames. The first error-free frame copy that arrives at the destination DANP node or destination PRP RedBox gets the RCT removed and the destination DANP node sends the frame to its higher layers. If the destination node is a RedBox, the frame is forwarded through the interlink port to the bridge-side of the RedBox.

A DANP does not forward frames between its two LRE ports. When or if the second copy arrives, it is detected as a duplicate and gets discarded, provided it arrives before a configurable duplicate discard timer times out.

A RedBox forwards frames with an RCT added on behalf of the connected VDANPs and keeps track of each VDANPs next RCT.SeqNr.

A SAN connected to LAN A or LAN B only receives one copy, and since a SAN is RCT unaware, it will forward the frame as is to its higher layers. This will not affect protocols running on the SAN, because most (if not all) protocols are designed to ignore frame data beyond the frame's payload.

A VDANP also only receives one frame copy, since the RedBox removes duplicates - and strips the RCT.

2. HSR-SAN

HSR is designed to function in a ring topology, ensuring zero recovery time. An HSR ring is composed of DANs each equipped with two ring ports, as depicted in Figure 2.135. These specific DANs are referred to as **DANHs**.

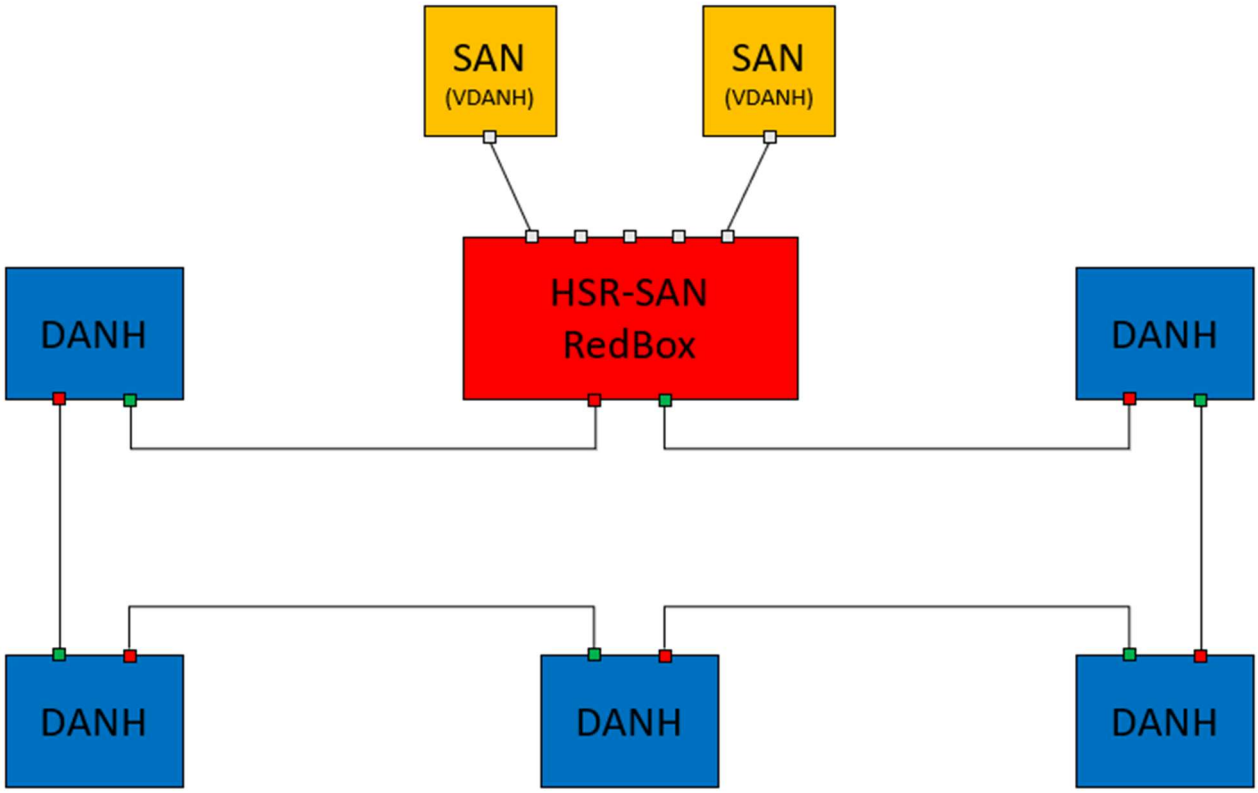


Figure 2.135 An HSR-SAN Redbox connected to an HSR ring

All devices within the HSR ring must be capable of processing an HSR tag on frames received from the ring and add the HSR tag to all frames sent to the ring. This implies that a SAN cannot be directly connected to the HSR ring. Instead, it must be connected through a RedBox on the RedBox's bridge-side. Such SANs are recognized as **V**irtual **DANHs** (**VDANHs**), as the RedBox is responsible for managing the pushing and popping of HSR tags on their behalf.

The **6-byte HSR tag**, which includes a sequence number (**HSR.SeqNr**), is inserted by DANHs and RedBoxes. Each RedBox maintains a sequence number for every attached VDANH.

A DANH simultaneously sends the same frame through both LRE ports, resulting in two frame copies circulating both clockwise and counter-clockwise in the ring.

A unicast frame, whose finaled destination is a node within the ring, travels in both directions around the ring until it reaches the destination node. The destination node forwards the first error-free frame copy to its higher layers or, in the case of a RedBox, to the bridge-side after removing the HSR tag. The frame is not forwarded to the other LRE port. If or when the second copy arrives, it is identified as a duplicate and discarded, provided it arrives before the configurable duplicate discard timer expires.

A unicast frame, whose finaled destination is not a node within the ring, is forwarded by every node in the ring until it reaches the originating node, where it is dropped.

A multicast or broadcast frame is forwarded by each node as there can be multiple consumers of this frame. Therefore, such frames always reach the originating node and are dropped.

3. HSR-PRP

The integration of HSR and PRP allows for the connection of a PRP network with an HSR ring. This specific topology necessitates the parallel use of two RedBoxes, as depicted in the Figure 2.136.

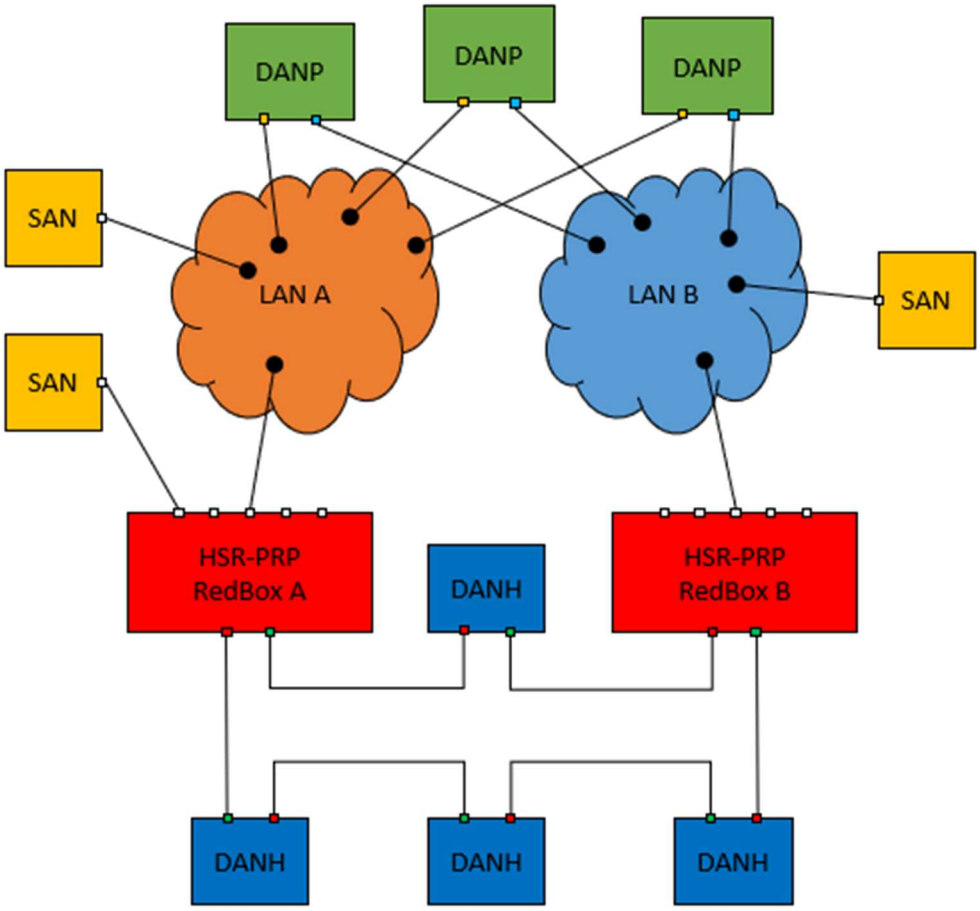


Figure 2.136 Two HSR-PRP RedBoxes interconnect a PRP network and an HSR ring

RedBox A connects to LAN A via a bridge-side port and to the HSR ring through its two LRE ports. Similarly, RedBox B connects to LAN B through a bridge-side port and to the HSR ring via its two LRE ports.

HSR-tagged traffic from the HSR ring, when forwarded to the interlink port, undergoes a transformation of the HSR tag to an RCT before it is injected towards the bridge-side of the RedBox.

In the same manner, **PRP-tagged** traffic from the PRP network, when forwarded through the interlink port towards the HSR ring, has the RCT transformed into an HSR tag with identical HSR.SeqNr.

If the traffic in the PRP network is not PRP-tagged (originating from a SAN), the RedBox maintains and inserts an HSR tag and sequence number on behalf of the SAN before forwarding it to the HSR ring.

To prevent traffic originating from the PRP network from being re-injected into the PRP network through the other RedBox, each HSR frame carries a **4-bit PathId** (**HSR.PathId**), which identifies the PRP network from which the frame originated.

The **PathId** is a concatenation of a **3-bit NetId** (**HSR.NetId**) and a **1-bit LanId** (**HSR.LanId**). The two RedBoxes connected to the same PRP network must be configured with the same NetId, a number ranging from 1 to 7. 0 is reserved and used by true DANHs and by RedBoxes in HSR-SAN mode.

The LanId identifies the RedBox (A or B) that injected the frame into the HSR ring. LanId 0 is used by RedBox A and LanId 1 is used by RedBox B. The LanId is included for supervision purposes on the HSR ring.

A RedBox in HSR-PRP mode does not forward a frame carrying its own HSR.NetId to it interlink. This process is referred to as NetId filtering.

An **RCT** also contains a PathId (**RCT.PathId**). Frames with an RCT on LAN A always carry LanId 0 and frames with an RCT on LAN B always carry LanId 1. As per the standard, the NetId is always 5 in PRP networks, so that the combined NetId and LanId in hexadecimal notation becomes 0xA (0b1010) for frames on LAN A and 0xB (0b1011) for frames on LAN B.

Frames from the HSR ring forwarded by the RedBox towards the interlink have the RCT inserted with a **LanID** corresponding to the configured LanId.

An HSR-PRP RedBox performs duplicate-discard on both the interlink and the LRE ports to prevent the same frame from being forwarded out the same RedBox port multiple times.

3.1. Connecting Multiple PRP Networks to a Single HSR Ring

Utilizing the RedBox types described above, a wide range of network topologies can be constructed. Figure 2.137 illustrates an example of connecting two PRP networks to a single HSR ring.

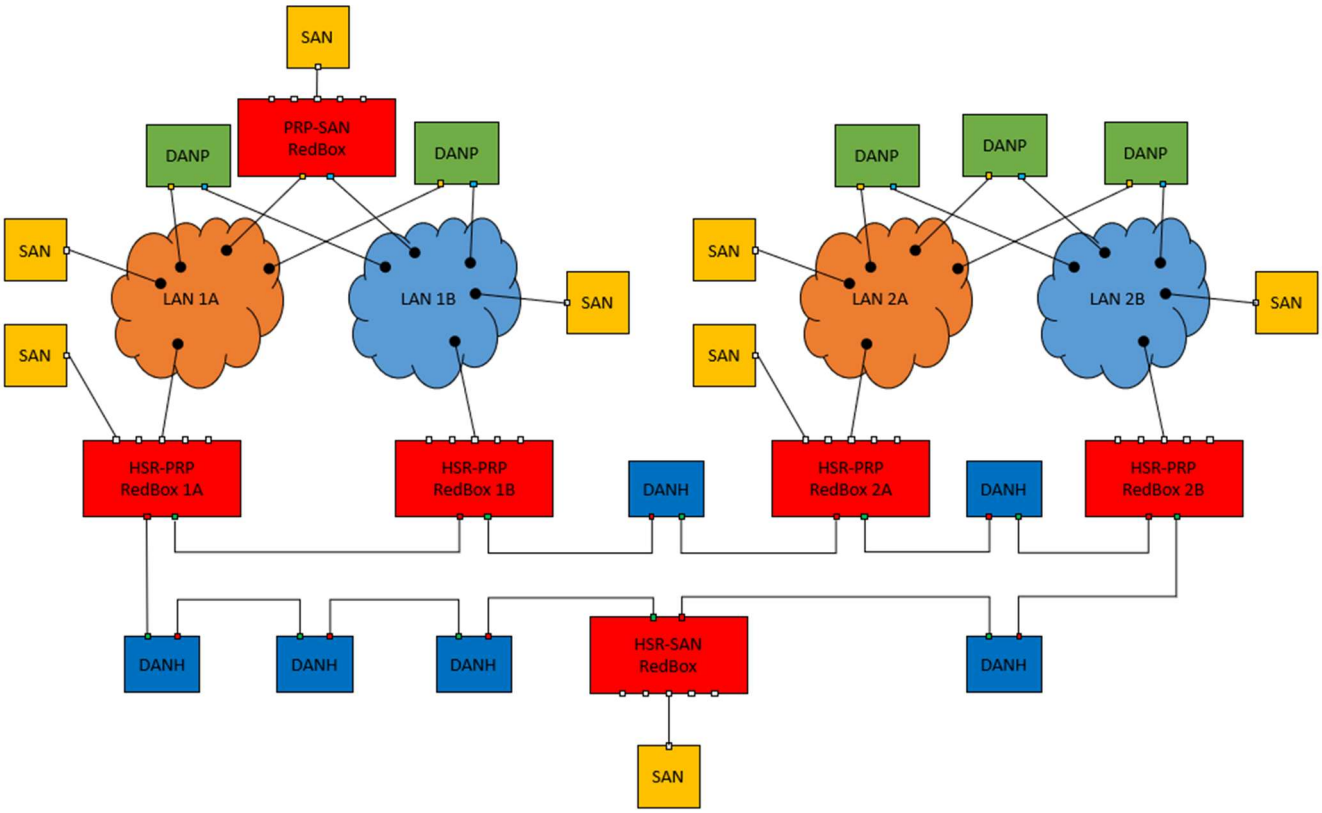


Figure 2.137 Multiple PRP networks connected to a single HSR ring

The 3-bit NetId facilitates the connection of up to seven distinct PRP networks to the same HSR ring. For illustrative purposes, two additional RedBoxes, one in PRP-SAN mode and another in HSR-SAN mode, are included in the diagram.

3.2. Connecting a PRP Network to Multiple HSR Rings

A PRP network can be connected to an unlimited number of HSR rings. However, these rings cannot be interconnected, neither by **QuadBoxes** (**HSR-HSR**) nor by another PRP network, as this would result in loops. All RedBoxes in the subsequent figure may utilize the same NetId.

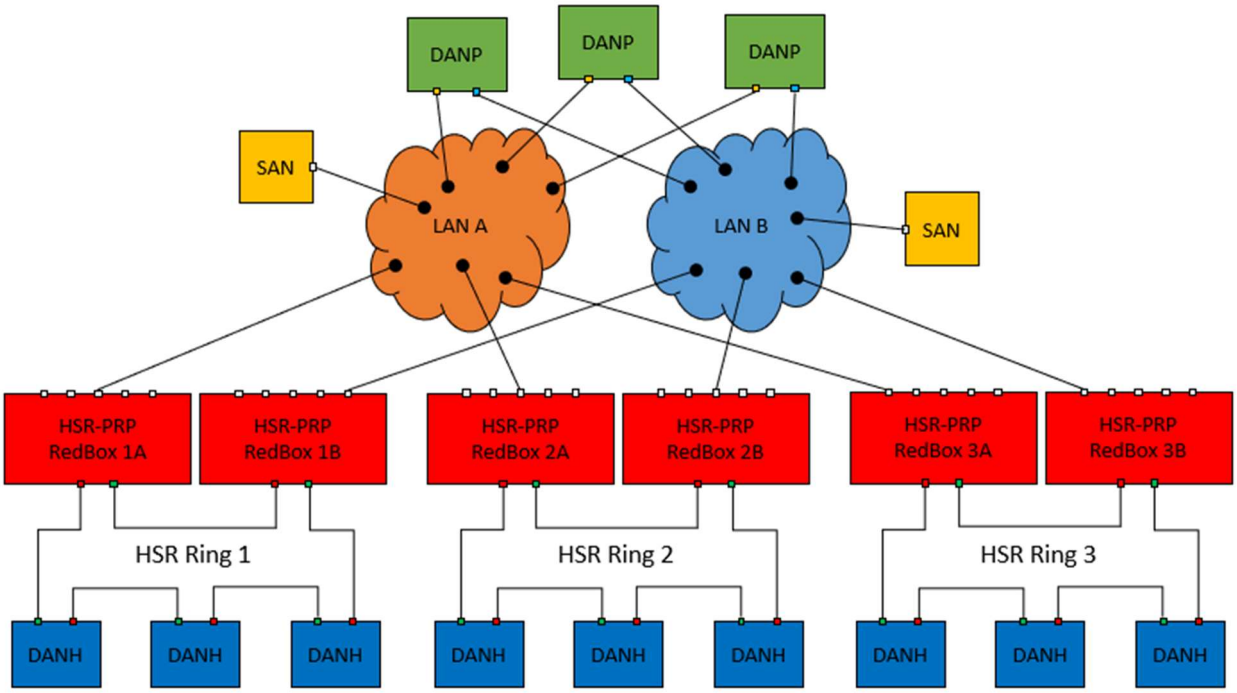


Figure 2.138 Single PRP network connected to multiple HSR rings

4. HSR-HSR

In **HSR-HSR** mode, traffic is HSR-tagged not only on the LRE ports but also on the interlink port.

Two RedBoxes in HSR-HSR mode can thus be connected back-to-back to form a socalled **QuadBox**, which is used to connect two separate HSR rings. In the following figure, two QuadBoxes operate in parallel to provide redundancy between the two HSR rings.

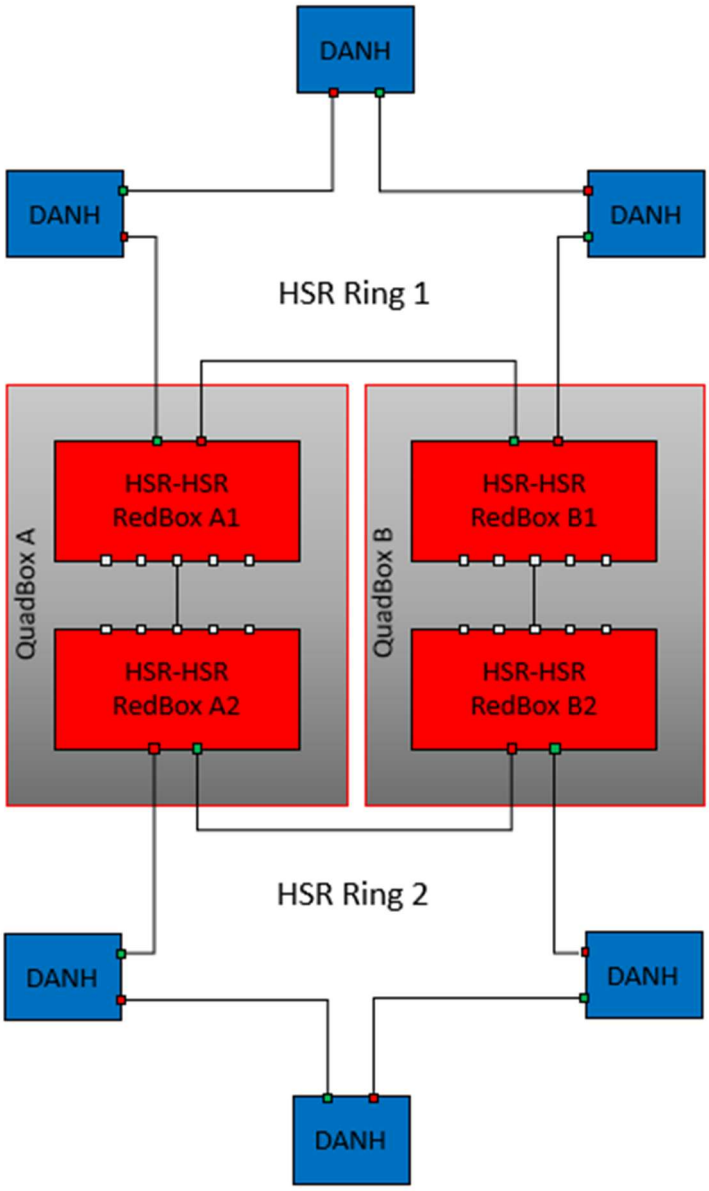


Figure 2.139 Connection of two HSR rings with two QuadBoxes

A QuadBox may or may not be located on the same physical device. The connection between the two RedBoxes forming a QuadBox is simply considered a "**wire**". If it is located on the same physical device, the two interlink ports should be the only ones in the same VLAN.

The QuadBoxes may or may not be configured with the same NetId (> 0). DANHs send with NetId 0, which is never NetId filtered by a RedBox. A frame sourced by a DANH in HSR Ring 1 and destined to a DANH in HSR ring 2 will therefore enter both RedBox A1 and B1 in two copies. Each of the RedBoxes will duplicate discard one of the copies, so that only one frame will be sent to the interlink of RedBox A2 and one to RedBox B2, both of which will generate two copies sent to HSR Ring 2.

Note that although the two RedBoxes have sent four copies of the frame to the HSR ring, each node on the ring will still only receive two copies, because the HSR-HSR RedBoxes perform duplicate discard also on their LRE ports, which prevents the same frame from being forwarded out the same LRE port multiple times. For example, the frame copy sent by RedBox A2 clockwise (through A2's Port B) will be filtered by RedBox B2 and not forwarded to RedBox B2's Port B if RedBox B2 has already sent this <SMAC, HSR.SeqNr> tuple towards its Port B.

Frame copies that travel the entire ring without being removed by a destination DANH are filtered by RedBox A2 and B2.

ProxyNode Table
The **ProxyNodeTable** tracks SMACs received in frames arriving on the interlink port from the bridge-side.

In addition to dynamically added entries, it contains two locked entries (only one in HSR-HSR mode):

- The RedBox' own MAC address. This is added as a DAN
- The bridge' s management MAC address. This is added as a SAN.

In HSR-HSR mode, the ProxyNodeTable is not populated with dynamic entries and the bridge's management MAC address is also not added.

In PRP-SAN and HSR-SAN mode, dynamically added entries are always marked as SANs.

In HSR-PRP mode, an entry is marked as a SAN by hardware. Software changes this to a DAN if a supervision frame mentioning the entry is received on the interlink from the PRP network side.

Once an entry is marked as a DAN (in HSR-PRP mode), frames from that SMAC must contain a valid RCT, and the LanId must match that of the RedBox, or the frame will be discarded.

A dynamic entry ages out after a certain amount of time of inactivity (the ProxyNodeTable age time) from that MAC address and - in HSR-PRP mode - if no supervision frames mentioning that SMAC have been received on the interlink port.

Besides the SAN/DAN flag, an entry in the ProxyNodeTable contains counters for the number of data frames it has received from a given node and the number of frames it has received with a wrong LanId (HSR-PRP mode, only), provided the entry is marked as a DAN, which it only can if a supervision frame mentioning it has arrived in the PRP network.

Supervision Frame Handling
Supervision frames are generated by DANs (hereunder RedBoxes) to notify other DANs connected to the PRP network or HSR ring about their or a VDAN's presence.

In HSR-SAN and HSR-HSR modes, supervision frames primarily serve informational purposes. However, in PRP-SAN and HSR-PRP modes, they play an active role in marking a specific node as a DAN in the NodesTable and ProxyNodeTable, respectively.

A supervision frame is a multicast frame transmitted to DMAC 01-15-4E-00-01-xx, where xx is configurable. The EtherType of supervision frame is 0x88FB.

Each supervision frame contains its own sequence number, which is incremented by one for each originated supervision frame. This sequence number is disregarded upon reception.

Supervision frames include one or two **T**ype/**L**ength **V**alues (**TLVs**), TLV1 and optionally a TLV2. Each TLV contains a MAC address and a TLV Type.

Supervision frames sent to a PRP network (PRP-SAN or HSR-PRP) have a TLV1 type of 20 or 21. A value of 20 is used when the DANP is in Duplicate Discard Mode and 21 is used when it is in Duplicate Accept mode. Duplicate Accept mode is not supported by the software, so only TLV1.Type == 20 is transmitted by RedBoxes. Supervision frames sent to an HSR ring (all HSR modes) have a TLV1 type of 23.

TLV2 is only used when the supervision frame is originated by a RedBox and it is not the RedBox' own supervision frame. In that case, TLV2's Type is 30 and TLV2's MAC address is the MAC address of the RedBox.

If TLV2 is not present, TLV1's MAC address is a DANP or a DANH. The RedBox itself transmits supervision frames without TLV2 only for its own MAC address.

If TLV2 is present, TLV1's MAC address is that of a VDAN.

In PRP-SAN, HSR-SAN, and HSR-PRP mode, the software regularly polls the ProxyNodeTable and originates proxied supervision frames at a configurable interval towards the LRE ports on behalf of the detected SANs (VDANs).

In HSR-PRP mode, supervision frames received from the PRP network will cause the software to stop sending proxied supervision frames on behalf of both TLV1.MAC and TLV2.MAC (if present), as they appear to send their own.

In HSR-PRP and HSR-HSR mode, the software also originates supervision frames towards the switch core, but only for the RedBox' own MAC address.

In HSR-PRP mode these supervision frames go to all ports that are members of the RedBox' supervision frame VLAN.

In HSR-HSR mode, the same applies, but the intention is that only the other RedBox in a QuadBox configuration should be member of that VLAN, and therefore only egress that other RedBox's LRE ports.

In PRP-SAN and HSR-SAN mode, any supervision frames received from the bridgeside are discarded by the RedBox at the interlink port, but it will be bridged normally in the SAN network.

In HSR-HSR mode, supervision frames not originated by the RedBox are hardware forwarded between interlink and LRE ports, that is, in both directions, as any other data frame.

The standard's corrigendum states that in HSR-PRP mode, the network operator may choose to let supervision frames received from the PRP network be forwarded as they are to the HSR ring and vice versa.

This may lead to problems if not all nodes on the HSR ring are PRP supervision frame aware (TLV1.Type is 20 or 21) or if not all DANs on the PRP network are HSR supervision frame aware.

Therefore, a PRP-to-HSR and an HSR-to-PRP configuration option allows for having the software forward supervision frames and changing TLV1.Type to the value expected within the HSR ring and PRP network, respectively. The corrigendum also states that if the original supervision frame did not include a TLV2, the RedBox must add a TLV2 with its own MAC and replace the supervision sequence number with the RedBox's own supervision sequence number. For better track of supervision frames' sequence numbers, the software does NOT use the RedBox' own supervision sequence number for software translated supervision frames but re-uses the one from the incoming packet. The supervision frame, however, always originated with the RedBox MAC as the frame's SMAC.

Whenever a supervision frame is received by the software it undergoes validation before it is actively used:

- DMAC must be 01-15-4e-00-01-xx, where xx is don't care
- TLV1 must be present and come first
- TLV1.Length must be correct
- TLV1.MAC must be a unicast MAC address
- TLV1.MAC must not be the RedBox's own MAC address
- TLV1.MAC must not be the device's management MAC address
- TLV1.Type must be any of the three valid types
- If TLV2 is present:
    - TLV2 must follow immediately after TLV1
    - TLV2.Length must be correct
    - TLV2.MAC must be a unicast MAC address
    - TLV2.MAC must not be the RedBox's own MAC address
    - TLV2.MAC must not be the device's management MAC address
    - TLV2.Type must be 30
- A null-TLV must follow immediately after TLV1 or TLV2 (if present)
- If received from PRP network:

  - RCT must be present
  - RCT.LanId must be correct
  - RCT.PRPSuffix must be 0x88FB
- If received from HSR ring:
  - HSR tag must be present
  - HSR.NetId must not be our own (HSR-PRP and HSR-HSR).

Any supervision frame that does not follow these rules is discarded by the software. Hardware-forwarding of supervision frames is based on the EtherType only, so in that case there is no guarantee that all these rules are obeyed.

Moreover, a valid supervision frame may be filtered and not used by the software because of one or more of the following reasons:

- The supervision frame was received on an LRE Port and
  - Port C is blocked for some reason or
  - Port C's VLAN ingress filtering is enabled, but Port C is not a member of the classified VLAN
- If TLV2.MAC is present and is either the RedBox' s own MAC address or the switch' s management MAC address or TLV2 is not present and TLV1.MAC is either of the two MAC addresses
- The supervision frame was received on a port in PRP mode but did not contain a valid RCT
- The supervision frame was received on a port in HSR mode but did not contain a valid HSR tag
- RedBox is in HSR-PRP mode and supervision frame received on LRE port and software HSR-to-PRP translation is enabled, but no ports in the PRP network are members of the classified VLAN.

Upon reception of a valid and non-filtered supervision frame on an LRE port, software adds both TLV1.MAC and TLV2.MAC (if present) to the NodesTable as DANs. It may happen that a supervision frame received from another RedBox mentions a TLV1.MAC not already in the NodesTable, because that MAC address is silent. In that case the entry will be created. For that reason, silent entries can be kept alive by the mere reception of supervision frames that "mentions" these entries. Moreover, if PRP-to- HSR or HSR-to-PRP supervision frame translation is active in some nodes in the PRP network or on the HSR ring, the frame's SMAC may not be the same as TLV2.MAC, so TLV2.MAC may also not pre-exist in the NodesTable.

Table 2.106 Descriptions of RedBox Configuration

Label	Description	Factory Default
Action	To create a given RedBox instance, press the Create button. Already created RedBox instances can be deleted with a click on the Delete button. Notice that the click itself doesn't change the underlying configuration. Only when the Save button is clicked, will the configuration take effect.	Null
Instance	Identifies the RedBox instance number.	Null
Enable	Enables or disables a given RedBox instance. If enabling, a click on the Save button causes software to perform additional checks before actually enabling the RedBox instance in hardware. If a check fails, the user will get notified. If disabling, the RedBox instance is removed entirely from hardware.	Disable
Mode	A RedBox may run in one of four different modes: • PRP-SAN	PRP-SAN

Label	Description	Factory Default
	• HSR-SAN • HSR-PRP • HSR-HSR In PRP-SAN mode, the two LRE ports (Port A and Port B) are connected to the PRP network's LAN A and LAN B, respectively. Port C corresponds to the remaining ports in the switch core and makes up the 'gateway' to the SAN network. Port C is also known as the interlink port. In HSR-SAN mode, the two LRE ports (Port A and Port B) connect to the HSR ring and the switch core (Port C) connects to the SAN network. In HSR-PRP mode, the two LRE ports connect to the HSR ring managed by this RedBox instance and Port C connects to a PRP network - either LAN A or LAN B. In HSR-HSR mode, the two LRE ports connect to the HSR ring managed by this RedBox instance and Port C connects to another RedBox' Port C. You may think of the connection between the two RedBoxes as a wire. The other RedBox may or may not be located on the same device as this RedBox.	
Port A	Select the physical interface that constitutes LRE Port A. A given physical port can serve only one specific RedBox instance. The drop-down box lists only those interfaces that the corresponding RedBox supports. It is possible to 'serialize' two or more RedBoxes by utilizing a special port called 'Neighbor'. With this interface, an internal connection is made to connect one RedBox to another, freeing up two physical ports on the device for other purposes. RedBox instance 1's Port A does not have a Neighbor option, because there is no RedBox 'to the left' of RedBox #1. Likewise, RedBox instance 5's Port B does not have a Neighbor option, because there is no RedBox 'to the right' of the last RedBox instance.	Null
Port B	Select the physical interface that constitutes LRE Port B. See description of Port A for details.	Null
Mode U	When checked, unicast frames with a DMAC in the ProxyNodeTable that arrive on an LRE port are - besides being forwarded to the interlink - also forwarded to the other LRE port. Not available in PRP-SAN mode.	Null

Label		Description	Factory Default
Net ID		The Net ID (called 'NetId' in IEC-62439-3) is a number between 1 and 7 and is used in HSR-PRP and HSR-HSR modes, only. The Net ID is along with the LAN ID ('LanId' in IEC-62439-3) used to form the 4-bit Path ID ('PathId' in IEC-62439-3), which is used in frames transmitted to the RedBox' HSR ring. In the other direction, it is used to prevent frames originated by this RedBox to return to the interlink and the PRP network (in HSR-PRP mode) or accompanying HSR RedBox (in HSR-HSR mode), by a method known as Net ID filtering: Frames arriving on the LRE ports carrying the same Net ID as the RedBox is configured with will be filtered towards Port C.	1
LAN ID		The LAN ID (called 'LanId' in IEC-62439-3) is used in HSR-PRP mode, only. It tells the RedBox whether the PRP-side of the RedBox is connected to LAN A or LAN B. In this way, the RedBox can convert the HSR tag in frames arriving on LRE ports to a correct RCT before it is sent to the PRP network.	A
Age Times	**NodesTable**	The NodesTable keeps track of source MAC addresses (SMACs) of frames received on LRE ports. In PRP-SAN mode, the NodesTable is used to identify a node either as a SAN or a DAN (DANP). The first time a given SMAC is seen on an LRE port, it is marked as a SAN, so the frames coming from the interlink and destined to that MAC address will be sent to one LRE port, only. If the same SMAC is seen on both Port A and Port B - or a supervision frame is received for that MAC address, the entry will be marked as a DAN, so that frames destined to that MAC address and coming from the interlink will have an RCT added and will be sent to both Port A and Port B. Frames arriving on LRE ports with same <SMAC, RCT.SeqNr> tuple are subject to duplicate discarding. In HSR modes (HSR-SAN, HSR-PRP, and HSR-HSR), the NodesTable serves a slightly different purpose. The first time a given SMAC is seen on an LRE port, that MAC address is added to the NodesTable as a DAN (SANs do not exist on HSR rings in Mode H). Frames destined to that MAC address coming from the interlink are always sent to both Port A and Port B with an HSR tag, and frames arriving on both	60

Label		Description	Factory Default
		Port A and Port B are subject to duplicate discarding based on the <SMAC, HSR.SeqNr> tuple. The NodesTable Age Time determines the number of seconds a given entry resides in the NodesTable after it was last seen on Port A or Port B. Valid range is 1-65 seconds with a default of 60 seconds	
	ProxyNodeTable	The ProxyNodeTable keeps track of source MAC addresses (SMACs) of frames received on the interlink port (Port C). In PRP-SAN and HSR-SAN mode, all nodes in the ProxyNodeTable are considered SANs, and frames coming from the LRE ports and leaving the interlink port will have the RCT (PRP-SAN) or HSR tag (HSR-SAN) removed. In HSR-PRP mode, a node in the ProxyNodeTable can either be a SAN or a DAN (DANP). A supervision frame sent by a DANP in the PRP network will cause the entry type to change from a SAN to a DAN. Once it is identified as a DAN, subsequent frames arriving from the DANP must carry an RCT. If not, those frames will be discarded by the RedBox and only forwarded in the PRP network. The ProxyNodeTable Age Time determines the number of seconds a given entry resides in the ProxyNodeTable after it was last seen on the interlink port. Valid range is 1 – 65 seconds with a default of 60 seconds.	60
	Duplicate Discard	The Duplicate Discard Age Time determines how long the RedBox shall wait for a copy of <SMAC, SeqNr> before the RedBox considers all copies received and forgets the entry. Valid range is 10 – 10000 milliseconds with a default of 40 milliseconds.	40
Supervision Frames	**VLAN ID**	The RedBox sends - towards the LRE ports - supervision frames on behalf of SANs connected to the switch core side of the RedBox in PRP-SAN, HSR-SAN, and HSR-PRP mode. This field chooses the VLAN ID with which these supervision frames are sent. If using the value 0, the RedBox sends with the interlink port's native VLAN ID (the Port VLAN ID). The RedBox software knows whether to tag the supervision frames based on the interlink port's tagging configuration. It	0

Label		Description	Factory Default
		also knows whether the interlink port is a member of the VLAN ID, and if not, it refrains from sending supervision frames. Notice: The RedBox hardware only supports recognizing HSR tags behind VLAN tags with a TPID of 0x8100 (C-tag), so if the interlink port is configured to VLAN tag with another TPID, the software sends with that TPID but receiving RedBoxes may not understand this as a VLAN tag, so it will not be able to find the HSR tag behind it, which may cause such frames to be discarded. This goes for all sorts of frames, not only supervision frames. Valid range is 0 - 4095 with a default of 0.	
	PCP	Whenever the RedBox software determines that frames should be transmitted VLAN tagged, it also inserts a PCP value into the VLAN tag. This value comes from this configuration. Notice, that even the native VLAN may have to be transmitted tagged, so the PCP value may also matter when the VLAN ID is set to 0. Valid range is 0 - 7 with a default of 7.	7
	DMAC LSByte	This field controls the value used in the least significant byte of the destination MAC address used in supervision frames sent by the RedBox, that is the 'xx' of 01:15:4E:00:01:xx. A network operator can identify certain parts of the network through the use of different values of this field. Upon reception of supervision frames, the RedBox ignores the LSbyte. Valid range is 0x00 - 0xFF with a default of 0x00.	0x00
	Interval	The interval with which supervision frames are sent by this RedBox. To avoid bursting of supervision frames, the first frame sent on behalf of a SAN is transmitted after a random number of milliseconds between 0 and this value. Subsequent supervision frames for a given SAN are transmitted this value seconds apart. Valid range is 1 – 60 seconds with a default of 2 seconds.	2
	PRP-to-HSR	This field is only used in HSR-PRP mode. When being checked, supervision frames from the PRP network are software forwarded as HSR supervision frames to the HSR ring. When unchecked, supervision frames from the PRP network are hardware forwarded	Checked

Label		Description	Factory Default
		without modifications to the HSR ring. Especially older HSR-capable equipment that only supports supervision frames of the HSR type require this option to be checked. Except for changing the supervision frame type from PRP-Duplicate-Discard or PRP-Duplicate-Accept to HSR when software forwarding, more checks are done on the supervision frame, such as checks for correct RCT, correct DMAC (except for least significant byte), correct TLV1.MAC, and correct TLV2.MAC. These checks cannot be performed when hardware forwarding the frames. Default is checked.	
	HSR-to-PRP	This field is only used in HSR-PRP mode. When being checked, supervision frames from the HSR ring are software forwarded as PRP-Duplicate-Discard supervision frames to the PRP network. When unchecked, supervision frames from the HSR ring are hardware forwarded without modifications to the PRP network. Especially older PRP-capable equipment that only supports supervision frames of the PRP type require this option to be checked. Except for changing the supervision frame type from HSR to PRP-Duplicate-Discard when software forwarding, more checks are done on the supervision frame, such as checks for correct HSR tag, correct DMAC (except for least significant byte), correct TLV1.MAC, and correct TLV2.MAC. These checks cannot be performed when hardware forwarding the frames. Default is checked.	Checked
Operational State		This shows the current operational state of a RedBox instance. A color indicates the state as follows: : The instance is not created or not enabled : The instance is enabled with no configurational warnings : The instance is enabled, but there are configurational warnings : The instance is enabled, but an internal error has occurred. See console or crashlog for details When yellow, hover the mouse over the image to see a list of configurational	

Label	Description	Factory Default
	warnings. The possible warnings are as follows: • The MTU is too high on at least one of the LRE ports (max is 2000) • The MTU is too high on at least one non-LRE port. Frames larger than 1994 cannot traverse the HSR/PRP network • Interlink port must use C-tags • Interlink port is not member of the supervision frame VLAN ID • The neighbor RedBox is not configured • The neighbor RedBox is not active • The neighbor's port A is not configured as a RedBox neighbor • The neighbor's port B is not configured as a RedBox neighbor • The neighbor's interlink port has coinciding VLAN memberships with this RedBox's interlink port • Interlink port has spanning tree enabled It is highly recommended to have a green color on enabled instances. It is important to notice that not all configuration errors can be detected by the RedBox software.	

Click **Save** button to save changes. Click **Reset** button to undo any changes made locally and revert to previously saved values. Click **Refresh** to refresh the page with current configuration and status. Local changes will be lost.

The following use simple test environment for drscribing how to set the configuration in PRP-SAN and HSR-SAN mode.

1. HSR-SAN

In this demonstration, two RHG9728 are used. The test environment is as Figure 2.140. Please refer to the following for setting RHG9728s.

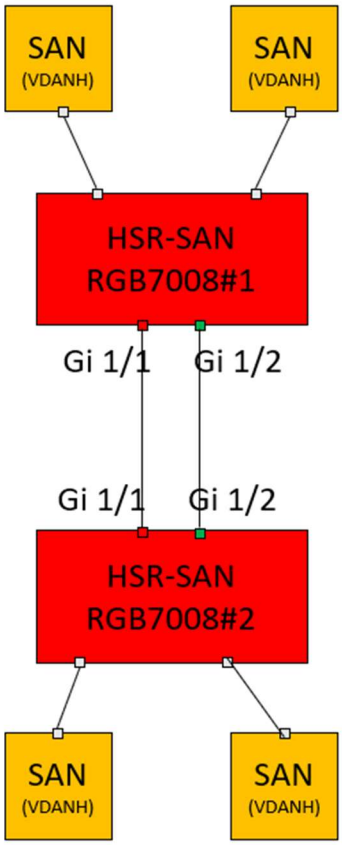


Figure 2.140 Demonstration of HSR-SAN

Step 1. Clock the **Create** of instance 1 as Figure 2.141.

RedBox Configuration

Refresh

Action	Instance	Enable	Mode	Port A	Port B	Mode U	Net ID	LAN ID	Age Times			Supervision Frames						Operational State
									NodesTable	ProxyNodeTable	Duplicate Discard	VLAN ID	PCP	DMAC LSByte	Interval	PRP-to-HSR	HSR-to-PRP	
Create	1		PRP-SAN				1	A	60	60	40	0	7	0x00	2			
Create	4		PRP-SAN				1	A	60	60	40	0	7	0x00	2			
Create	5		PRP-SAN				1	A	60	60	40	0	7	0x00	2			

Save Reset

Figure 2.141 Enable RedBox in HSR-SAN mode (Step 1)

Step 2. Click the **Enable** of instance 1 as Figure 2.142.

RedBox Configuration

Refresh

Action	Instance	Enable	Mode	Port A	Port B	Mode U	Net ID	LAN ID	Age Times			Supervision Frames						Operational State
									NodesTable	ProxyNodeTable	Duplicate Discard	VLAN ID	PCP	DMAC LSByte	Interval	PRP-to-HSR	HSR-to-PRP	
Delete	1	☑	PRP-SAN				1	A	60	60	40	0	7	0x00	2			
Create	4		PRP-SAN				1	A	60	60	40	0	7	0x00	2			
Create	5		PRP-SAN				1	A	60	60	40	0	7	0x00	2			

Save Reset

Figure 2.142 Enable RedBox in HSR-SAN mode (Step 2)

Step 3. Select the **Mode**, **Port A** and **Port B** of instance 1 as Figure 2.143. Mode is selected as PRP-SAN, Port A is selected as Gi 1/1 and Port B is Selected as Gi 1/2 in the demonstration.

RedBox Configuration

Refresh

Action	Instance	Enable	Mode	Port A	Port B	Mode U	Net ID	LAN ID	Age Times			Supervision Frames						Operational State
									NodesTable	ProxyNodeTable	Duplicate Discard	VLAN ID	PCP	DMAC LSByte	Interval	PRP-to-HSR	HSR-to-PRP	
Delete	1	☑	HSR-SAN	Gi 1/1	Gi 1/2	☐	1	A	60	60	40	0	7	0x00	2			
Create	4		PRP-SAN				1	A	60	60	40	0	7	0x00	2			
Create	5		PRP-SAN				1	A	60	60	40	0	7	0x00	2			

Save Reset

Figure 2.143 Enable RedBox in HSR-SAN mode (Step 3)

Step 4. Press **Save** button to save the configuration. The **Operational State** of instance 1 will become if the configuration is correct as Figure 2.144.

RedBox Configuration

Refresh

Action	Instance	Enable	Mode	Port A	Port B	Mode U	Net ID	LAN ID	Age Times			Supervision Frames				PRP-to-HSR	HSR-to-PRP	Operational State
									NodesTable	ProxyNodeTable	Duplicate Discard	VLAN ID	PCP	DMAC LSByte	Interval			
Delete	1	☑	HSR-SAN	Gi 1/1	Gi 1/2	☐	1	A	60	60	40	0	7	0x00	2	☑	☑	
Create	4	☐	PRP-SAN			☐	1	A	60	60	40	0	7	0x00	2	☑	☑	
Create	5	☐	PRP-SAN			☐	1	A	60	60	40	0	7	0x00	2	☑	☑	

Save Reset

Figure 2.144 Enable RedBox in HSR-SAN mode (Step 4)

After setting both RHG9728s' instance 1. The HSR-SAN environment is successfully established. Refer to Section 錯誤! 找不到參照來源。 and 錯誤! 找不到參照來源。 for knowing how to check the RedBox instance's status and statistics.

3 Monitor

The Atop's RHG9728 managed switch has an extensive set of status monitoring features on the WebUI. The user can select the submenus under the **Monitor** menu to check for the information or current status of the operations and protocols running on the Atop's RHG9728 managed switch. The following sections will describe each submenu under the **Monitor** menu.

3.1 System

3.1.1 Information

System information webpage shown in Figure 3.1 provides information of both hardware and software of the RHG9728 managed switch. Description of each field is explained in Table 3.1.

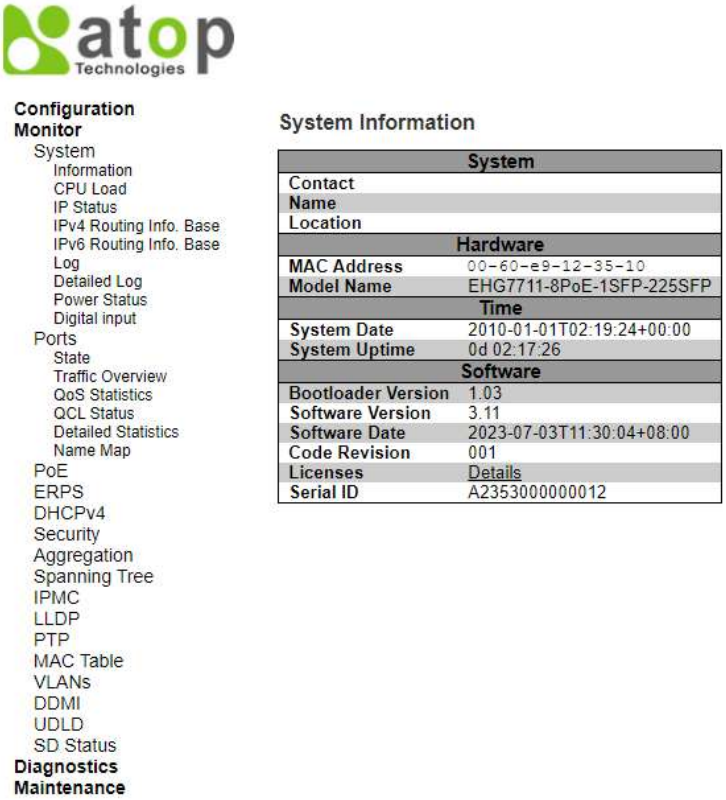


Figure 3.1 Webpage to Monitor System Information

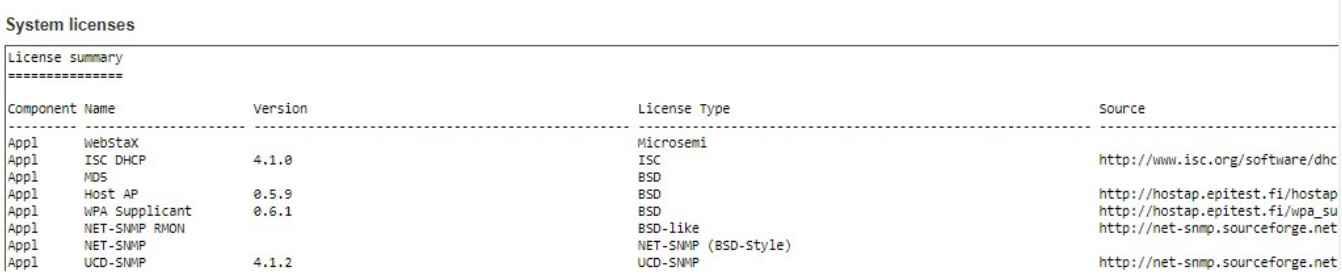
Table 3.1 Monitoring Descriptions of System Information

Label	Description	Factory Default
Contact	The system contact configured in Configuration | System | Information | System Contact.	Null
Name	The system name configured in Configuration | System | Information | System Name.	Null
Location	The system location configured in Configuration | System | Information | System Location.	Null
MAC Address	The MAC Address of this switch.	DUT's MAC address
Model Name	The Chip ID of this switch.	Ex: RHG9728-410SFP
System Date	The current (GMT) system time and date. The system time is obtained through the Timing server running on the switch, if any.	DUT's current time
System Uptime	The period of time the device has been operational.	DUT's bootup time

Label	Description	Factory Default
Bootloader Version	Version of firmware.	DUT's bootloader version
Software Version	The software version of this switch.	DUT's firmware version
Software Date	The date when the switch software was produced.	DUT's firmware builded time
Code Revision	The version control identifier of the switch software.	001
Licenses	Summary of the software license e.g., component, name, version, license type, and source.	

Check the **Auto-refresh** box to refresh the page automatically. The automatic refresh occurs every 3 seconds. Otherwise, click **Refresh** box to refresh the page immediately.

After Clicking Licenses, users will be directed to the summary of software license as shown in Figure 3.2.



System licenses

License summary
==========

Component	Name	Version	License Type	Source
Appl	WebStaX		Microsemi	
Appl	ISC DHCP	4.1.0	ISC	http://www.isc.org/software/dhc
Appl	MD5		BSD	
Appl	Host AP	0.5.9	BSD	http://hostap.epitest.fi/hostap
Appl	WPA Supplicant	0.6.1	BSD	http://hostap.epitest.fi/wpa_su
Appl	NET-SNMP RMON		BSD-like	http://net-snmp.sourceforge.net
Appl	NET-SNMP		NET-SNMP (BSD-Style)	
Appl	UCD-SNMP	4.1.2	UCD-SNMP	http://net-snmp.sourceforge.net

Figure 3.2 Summary of Software License

3.1.2 CPU Load

This page displays the CPU load, using an SVG graph. The load is measured as averaged over the last 100ms, 1sec and 10 seconds intervals. The last 120 samples are graphed, and the last numbers are displayed as text as well. In order to display the SVG graph, your browser must support the SVG format. Consult the SVG Wiki for more information on browser support. Specifically, at the time of writing, Microsoft Internet Explorer will need to have a plugin installed to support SVG.

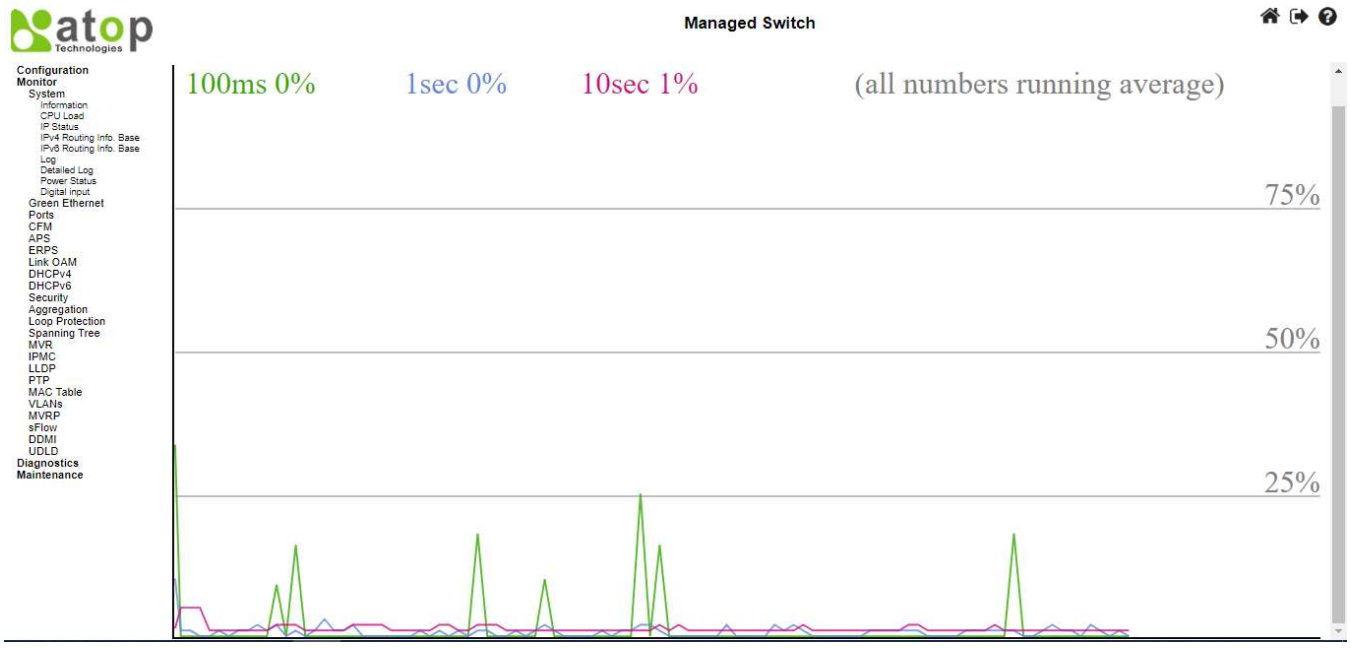


Figure 3.3 Webpage to Monitor System's CPU Load

Check the **Auto-refresh** box to refresh the page automatically. The automatic refresh occurs every 3 seconds.

3.1.3 IP Status

This page displays the status of the IP protocol layer. The status is defined by the IP interfaces, the IPv6 routes and the neighbour cache (ARP cache) status.

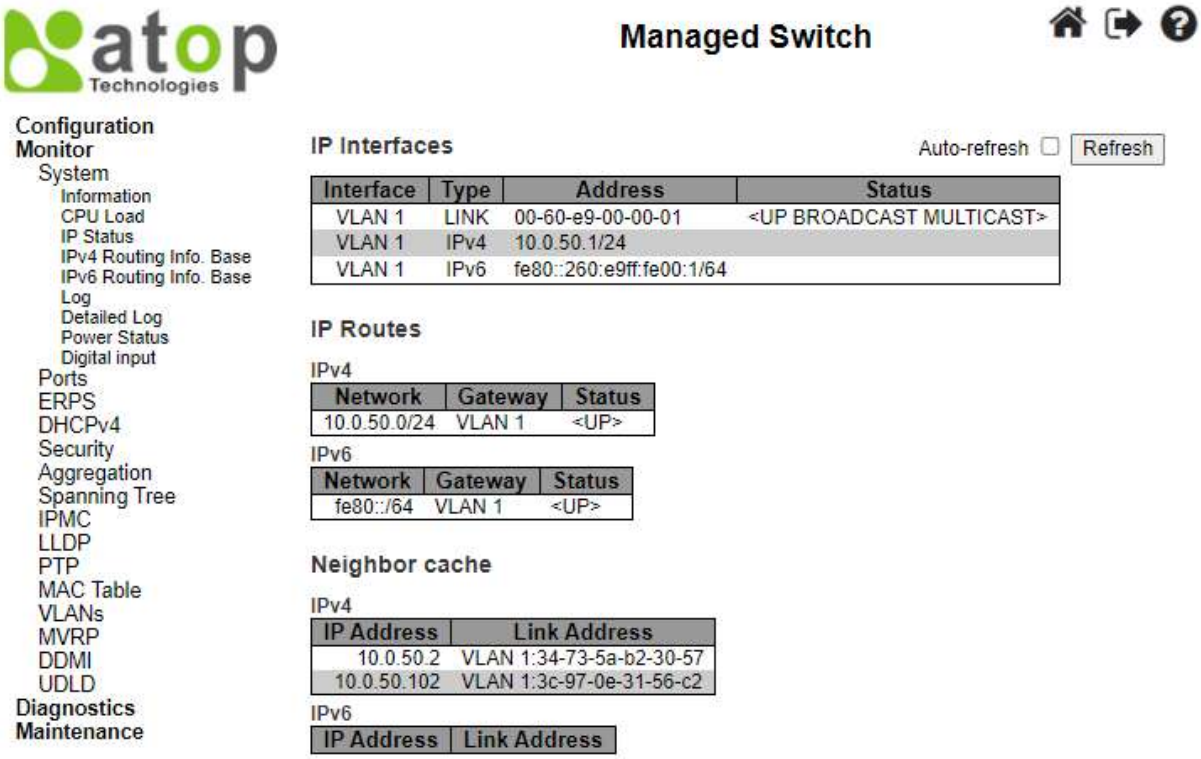


Figure 3.4 Webpage to Monitor System's IP Status

Table 3.2 Monitor Descriptions of System's IP Status

Label	Description	Factory Default
IP Interfaces		
Interface	The name of the interface.	VLAN 1
Type	The address type of the entry. This may be **LINK**, **IPv4** or **IPv6**.	LINK, IPv4, IPv6
Address	The current address of the interface (of the given type).	DUT's MAC address/ IPv4 address/ IPv6 address
Status	The status flags of the interface (and/or address).	<UP BROADCAST MULTICAST>
IP Routes		
Network	The destination IPv4/IPv6 network or host address of this route.	10.0.50.0/24, fe80::/64
Gateway	The gateway address of this route.	VLAN 1
Status	The status flags of the route.	<UP>
Neighbour cache		
IP Address	The IPv4/IPv6 address of the entry.	-
Link Address	The Link (MAC) address for which a binding to the IP address given exist.	-

Check the **Auto-refresh** box to refresh the page automatically. The automatic refresh occurs every 3 seconds.

3.1.4 IPv4 Routing Info. Base

This table in Figure 3.5 provides IPv4 routing status. Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the webpage will show the beginning entries of this table. The "Start from ID" input field allow the user to change the starting point in this table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next entry match. In addition, the input fields on the webpage will upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field. Table 3.3 summarizes the description of each label in Routing Information Base webpage.

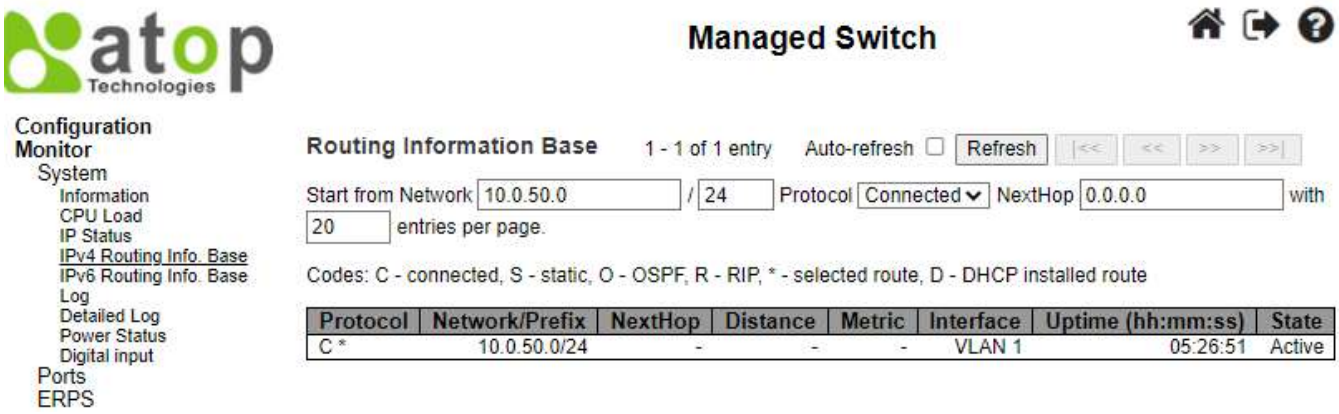


Figure 3.5 Webpage to Monitor System's IPv4 Routing Information Base

Table 3.3 Monitoring Descriptions of System's IPv4 Routing Information Base

Label	Description
Protocol	The protocol that installed this route. **DHCP**: The route is created by DHCP. **Connected**: The destination network is connected directly. **Static**: The route is created by user. **OSPF**: The route is created by OSPF.
Network/Prefix	Network and prefix (example 10.0.0.0/16) of the given route entry.
NextHop	Next-hop IP address. All-zeroes indicates the link is directly connected.
Interface	Next-hop interface.
Distance	Distance of the route.
Metric	Metric of the route.
Uptime (hh:ss:mm)	Time (in seconds) since this route was created
State	Destination is active.

Click **Refresh button** to refresh the page immediately. Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled. << : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled. >> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled. >>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

3.1.5 IPv6 Routing Info. Base

This table in Figure 3.6 provides IPv6 routing status. Each page shows up to 999 table entries, selected through the "entries per page" input field. When first visited, the web page will show the beginning entries of this table. The "Start from ID" input field allow the user to change the starting point in this table. Clicking the **Refresh button** will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a **Refresh button** click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field. Table 3.4 summarizes the description of each label in Routing Information Base webpage.

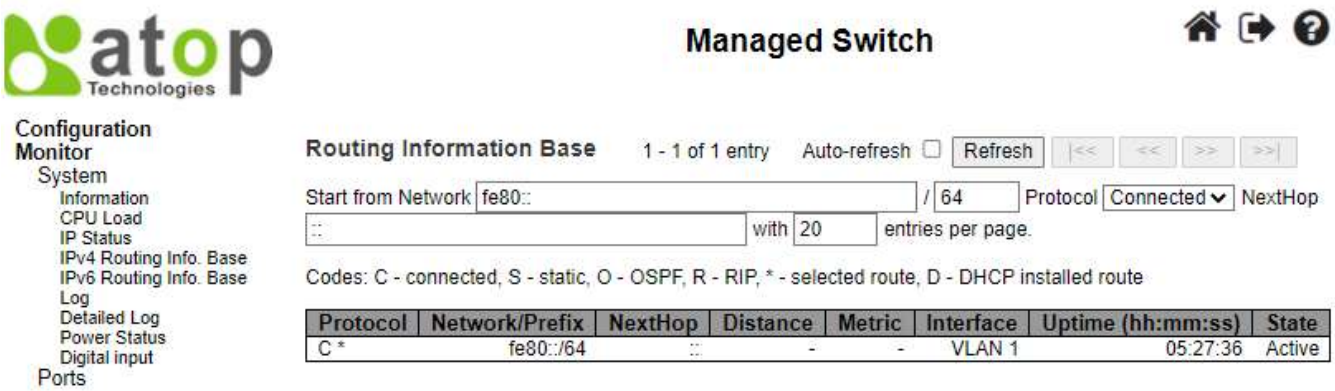


Figure 3.6 Webpage to Monitor System's IPv6 Routing Information Base

Table 3.4 Monitoring Descriptions of System's IPv6 Routing Information Base

Label	Description
Protocol	The protocol that installed this route. **DHCP**: The route is created by DHCP. **Connected**: The destination network is connected directly. **Static**: The route is created by user. **OSPF**: The route is created by OSPF. **RIP**: The route is created by RIP.
Network/Prefix	Network and prefix (example 10.0.0.0/16) of the given route entry.
NextHop	Next-hop IP address. All-zeroes indicates the link is directly connected.
Distance	Distance of the route.
Metric	Metric of the route.
Interface	If the next-hop address is a link-local address, then this is the VLAN interface of the link-local address. Otherwise, this value is not used
Uptime (hh:ss:mm)	Time (in seconds) since this route was created
State	Destination is active.

Click **Refresh button** to refresh the page immediately. Auto-refresh ☐ : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. |<< : Updates the table entries, starting from the first available entry. If the first entry of the table is displayed, the button is disabled. << : Updates the table entries, ending at the entry prior to the first entry currently displayed. If the first entry of the table is displayed, the button is disabled. >> : Updates the table entries, starting from the entry next to the last entry currently displayed. If the last entry of the table is displayed, the button is disabled. >>| : Updates the table entries, ending at the last available entry. If the last entry of the table is displayed, the button is disabled.

3.1.6 Log

The managed switch's system log information is provided in this **Log** webpage shown in Figure 3.7. Each page can display up to 999 table entries which can be selected through the "**entries per page**" input field. When first visited, the web page will show the beginning entries of this table. The "**Level**" input field is used to filter the display system log entries. The "**Clear Level**" input field is used to specify which system log entries will be cleared. To clear specific system log entries, select the clear level first then click the **Clear** button.

The "**Start from ID**" input field allows the user to change the starting point in this table. Clicking **the Refresh** button will update the displayed table starting from that or the closest next entry match. In addition, these input fields will upon a **Refresh** button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start input field.

The [>>] will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the [>>|] button to start over.

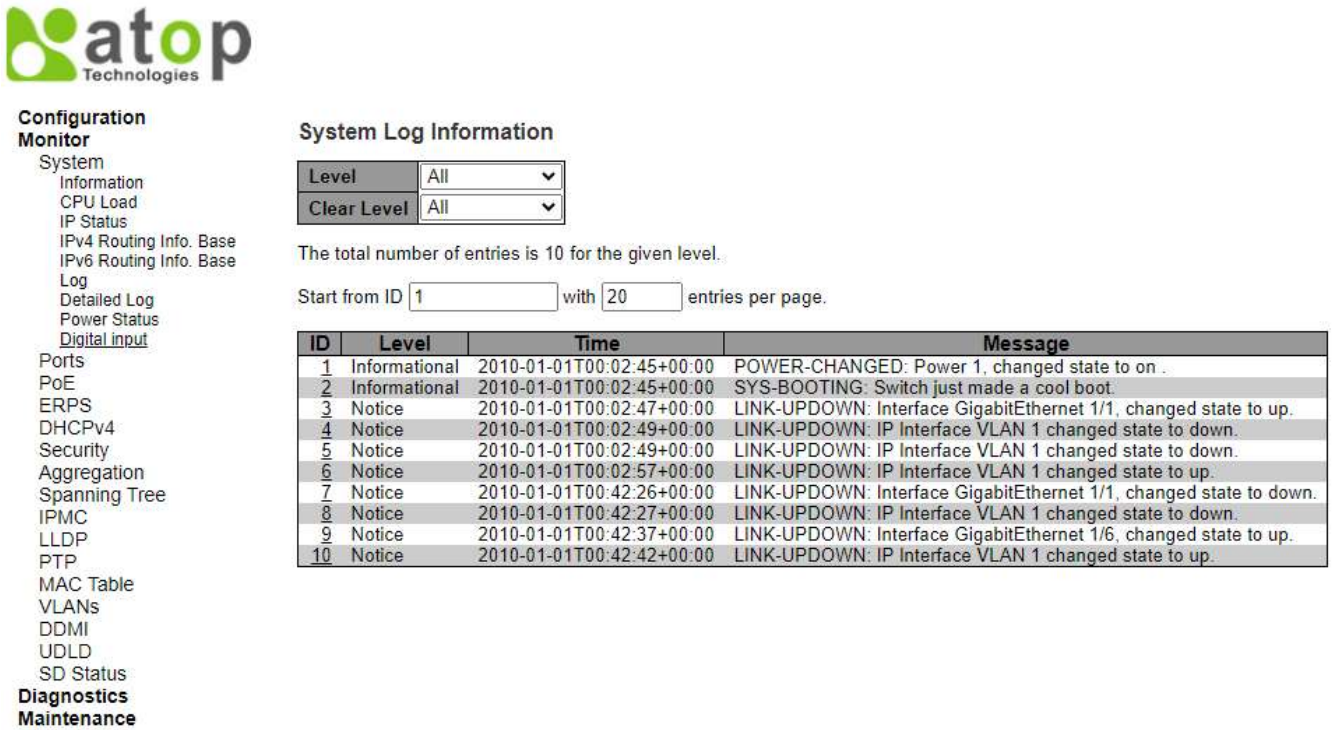


Figure 3.7 Webpage to Monitor System Log

Table 3.5 Monitoring Descriptions of System Log

Label	Description
ID	The identification of the system log entry.
Level	The level of the system log entry. **Informational**: The system log entry is belonged information level. **Warning**: The system log entry is belonged warning level. **Error**: The system log entry is belonged error level.
Time	The occurred time of the system log entry.
Message	The detail message of the system log entry.

3.1.7 Detailed Log

The managed switch system detailed log information is provided in this webpage shown in Figure 3.8. Table 3.6 provides descriptions for the Detailed System Log Information.

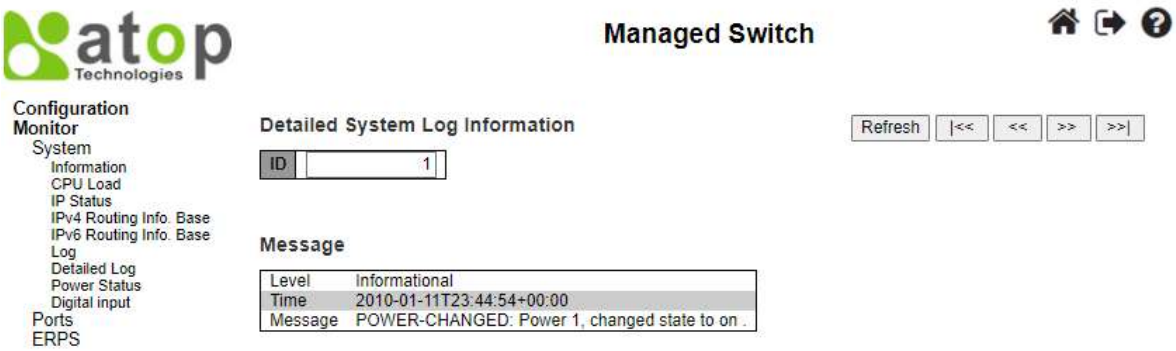


Figure 3.8 Webpage to Monitor System Detailed Log

Table 3.6 Monitoring Descriptions of System Detailed Log

Label	Description
Level	The severity level of the system log entry. **Informational**: The system log entry is belonged information level. **Warning**: The system log entry is belonged warning level. **Error**: The system log entry is belonged error level.
ID	The ID (>= 1) of the system log entry.
Message	The detail message of the system log entry.

3.1.8 Power Status

This webpage in Figure 3.9 shows **Power Status** of the device. There are two or three powers: Power1, Power 2, and Power3, and the power state can be either On and Off. Some models support two powers, and some models support three powers.

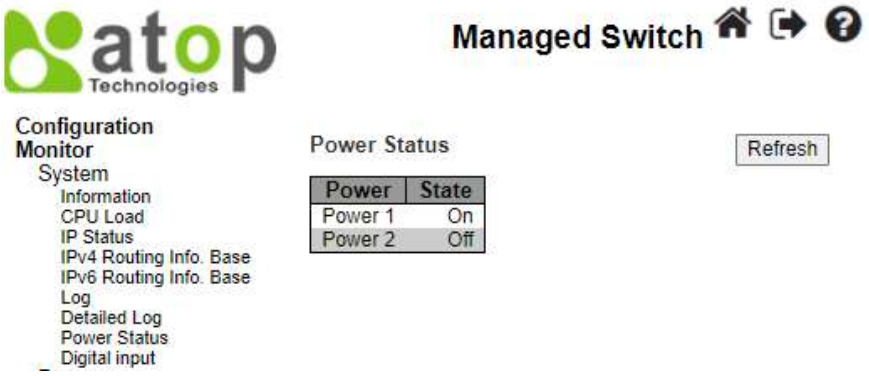


Figure 3.9 Webpage to Monitor System's Power Status

3.1.9 Digital Input

Status of Digital Input (DI) can be checked on this webpage shown in Figure 3.10. When it is "ON", the device detects the signal from DI port. When it is "OFF", the device will not detect the signal from DI port.

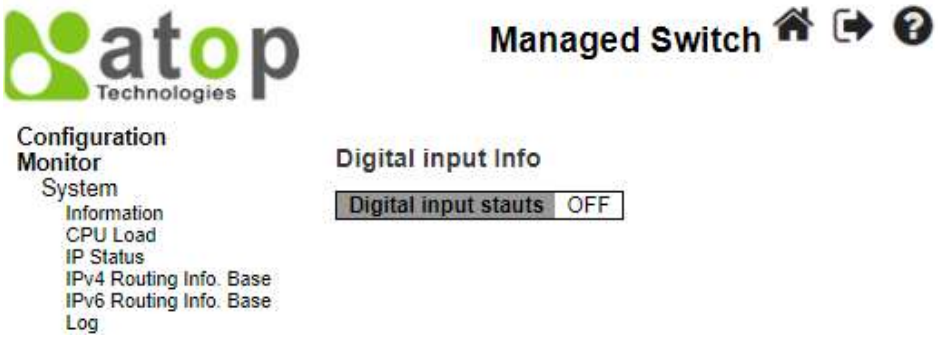


Figure 3.10 Webpage to Monitor System's Digital Input

3.2 Ports

3.2.1 State

This State webpage shown in Figure 3.11 provides an overview of the current switch port states. The port states are typically illustrated as follows:

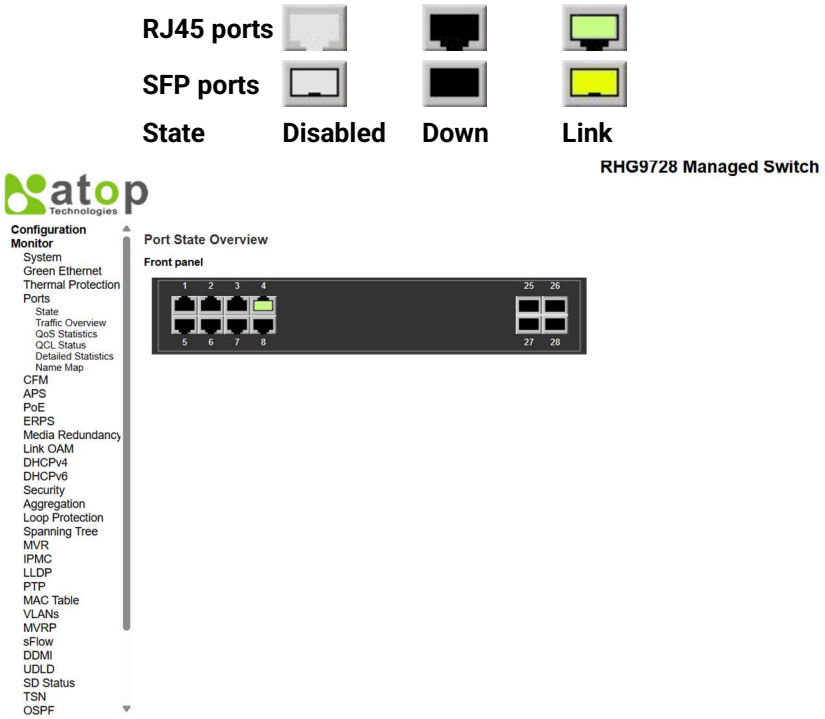
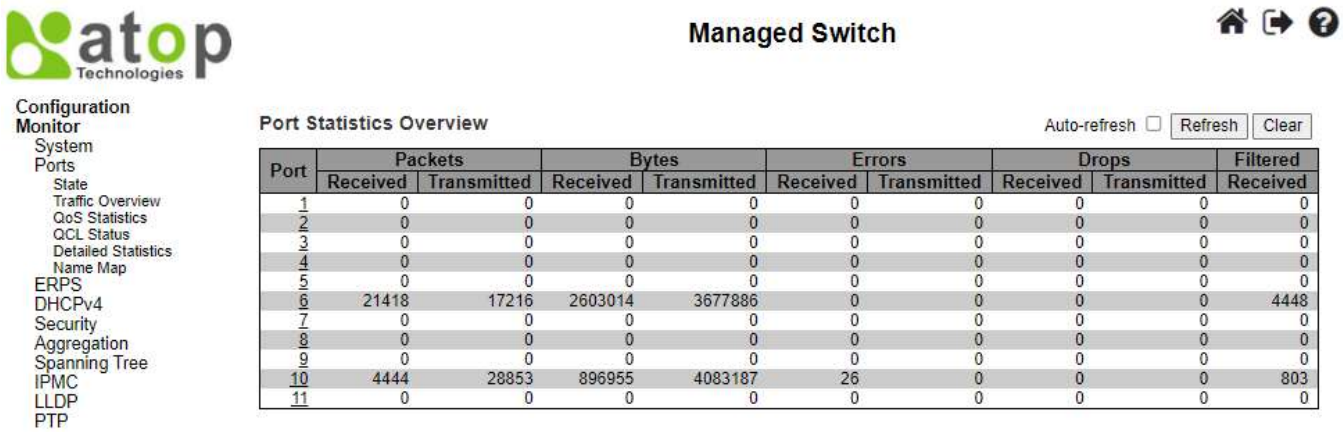


Figure 3.11 Webpage of RHG9728 to Monitor Port State

Check the **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh** button to refresh the page immediately.

3.2.2 Traffic Overview

This Traffic Overview webpage provides an overview of general traffic statistics for all ports of managed switch as shown in Figure 3.12. Table 3.7 describes column labels for the Port Statics Overview.



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	21418	17216	2603014	3677886	0	0	0	0	4448
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	4444	28853	896955	4083187	26	0	0	0	803
11	0	0	0	0	0	0	0	0	0

Figure 3.12 Webpage to Monitor Traffic Overview of Ports

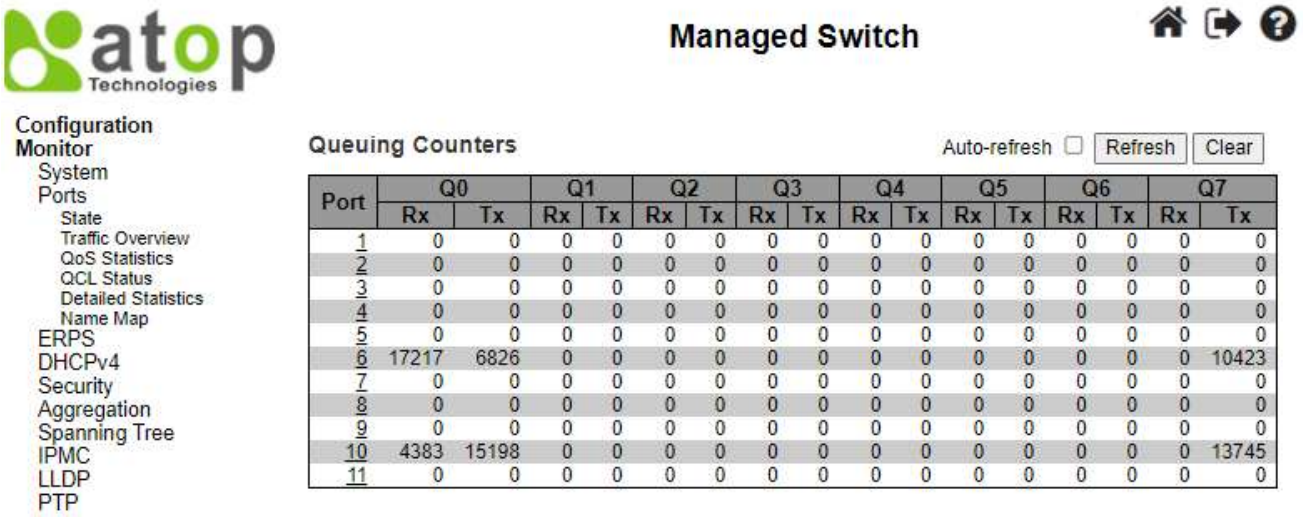
Table 3.7 Monitoring Descriptions of Traffic Overview of Ports

Label	Description	Factory Default
Port	The logical port for the settings contained in the same row.	Port Number
Packets	The number of received and transmitted packets per port.	0
Bytes	The number of received and transmitted bytes per port.	0
Errors	The number of frames received in error and the number of incomplete transmissions per port.	0
Drops	The number of frames discarded due to ingress or egress congestion.	0
Filtered	The number of received frames filtered by the forwarding process.	0

Check the **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.2.3 QoS Statistics

QoS Statistics webpage in Figure 3.13 provides statistics for different queues on all managed switch's ports. The labels of the Queueing Counters are described in Table 3.8.



Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	17217	6826	0	0	0	0	0	0	0	0	0	0	0	0	0	10423
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	4383	15198	0	0	0	0	0	0	0	0	0	0	0	0	0	13745
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 3.13 Webpage to Monitor Queuing Counters

Table 3.8 Monitoring Descriptions of Queuing Counters

Label	Description
Port	The logical port for the settings contained in the same row.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority queue.
Rx/Tx	The number of received and transmitted packets per queue.

Check the **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Clear button** to clears the counters for all ports. Click **Refresh button** to refresh the page immediately.

3.2.4 QCL Status

This webpage in Figure 3.14 shows the QoS Control List (QCL) status by different QCL users. Each row describes the QoS Control Entry (QCE) that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch. Table 3.9 summarizes the descriptions of the labels in the QoS Control List Status.

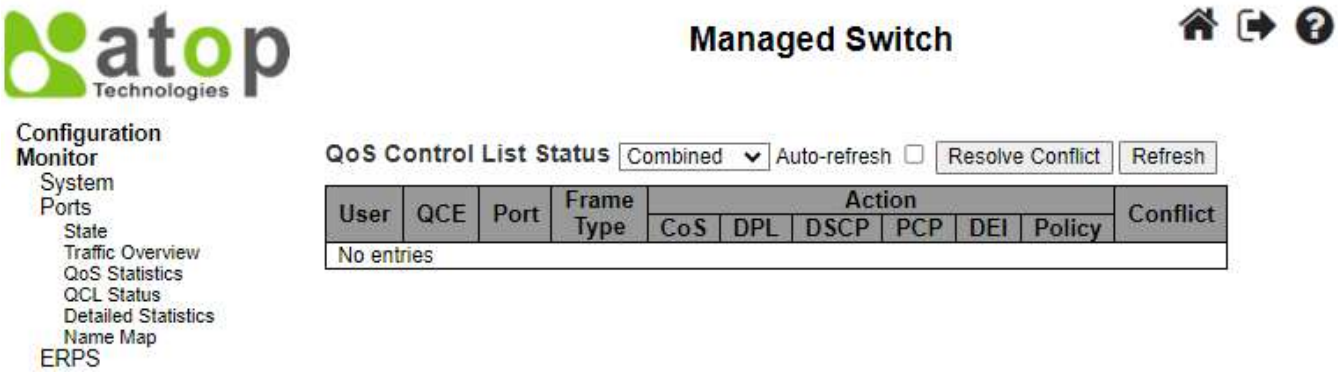


Figure 3.14 Webpage to Monitor QoS Control List Status

Table 3.9 Monitoring Descriptions of QoS Control List Status

Label	Description
User	Indicates the QCL user.
QCE	Indicates the QCE id.
Port	Indicates the list of ports configured with the QCE.
Frame Type	Indicates the type of frame. Possible values are: **Any:** Match any frame type. **Ethernet**: Match EtherType frames. **LLC**: Match (LLC) frames. **SNAP**: Match (SNAP) frames. **IPv4**: Match IPv4 frames. **IPv6**: Match IPv6 frames.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. Possible actions are: **CoS:** Classify Class of Service. **DPL:** Classify Drop Precedence Level. **DSCP:** Classify DSCP value. **PCP:** Classify PCP value. **DEI:** Classify DEI value. **Policy:** Classify ACL Policy number.
Conflict	Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button.

Select the QCL status from this **Combined** drop-down list. Check the **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Resolve Conflict button** to release the resources required to add QCL entry, in case the conflict status for any QCL entry is 'yes'. Click **Clear button** to clear the counters for all ports. Click **Refresh button** to refresh the page immediately

3.2.5 Detailed Statistics

This webpage in Figure 3.15 provides detailed traffic statistics for a specific switch port. The user can use the port select box to select which switch port details to display. The displayed counters are the totals for receive and transmit, the size counters for receive and transmit, and the error counters for receive and transmit. Descriptions of statistics labels are summarized in Table 3.10.

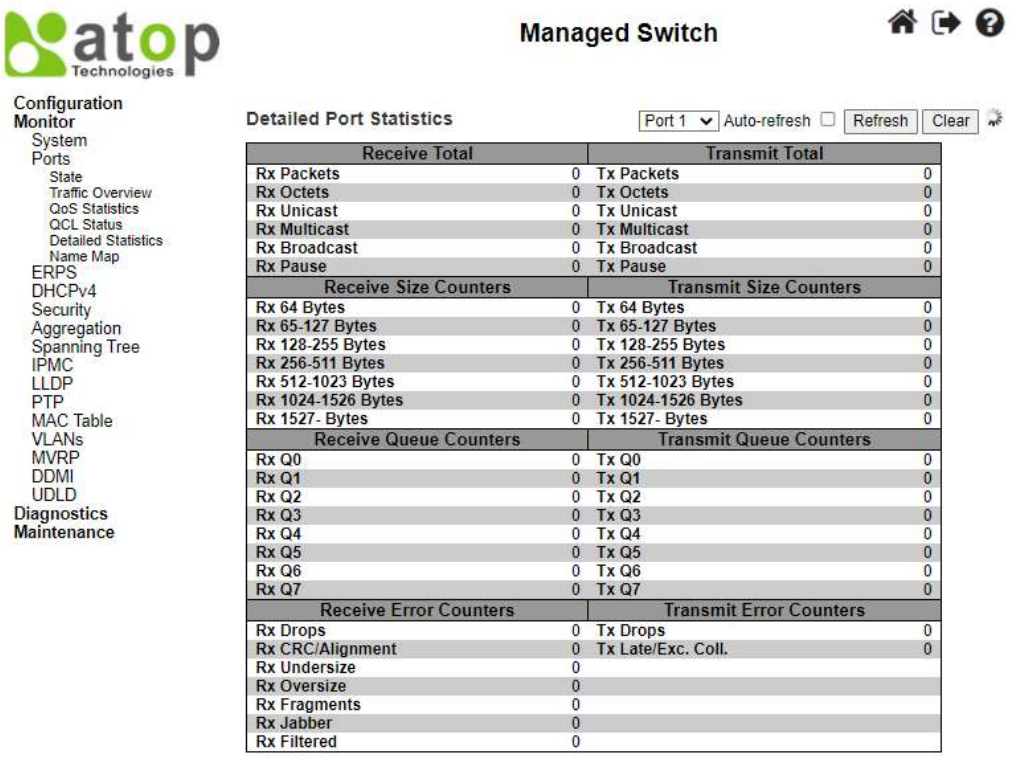


Figure 3.15 Webpage to Monitor Detailed Port Statistics

Table 3.10 Monitoring Descriptions of Detailed Port Statistics

Label	Description
Receive Total and Transmit Total	
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Receive and Transmit Size Counters	
The number of received and transmitted (good and bad) multicast packets.	
Receive and Transmit Queue Counters	
The number of received and transmitted (good and bad) broadcast packets.	
Receive Error Counters	
Rx Drops	The number of frames dropped due to lack of receive buffers or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short frames received with valid CRC. Short frames are frames that are smaller than 64 bytes.
Rx Oversize	The number of long frames received with valid CRC. Long frames are frames that are longer than the configured maximum frame length for this port.

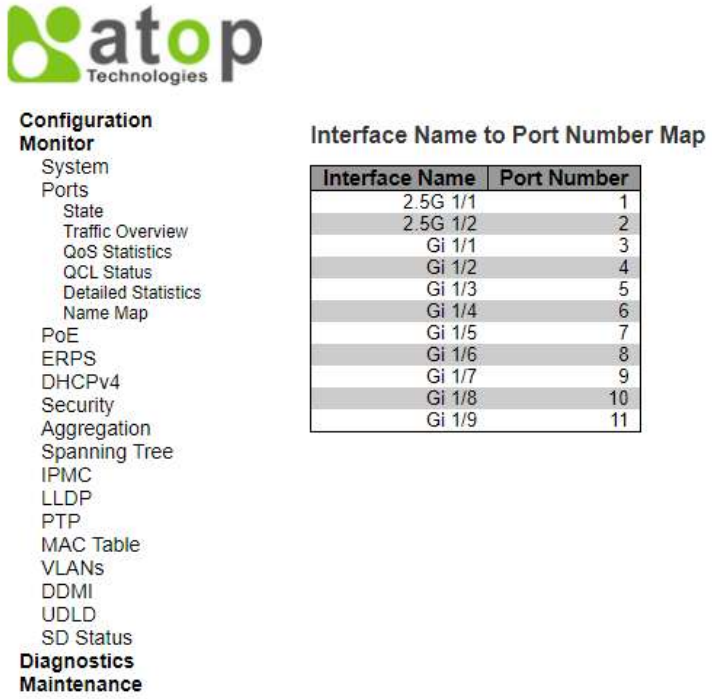
Label	Description
Receive Total and Transmit Total	
Rx Fragments	The number of short frames received with invalid CRC. Short frames are frames that are smaller than 64 bytes.
Rx Jabber	The number of long frames received with invalid CRC. Long frames are frames that are longer than the configured maximum frame length for this port.
Rx Filtered	The number of received frames filtered by the forwarding process.
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late/Exc. Coll.	The number of frames dropped due to excessive or late collisions.

The port select box determines which port is affected by clicking the buttons.

Check the **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Clear button** to clear the counters for all ports. Click **Refresh button** to refresh the page immediately

3.2.6 Name Map

This webpage provides interface name to port number mapping. Many Web pages use a port number to express an interface, whereas Command Line Interface (CLI) uses interface names. The table shown in Figure 3.16 provides a means to convert from one to the other.



Interface Name	Port Number
2.5G 1/1	1
2.5G 1/2	2
Gi 1/1	3
Gi 1/2	4
Gi 1/3	5
Gi 1/4	6
Gi 1/5	7
Gi 1/6	8
Gi 1/7	9
Gi 1/8	10
Gi 1/9	11

Figure 3.16 Webpage to Name Map

3.3 ERPS

ERPS is an abbreviation for Ethernet Ring Protection Switching defined in ITU/T G.8032. It provides fast protection and recovery switching for Ethernet traffic in a ring topology while also ensuring that the Ethernet layer remains loop-free. This ERPS webpage reports the current status of ERPS instances on the managed switch as shown in Figure 3.17.

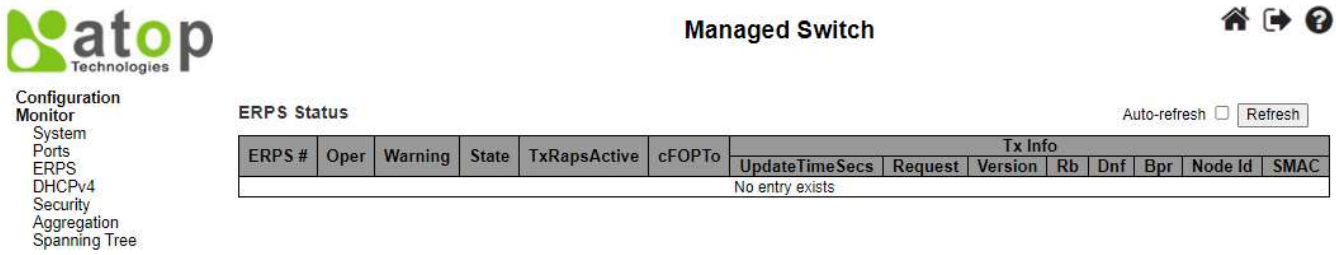


Figure 3.17 Webpage to ERPS Status

Table 3.11 Description of ERPS Status

Label	Description
ERPS	The ID of the ERPS. Click on link to get to ERPS instance page, you can reset counters and issue commands.
Oper	The operational state of ERPS instance. ●: Active. ●: Disabled or Internal error.
Warning	Operational warnings of ERPS instance. ●: No warnings. ●: There are warnings, use tooltip to see.
State	Specifies protection/node state of ERPS.
TxRapsActive	Specifies whether we are currently supposed to be transmitting R-APS PDUs on our ring ports.
cFOPTo	Failure of Protocol - R-APS Rx Time Out.
Tx Info	
UpdateTimeSecs	Time in seconds since boot that this structure was last updated.
Request	Request/state according to G.8032, table 10-3.
Version	Version of received/used R-APS Protocol. 0 means v1, 1 means v2, etc.
Rb	RB (RPL blocked) bit of R-APS info. See Figure 10-3 of G.8032.
Dnf	DNF (Do Not Flush) bit of R-APS info. See Figure 10-3 of G.8032."
Bpr	BPR (Blocked Port Reference) of R-APS info. See Figure 10-3 of G.8032.
Node Id	Node ID of this request.
SMAC	The Source MAC address used in the request/state.

Figure 3.18 shows detailed status of the EPRS where the parameters and commands are described in Table 3.12

ERPS Status

Configuration

ERPS #	Ver	Type	VC	Prop	Port0	Port1	Ring Id	Node Id	Level	VLAN	PCP	Rev	Guard	WTR	HoldOff	Enable
1	v1	Major	✗	✗	4	5	1	00:00:00:00:00:00	7	7	7	✓	500	5	0	✓

Status

Oper	Warning	State	TxRapsActive	cFOPTo	Tx Info							
					UpdateTimeSecs	Request	Version	Rb	Dnf	Bpr	Node Id	SMAC
●	●	Idle	✓	✗	28954	No Request	0	✗	✗	RingPort1	00:01:C1:00:C9:99	00:00:00:00:00:00

Status Ports

Parameter	Port0	Port1
Blocked	✗	✓
Signal Fail	✗	✗
Failure of Protocol - Provisioning Mismatch	✗	✗
UpdateTimeSecs	0	28948
Request state	No Request	No Request
Version of received R-APS. 0 means v1 etc	0	0
RPL blocked bit of R-APS info	✗	✗
Do Not Flush bit of R-APS info	✗	✗
Blocked Port Reference of R-APS info	RingPort0	RingPort0
Node ID of this request	00:00:00:00:00:00	00:01:C1:00:C9:90
Source MAC address used in the request/state	00:00:00:00:00:00	00:01:C1:00:C9:94

Counters

Counter type	Port0	Port1
Received erroneous R-APS PDUs	0	0
Received R-APS PDUs with our own node ID	1	3
Received R-APS PDUs during guard timer	0	0
Received R-APS PDUs causing FOP-PM	0	0
Received NR R-APS PDUs	0	6
Received NR, RB R-APS PDUs	0	0
Received SF R-APS PDUs	0	5
Received FS R-APS PDUs	0	0
Received MS R-APS PDUs	0	0
Received Event R-APS PDUs	0	0
Transmitted NR R-APS PDUs	3	3
Transmitted NR, RB R-APS PDUs	3	3
Transmitted SF R-APS PDUs	0	9
Transmitted FS R-APS PDUs	0	0
Transmitted MS R-APS PDUs	0	0
Transmitted Event R-APS PDUs	0	0
Number of local signal fails	1	2
Number of FDB flushes	5	5

Reset Counters

Command

Command
No request

Save Reset Back

Figure 3.18 Webpage to ERPS Detailed Status

Table 3.12 Description of ERPS Detailed Status

Label	Description
Configuration	This table shows the current configuration for this ERPS instance. Go to the ERPS Configuration help page for further explanation.
Status	This shows the current status of the ERPS instance. Go to the ERPS Status help page for further explanation.
Status Ports	This shows the current status of the ERPS instance. Go to the ERPS Status help page for further explanation.
Counters	This shows a number of counters useful for debug purpose. The Counter type column indicate the counted frame attribute.
ERPS Command	No request: There is no active local command on this instance. Issuing this command has no effect. Clear: Clear a switchover (FS or MS) request and a WTB/WTR condition and force reversion even if not revertive. Force switch to Port0: Causes a forced switchover. Blocks port1 and unblocks port0. Force switch to Port1: Causes a forced switchover. Blocks port0 and unblocks port1. Manual switch to Port0: Causes a switchover if the signal is good and no forced switch is in effect. Blocks port1 and unblocks port0. Manual switch to Port1: Causes a switchover if the signal is good and no forced switch is in effect. Blocks port0 and unblocks port1.

3.4 DHCPv4

3.4.1 Snooping Table

This Snooping Table webpage shown in Figure 3.19 displays the dynamic IP assigned information after DHCP Snooping mode is disabled. All DHCP clients obtained the dynamic IP address from the DHCP server will be listed in this table except for local VLAN interface IP addresses. Entries in the Dynamic DHCP snooping Table are shown on this page.

Each page shows up to 99 entries from the Dynamic DHCP snooping table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic DHCP snooping Table. The "MAC address" and "VLAN" input fields allow the user to select the starting point in the Dynamic DHCP snooping Table. Clicking the **Refresh button** will update the displayed table starting from that or the closest next Dynamic DHCP snooping Table match. In addition, the two input fields will - upon a **Refresh button** click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

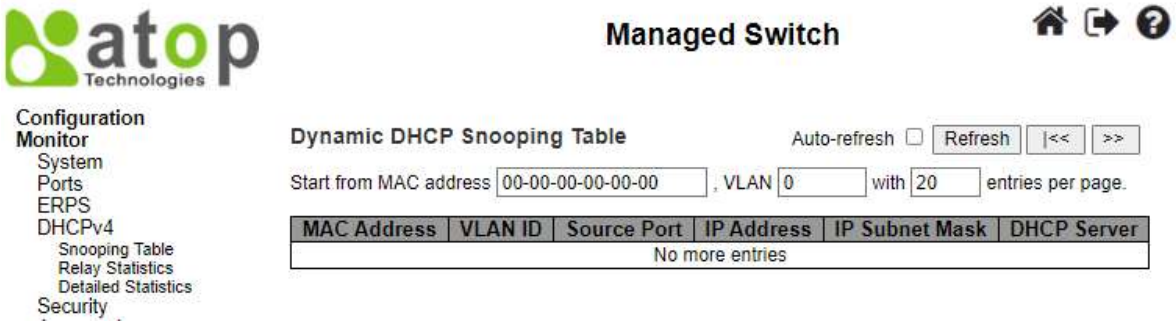


Figure 3.19 Webpage to Monitor Dynamic DHCP Snooping Table

Table 3.13 Monitoring Descriptions of Dynamic DHCP Snooping Table

Label	Description
MAC Address	User MAC address of the entry.
VLAN ID	VLAN-ID in which the DHCP traffic is permitted.
Source Port	Switch Port Number for which the entries are displayed.
IP Address	User IP address of the entry.
IP Subnet Mask	User IP subnet mask of the entry.
DHCP Server	DHCP Server address of the entry.

Check **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Clear** button to clear DHCP Message Received Counters and DHCP Message Sent Counters. Click **Refresh** button to refresh the page immediately. Click |<< to update the table starting from the first entry in the Dynamic DHCP snooping Table. Click >> to update the table entries, starting from the last entry currently displayed.

3.4.2 Relay Statistics

This webpage provides statistics for DHCP relay as shown in Figure 3.20. Description of each Server Statistics is summarized in Table 3.14.

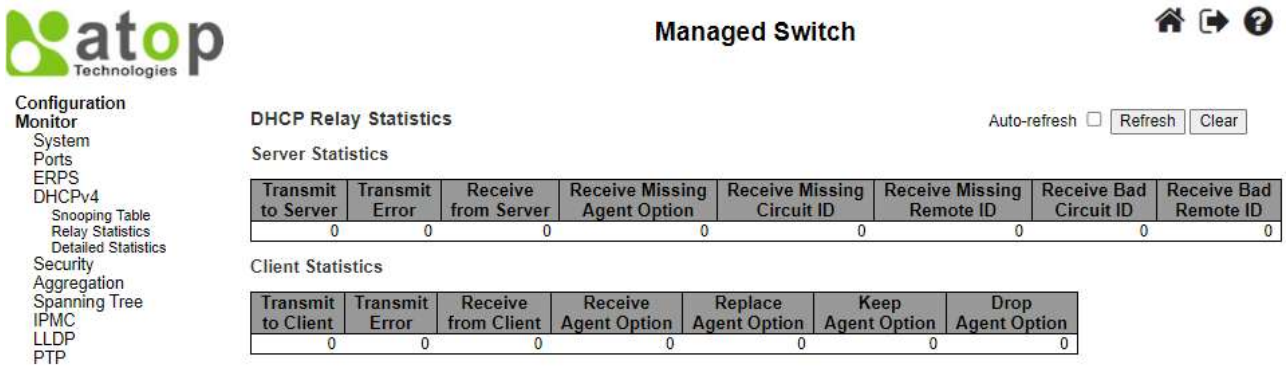


Figure 3.20 Webpage to Monitor DHCP Relay Statistics

Table 3.14 Monitoring Descriptions of DHCP Relay Statistics

Label	Description
Server Statistics	
Transmit To Server	The number of packets that are relayed from client to server.
Transmit Error	The number of packets that resulted in errors while being sent to clients.
Receive from Server	The number of packets received from server.
Receive Missing Agent Option	The number of packets received without agent information options.
Receive Missing Circuit ID	The number of packets received with the Circuit ID option missing.
Receive Missing Remote ID	The number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	The number of packets whose Circuit ID option did not match known circuit ID.
Receive Bad Remote ID	The number of packets whose Remote ID option did not match known Remote ID.
Client Statistics	
Transmit To Client	The number of relayed packets from server to client.
Transmit Error	The number of packets that resulted in error while being sent to servers.
Receive from Client	The number of received packets from server.
Receive Agent Option	The number of received packets with relay agent information option.
Replace Agent Option	The number of packets which were replaced with relay agent information option.
Keep Agent Option	The number of packets whose relay agent information was retained.
Drop Agent Option	The number of packets that were dropped which were received with relay agent information

Check **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately. Click **Clear button** clear all statistics.

3.4.3 Detailed Statistics

This Detailed Statistics webpage in Figure 3.21 provides statistics for DHCP snooping. Notice that the normal forward per-port TX statistics is not increased if the incoming DHCP packet is done by L3 forwarding mechanism. And clear the statistics on specific port may not take effect on global statistics since it gathers the different layer overview. Descriptions of Statistics are summarized in Table 3.15.

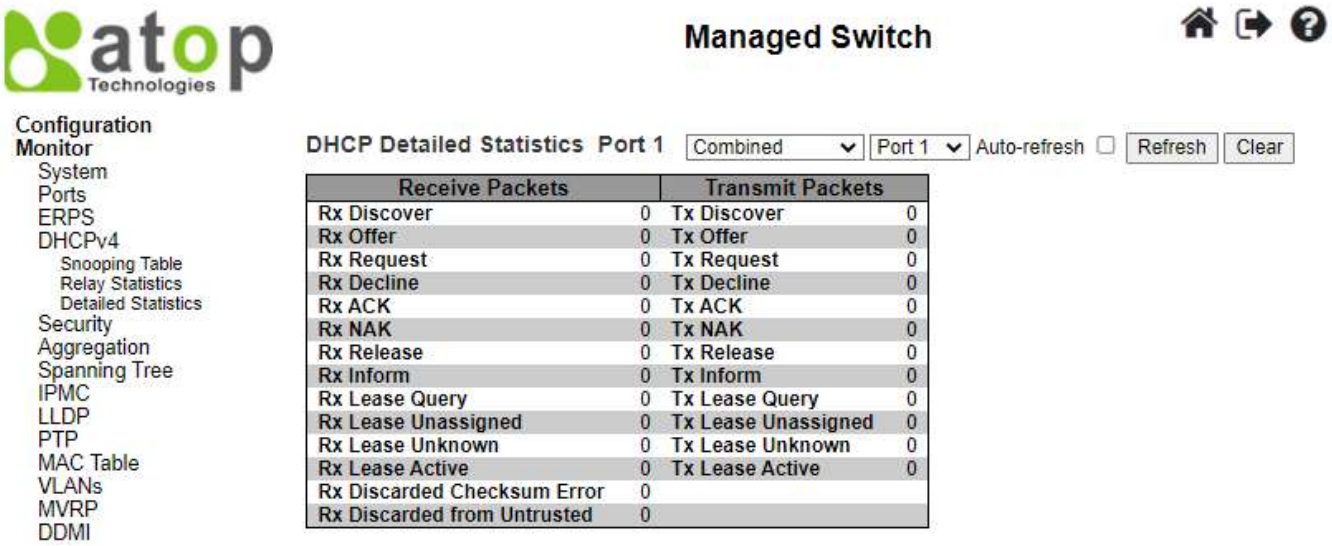


Figure 3.21 Webpage to Monitor DHCP Server Statistics

Table 3.15 Monitoring Descriptions of DHCP Detailed Statistics Port 1

Label	Description
Rx and Tx Discover	The number of discover (option 53 with value 1) packets received and transmitted.
Rx and Tx Offer	The number of offer (option 53 with value 2) packets received and transmitted.
Rx and Tx Request	The number of request (option 53 with value 3) packets received and transmitted.
Rx and Tx Decline	The number of decline (option 53 with value 4) packets received and transmitted.
Rx and Tx ACK	The number of ACK (option 53 with value 5) packets received and transmitted.
Rx and Tx NAK	The number of NAK (option 53 with value 6) packets received and transmitted.
Rx and Tx Release	The number of release (option 53 with value 7) packets received and transmitted
Rx and Tx Inform	The number of inform (option 53 with value 8) packets received and transmitted.
Rx and Tx Lease Query	The number of lease query (option 53 with value 10) packets received and transmitted.
Rx and Tx Lease Unassigned	The number of lease unassigned (option 53 with value 11) packets received and transmitted.
Rx and Tx Lease Unknown	The number of lease unknown (option 53 with value 12) packets received and transmitted.
Rx and Tx Lease Active	The number of lease active (option 53 with value 13) packets received and transmitted.
Rx Discarded Checksum Error	The number of discard packet that IP/UDP checksum is error.
Rx Discarded from Untrusted	The number of discarded packets that are coming from untrusted port.

The Combined DHCP user select box determines which user is affected by clicking the buttons. Port 1 .

The port select box determines which port is affected by clicking the buttons. Auto-refresh : Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh** button to refresh the page immediately. Click **Clear** button to blear all statistics

3.5 Security

3.5.1 Network

3.5.1.1 Port Security Overview

This webpage in Figure 3.22 shows the Port Security status. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise. The status page is divided into two sections - one with a legend of user modules and one with the actual port status. Table 3.16 summarizes the descriptions of Port Security Switch Status.

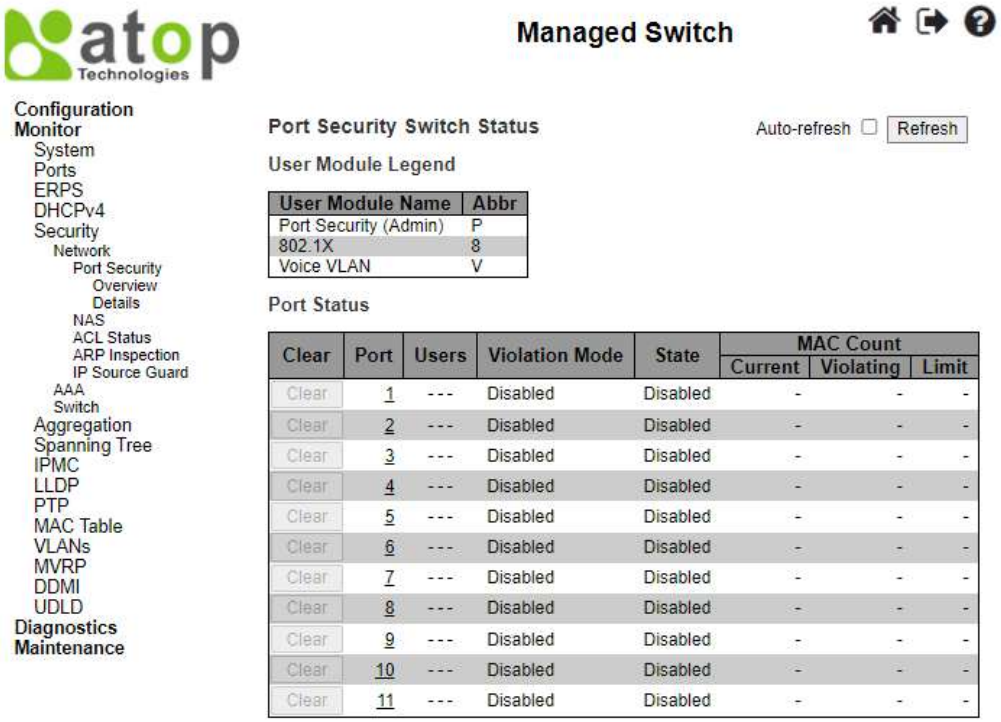


Figure 3.22 Webpage to Monitor DHCP Server Statistics

Table 3.16 Monitoring Descriptions of Port Security Switch Status

Label	Description
User Module Legend	
User Module Name	The full name of a module that may request Port Security services.
Abbr	A one-letter abbreviation of the user module. This is used in the Users column in the port status table.
Port Status	
Clear	Click to remove all dynamic MAC addresses on all VLANs on this port. The button is only clickable if number of secured MAC addresses is non-zero.
Port	The port number for which the status applies. Click the port number to see the status for this particular port.
Users	Each of the user modules has a column that shows whether that module has enabled Port Security or not. A '-' means that the corresponding user module is not enabled, whereas a letter indicates that the user module abbreviated by that letter (see Abbr) has enabled port security.

Label	Description
User Module Legend	
Violation Mode	Shows the configured Violation Mode of the port. It can take one of four values: **Disabled**: Port Security is not administratively enabled on this port. **Protect**: Port Security is administratively enabled in Protect mode. **Restrict**: Port Security is administratively enabled in Restrict mode. **Shutdown**: Port Security is administratively enabled in Shutdown mode.
State	Shows the current state of the port. It can take one of four values: **Disabled**: No user modules are currently using the Port Security service. **Ready**: The Port Security service is in use by at least one user module, and is awaiting frames from unknown MAC addresses to arrive. **Limit Reached**: The Port Security service is administratively enabled and the limit is reached. **Shut down**: The Port Security service is administratively enabled and the port is shut down. No MAC addresses can be learned on the port until it is administratively re-opened by administratively taking the port down and then back up on the "Configuration→Ports" page. Alternatively, the switch may be booted or reconfigured Port Security-wise.
MAC Count (Current, Violating, Limit)	The three columns indicate the number of currently learned MAC addresses (forwarding as well as blocked), the number of violating MAC address (only counting in Restrict mode) and the maximum number of MAC addresses that can be learned on the port, respectively. If no user modules are enabled on the port, the Current column will show a dash (-). If Port Security is not administratively enabled on the port, the Violating and Limit columns will show a dash (-)..

Check **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.5.1.2 Port Security Details

This page shows the MAC addresses secured by the Port Security module. Port Security is a module with no direct configuration. Configuration comes indirectly from other modules - the user modules. When a user module has enabled port security on a port, the port is set-up for software-based learning. In this mode, frames from unknown MAC addresses are passed on to the port security module, which in turn asks all user modules whether to allow this new MAC address to forward or block it. For a MAC address to be set in the forwarding state, all enabled user modules must unanimously agree on allowing the MAC address to forward. If only one chooses to block it, it will be blocked until that user module decides otherwise.

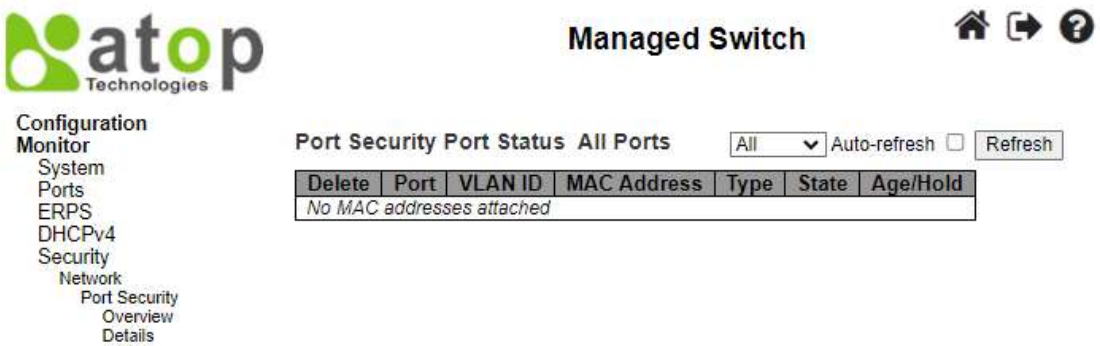


Figure 3.23 Webpage to Monitor Port Security Port Status All Ports

Table 3.17 Monitoring Descriptions of Port Security Port Status All Ports

Label	Description
Delete	Click to remove this particular MAC addresses from MAC address table. The button is only clickable if the entry type is Dynamic. Use the "Configuration→Security→Port Security→MAC Addresses" page to remove Static and Sticky entries.
Port	If all ports are shown (can be selected through the drop-down box on the top right), this one shows the port to which the MAC address is bound.
MAC Address & VLAN ID	The MAC address and VLAN ID that is seen on this port. If no MAC addresses are learned, a single row stating "No MAC addresses attached" is displayed.
Type	Indicates the type of entry. Takes one of three values: • **Dynamic**: The entry is learned through learn frames coming to the Port Security module while the port in question is not in sticky mode. • **Static**: The entry is entered by the end-user through management. Entry is not subject to aging. • **Sticky**: When the port is in sticky mode, all entries that would otherwise have been learned as dynamic are learned as sticky. Sticky entries are part of the running-config and can therefore be saved to startup-config. An important aspect of sticky MAC addresses is that they survive link changes (in contrast to Dynamic, which will have to be learned again). They also survive reboots if running-config is saved to startup-config.
State	Indicates whether the corresponding MAC address is blocked or forwarding. In the blocked state, it will not be allowed to transmit or receive traffic.
Age/Hold	If at least one user module has decided to block this MAC address, it will stay in the blocked state until the hold time (measured in seconds) expires. If all user modules have decided to allow this MAC address to forward, and aging is enabled, the Port Security module will periodically check that this MAC address still forwards traffic. If the age period (measured in seconds) expires and no frames have been seen, the MAC address will be removed from the MAC table. Otherwise, a new age period will begin. If aging is disabled or a user module has decided to hold the MAC address indefinitely, a dash (-) will be shown.

Use the port select box Port 1 to select which port to show status for. Click on **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately

3.5.1.3 NAS Switch

This page provides an overview of the current NAS port states. NAS is an acronym for **N**etwork **A**ccess **S**erver. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

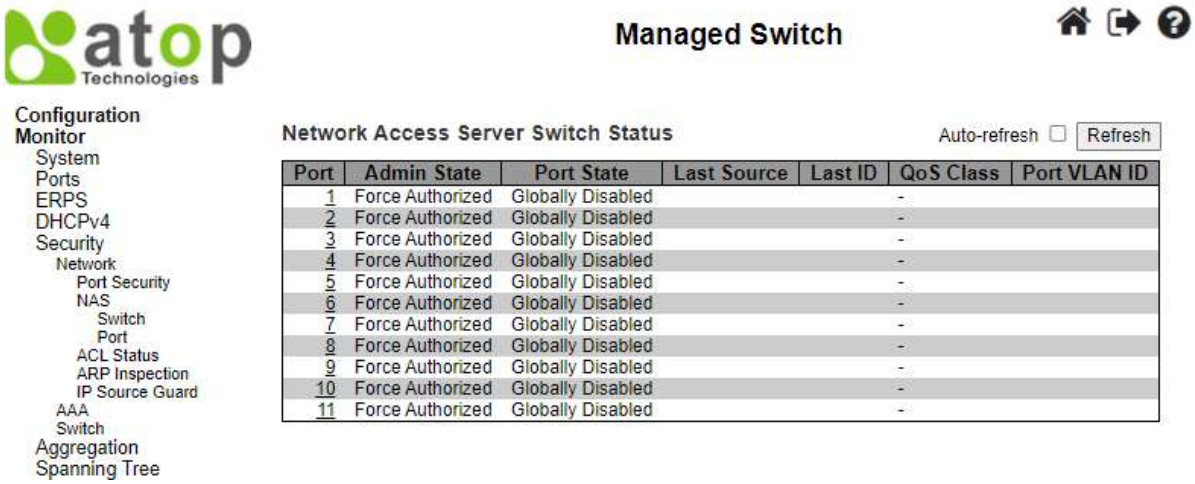


Figure 3.24 Webpage to Monitor Network Access Server Switch Status

Table 3.18 Monitoring Descriptions of Network Access Server Switch Status

Label	Description
Port	The switch port number. Click to navigate to detailed NAS statistics for this port.
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.
QoS Class	QoS Class assigned to the port by the RADIUS server if enabled.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs at Configuration->Security->Network->NAS. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs Configuration->Security->Network->NAS.

Check **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.5.1.4 NAS Port

This page provides detailed NAS statistics for a specific switch port running EAPOL-based IEEE 802.1X authentication. For MAC-based ports, it shows selected backend server (RADIUS Authentication Server) statistics, only. Use the port select box to select which port details to be displayed.

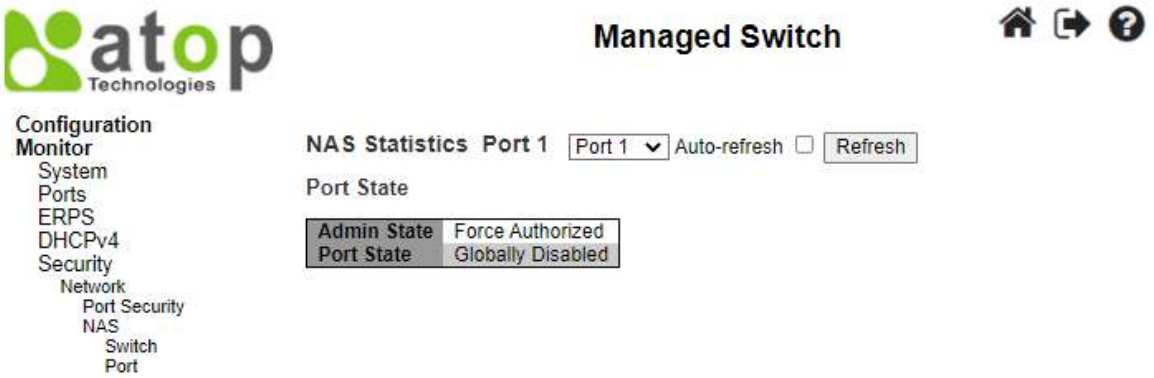


Figure 3.25 Webpage to Monitor NAS Statistics Port 1

able 3.19 Monitoring Descriptions of NAS Statistics Port 1

Label	Description
Port State	
Admin State	The port's current administrative state. Refer to NAS Admin State for a description of possible values.
Port State	The current state of the port. Refer to NAS Port State for a description of the individual states.
QoS Class	The QoS class assigned by the RADIUS server. The field is blank if no QoS class is assigned.
Port VLAN ID	The VLAN ID that NAS has put the port in. The field is blank, if the Port VLAN ID is not overridden by NAS. If the VLAN ID is assigned by the RADIUS server, "(RADIUS-assigned)" is appended to the VLAN ID. Read more about RADIUS-assigned VLANs Configuration->Security->Network->NAS. If the port is moved to the Guest VLAN, "(Guest)" is appended to the VLAN ID. Read more about Guest VLANs Configuration->Security->Network->NAS.
Port Counters	
EAPOL Counters	These supplicant frame counters are available for the following administrative states: • Force Authorized • Force Unauthorized • Port-based 802.1X
Backend Server Counters	These backend(RADIUS) frame counters are available for the following administrative states: • Port-based 802.1X
Last Supplicant/Client Info	Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states: • Port-based 802.1X • Single 802.1X • Multi 802.1X • MAC-based Auth.
Selected Counters	
Selected Counters	The Selected Counters table is visible when the port is in one of the following administrative states: • MAC-based Auth. The table is identical to and is placed next to the Port Counters table, and will be empty if no MAC address is currently selected. To populate the table, select one of the attached MAC Addresses from the table below.
Attached MAC Addresses	
Identity	Shows the identity of the supplicant, as received in the Response Identity EAPOL frame. Clicking the link causes the supplicant's EAPOL and Backend Server counters to be shown in the Selected Counters table. If no supplicants are attached, it shows No supplicants attached. This column is not available for MAC-based Auth.
MAC Address	For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.
VLAN ID	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.
State	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.

Label	Description
Port State	
Last Authentication	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

The port select box Port 1 determines which port is affected when clicking the buttons. Check Auto-refresh box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately. The **Clear button** is available in the following modes: **Force Authorized**, **Force Unauthorized**, **Port-based 802.1X**, and **Single 802.1X mode**. Click to clear the counters for the selected port. The **Clear All** button is available in the following modes: **Multi 802.1X** and **MAC-based Auth.X**. Click to clear both the port counters and all of the attached client's counters. The "Last Client" will not be cleared. However, the **Clear This** button is available in the following modes: **Multi 802.1X** and **MAC-based Auth.X**. Click to clear only the currently selected client's counters.

3.5.1.5 ACL Status

This page shows the ACL status by different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

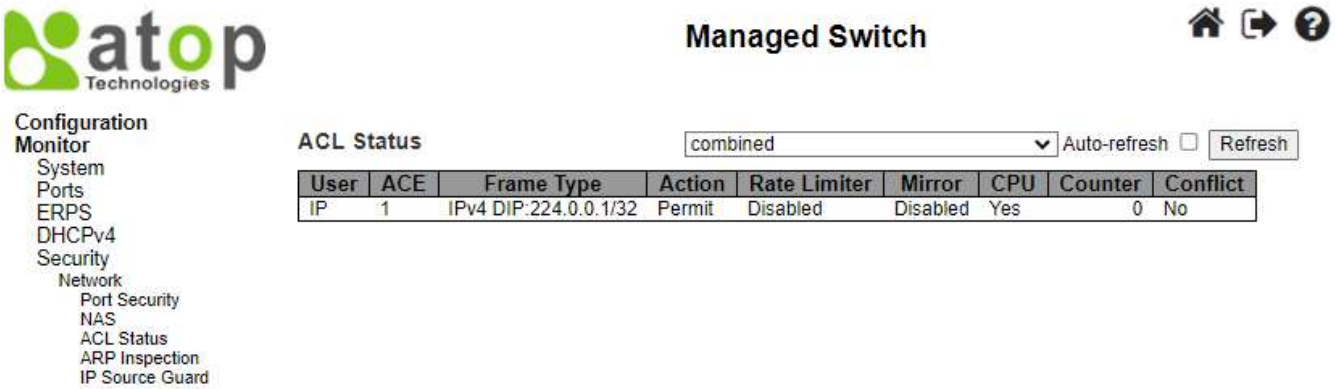


Figure 3.26 Webpage to Monitor ACL Status

Table 3.20 Monitoring Descriptions of ACL Status

Label	Description
User	Indicates the ACL user.
ACE	Indicates the ACE ID on local switch.
Frame Type	Indicates the frame type of the ACE. Possible values are: **Any**: The ACE will match any frame type. **EType**: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. **ARP**: The ACE will match ARP/RARP frames. **IPv4**: The ACE will match all IPv4 frames. **IPv4/ICMP**: The ACE will match IPv4 frames with ICMP protocol. **IPv4/UDP**: The ACE will match IPv4 frames with UDP protocol. **IPv4/TCP**: The ACE will match IPv4 frames with TCP protocol. **IPv4/Other**: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. **IPv6**: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. **Permit**: Frames matching the ACE may be forwarded and learned. **Deny**: Frames matching the ACE are dropped. **Filter**: Frames matching the ACE are filtered.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
CPU	Forward packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.

Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.

The select box combined determines which ACL user is affected by clicking the buttons. Check **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately

3.5.1.6 ARP Inspection

Entries in the Dynamic ARP Inspection Table are shown on this page. The Dynamic ARP Inspection Table contains up to 256 entries, and is sorted first by port, then by VLAN ID, then by MAC address, and then by IP address. All dynamic entries are learning from DHCP Snooping.

Each page shows up to 99 entries from the Dynamic ARP Inspection table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Dynamic ARP Inspection Table. The "Start from port address", "VLAN", "MAC address" and "IP address" input fields allow the user to select the starting point in the Dynamic ARP Inspection Table. Clicking the **Refresh button** will update the displayed table starting from that or the closest next Dynamic ARP Inspection Table match. In addition, the two input fields will - upon a **Refresh button** click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

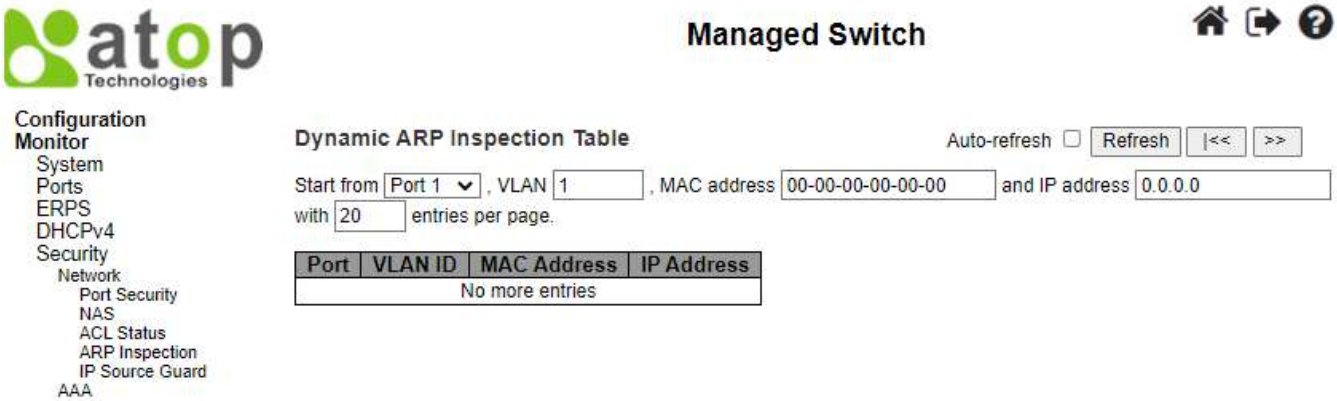


Figure 3.27 Webpage to Monitor Dynamic ARP Inspection Table

Table 3.21 Monitoring Descriptions of Dynamic ARP Inspection Table

Label	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the ARP traffic is permitted.
MAC Address	User MAC address of the entry.
IP Address	User IP address of the entry.

Check **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click Refresh button to refresh the page immediately. Click **Clear button** to flushes all dynamic entries. Click |<< to update the table starting from the first entry in the Dynamic ARP Inspection Table. Click >> to update the table, starting with the entry after the last entry currently displayed.

3.5.1.7 IP Source Guard

Entries in the Dynamic IP Source Guard Table are shown on this page. The Dynamic IP Source Guard Table is sorted first by port, then by VLAN ID, then by IP address, and then by MAC address.

Each page shows up to 99 entries from the Dynamic IP Source Guard table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of

the Dynamic IP Source Guard Table. The "Start from port address", "VLAN" and "IP address" input fields allow the user to select the starting point in the Dynamic IP Source Guard Table. Clicking the Refresh button will update the displayed table starting from that or the closest next Dynamic IP Source Guard Table match. In addition, the two input fields will - upon a Refresh button click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

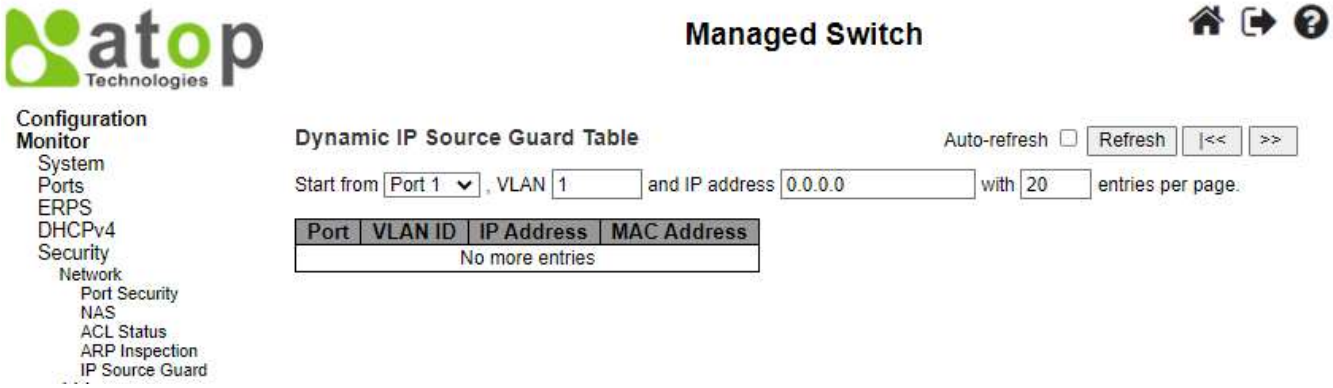


Figure 3.28 Webpage to Monitor Dynamic IP Source Guard Table

Table 3.22 Monitoring Descriptions of Dynamic IP Source Guard Table

Label	Description
Port	Switch Port Number for which the entries are displayed.
VLAN ID	VLAN-ID in which the IP traffic is permitted.
IP Address	User IP address of the entry.
MAC Address	Source MAC address.

Check Auto-refresh box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click Refresh button to refresh the page immediately. Click Clear button to flush all dynamic entries. Click |<< to update the table starting from the first entry in the Dynamic ARP Inspection Table. Click >> to update the table, starting with the entry after the last entry currently displayed.

3.5.2 AAA

3.5.2.1 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the Authentication configuration page.

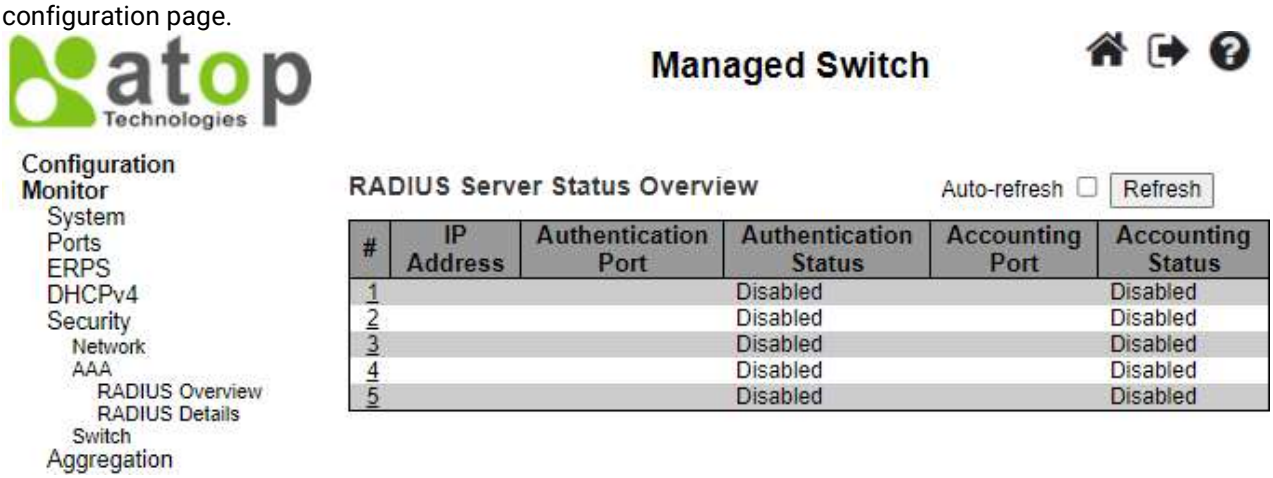


Figure 3.29 Webpage to Monitor RADIUS Server Status Overview

Table 3.23 Monitoring Descriptions of RADIUS Server Status Overview

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics for this server.
IP Address	The IP address of this server.
Authentication Port	UDP port number for authentication.
Authentication Status	The current status of the server. This field takes one of the following values: **Disabled**: The server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Accounting Port	UDP port number for accounting.
Accounting Status	The current status of the server. This field takes one of the following values: **Disabled**: The server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

Check **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh** button to refresh the page immediately

After clicking on each port, the following webpage will be launched, as shown in Figure 3.30. Table 3.24 shows the description of each port's RADIUS server status.

RADIUS Authentication Statistics for Server #1 Server #1 Auto-refresh Refresh Clear

Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address			
State			Disabled
Round-Trip Time			0 ms

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address			
State			Disabled
Round-Trip Time			0 ms

Figure 3.30 Webpage to Monitor Each Port's RADIUS Server Status

Table 3.24 Monitoring Descriptions of Each Port's RADIUS Server Status

Label	Description
RADIUS Authentication Statistics for Server#1 **RADIUS Authentication Statistics** map closely to those specified in RFC4668 - RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for. For **RADIUS authentication server packet counter**, there are seven receive and four transmit counters.	
Receive Packets	
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Unknown Types	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Packets Dropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Transmit Packets	
Access Requests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Access Retransmission	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Pending Requests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Timeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Other Info	
IP Address	IP address and UDP port for the authentication server in question.
State	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left

	before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

3.5.2.2 RADIUS Details

This page provides detailed statistics for a particular RADIUS server.

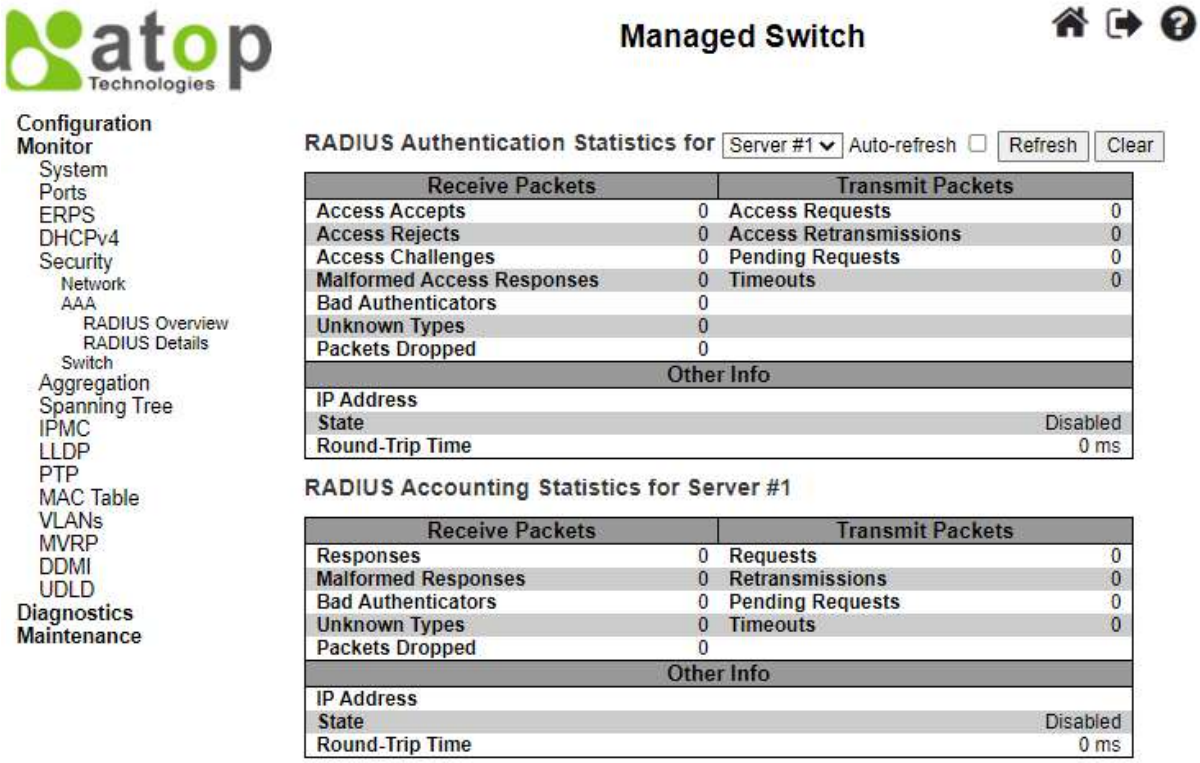


Figure 3.31 Webpage to Monitor RADIUS Authentication and Accounting Statistics

Table 3.25 Monitoring Descriptions of RADIUS Authentication and Accounting Statistics

Label	Description
RADIUS Authentication Statistics for Server#1 **RADIUS Authentication Statistics** map closely to those specified in RFC4668 – RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for. For **RADIUS authentication server packet counter**, there are seven receive and four transmit counters.	
Receive Packets	
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Malformed Access Responses	The number of malformed RADIUS Access Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message

Label	Description
RADIUS Authentication Statistics for Server#1 **RADIUS Authentication Statistics** map closely to those specified in RFC4668 – RADIUS Authentication Client MIB. Use the server select box to switch between the backend servers to show details for. For **RADIUS authentication server packet counter**, there are seven receive and four transmit counters.	
Receive Packets	
	Authenticator attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Unknown Types	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Packets Dropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Transmit Packets	
Access Requests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Access Retransmission	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Pending Requests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.
Timeouts	The number of authentication timeouts to the server. After timeout a, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Other Info	
IP Address	IP address and UDP port for the authentication server in question.
State	Shows the state of the server. It takes one of the following values: **Disabled**: The selected server is disabled. **Not Ready**: The server is enabled, but IP communication is not yet up and running. **Ready**: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. **Dead (X seconds left)**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

The server select box determines which server is affected by clicking the buttons. Click check Auto-refresh box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click Refresh button to refresh the page immediately. Click Clear button to clear the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation.

3.5.3 Switch

3.5.3.1 RMON Statistics

This page provides an overview of RMON Statistics entries. Each page shows up to 99 entries from the Statistics table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the Statistics table. The first displayed will be the one with the lowest ID found in the Statistics table.

The "Start from Control Index" allows the user to select the starting point in the Statistics table. Clicking the Refresh button will update the displayed table starting from that or the next closest Statistics table match. The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

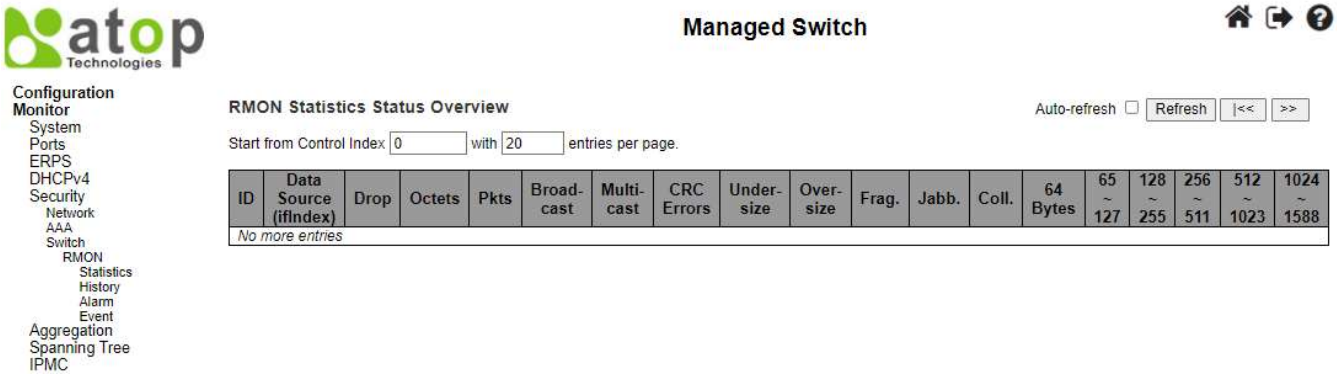


Figure 3.32 Webpage to Monitor RMON Statistics Status Overview

Table 3.26 Monitoring Descriptions of RMON Statistics Status Overview

Label	Description
ID	Indicates the index of Statistics entry.
Data Source(ifIndex)	The port ID which wants to be monitored.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broad-cast	The total number of good packets received that were directed to the broadcast address.
Multi-cast	The total number of good packets received that were directed to a multicast address.
CRC Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Under-size	The total number of packets received that were less than 64 octets.
Over-size	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
64 Bytes	The total number of packets (including bad packets) received that were 64 octets in length.

Label	Description
65~127	The total number of packets (including bad packets) received that were between 65 to 127 octets in length.
128~255	The total number of packets (including bad packets) received that were between 128 to 255 octets in length.
256~511	The total number of packets (including bad packets) received that were between 256 to 511 octets in length.
512~1023	The total number of packets (including bad packets) received that were between 512 to 1023 octets in length.
1024~1588	The total number of packets (including bad packets) received that were between 1024 to 1588 octets in length.

Check Auto-refresh box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click Refresh button to refresh the page immediately. Click |<< to update the table starting from the first entry in the Statistics table, i.e. the entry with the lowest ID. Click >> to updates the table, starting with the entry after the last entry currently displayed.

3.5.3.2 RMON History

This page provides an overview of RMON History entries. Each page shows up to 99 entries from the History table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the History table. The first displayed will be the one with the lowest History Index and Sample Index found in the History table. The "Start from History Index and Sample Index" allows the user to select the starting point in the History table. Clicking the Refresh button will update the displayed table starting from that or the next closest History table match. The >> will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

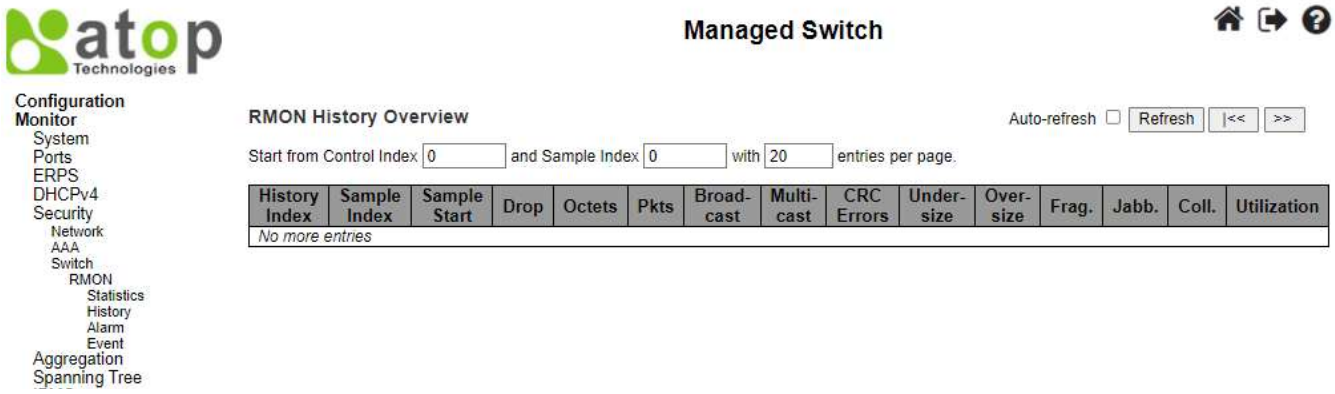


Figure 3.33 Webpage to Monitor RMON History Overview

Table 3.27 Monitoring Descriptions of RMON History Overview

Label	Description
History Index	Indicates the index of History control entry.
Sample Index	Indicates the index of the data entry associated with the control entry.
Sample Start	The value of sysUpTime at the start of the interval over which this sample was measured.
Drop	The total number of events in which packets were dropped by the probe due to lack of resources.
Octets	The total number of octets of data (including those in bad packets) received on the network.
Pkts	The total number of packets (including bad packets, broadcast packets, and multicast packets) received.
Broadcast	The total number of good packets received that were directed to the broadcast address.
Multicast	The total number of good packets received that were directed to a multicast address.

CRCErrors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Undersize	The total number of packets received that were less than 64 octets.
Oversize	The total number of packets received that were longer than 1518 octets.
Frag.	The number of frames which size is less than 64 octets received with invalid CRC.
Jabb.	The number of frames which size is larger than 64 octets received with invalid CRC.
Coll.	The best estimate of the total number of collisions on this Ethernet segment.
Utilization	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.

Click Auto-refresh box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately. Click |<< to update the table starting from the first entry in the History table, i.e., the entry with the lowest History Index and Sample Index. Click >> to update the table, starting with the entry after the last entry currently displayed.

3.5.3.3 RMON Alarm

Configure RMON Alarm table on this page. The entry index key is ID.

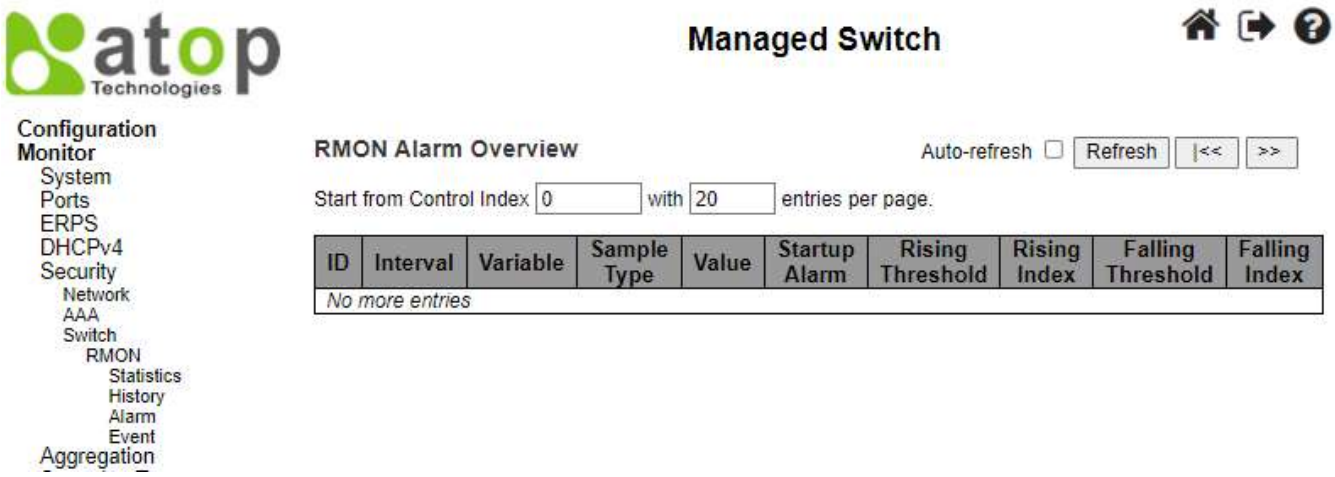


Figure 3.34 Webpage to Monitor RMON Alarm Overview

Table 3.28 Monitoring Descriptions of RMON Alarm Overview

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
ID	Indicates the index of the entry. The range is from 1 to 65535.
Interval	Indicates the interval in seconds for sampling and comparing the rising and falling threshold. The range is from 1 to 2^31-1.
Variable	Indicates the particular variable to be sampled, the possible variables are: *InOctets:* The total number of octets received on the interface, including framing characters. *InUcastPkts:* The number of uni-cast packets delivered to a higher-layer protocol. *InNUcastPkts:* The number of broad-cast and multi-cast packets delivered to a higher-layer protocol. *InDiscards:* The number of inbound packets that are discarded even the packets are normal. *InErrors:* The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. *InUnknownProtos:* the number of the inbound packets that were discarded because of the unknown or un-support protocol. *OutOctets:* The number of octets transmitted out of the interface, including framing characters. *OutUcastPkts:* The number of uni-cast packets that request to transmit. *OutNUcastPkts:* The number of broad-cast and multi-cast packets that request to transmit. *OutDiscards:* The number of outbound packets that are discarded event the packets are normal. *OutErrors:* The number of outbound packets that could not be transmitted because of errors. *OutQLen:* The length of the output packet queue (in packets).

Label	Description
Sample Type	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: *Absolute:* Get the sample directly. *Delta:* Calculate the difference between samples (default).
Value	The value of the statistic during the last sampling period.
Startup Alarm	The method of sampling the selected variable and calculating the value to be compared against the thresholds, possible sample types are: *Rising* Trigger alarm when the first value is larger than the rising threshold. *Falling* Trigger alarm when the first value is less than the falling threshold. *RisingOrFalling* Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default).
Rising Threshold	Rising threshold value (-2147483648-2147483647).
Rising Index	Rising event index (1-65535).
Falling Threshold	Falling threshold value (-2147483648-2147483647)
Falling Index	Falling event index (1-65535).

Click **Add New Entry button** to add a new access management entry. Click **Save button** to save changes. Click **Reset button** to undo any changes made locally and revert to previously saved values.

3.5.3.4 RMON Event

Configure RMON Event table on this page. The entry index key is ID.

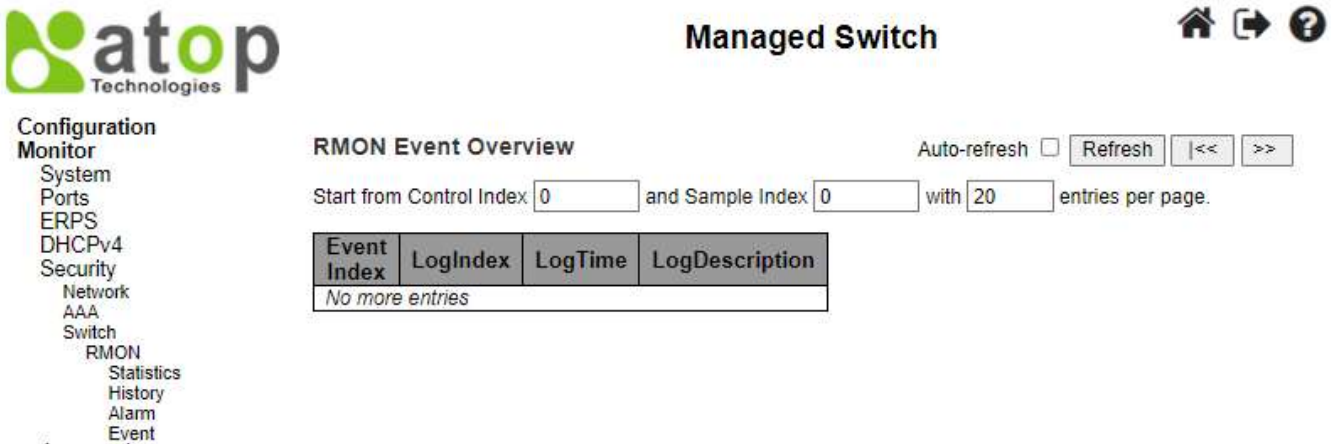


Figure 3.35 Webpage to Monitor RMON Event

Table 3.29 Monitoring Descriptions of RMON Event

Label	Description
Event Index	Indicates the index of the event entry.
Log Index	Indicates the index of the log entry.
LogTime	Indicates Event log time
LogDescription	Indicates the Event description.

3.6 Aggregation

3.6.1 Status

This page is used to see the status of ports in Aggregation group. Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

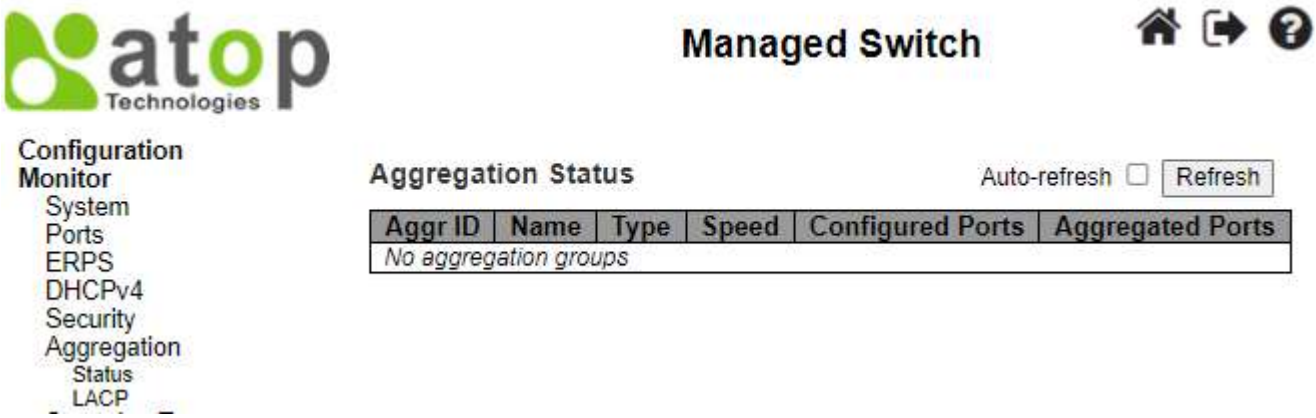


Figure 3.36 Webpage to Monitor Aggregation Status

Table 3.30 Monitoring Descriptions of Aggregation Status

Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance.
Name	Name of the Aggregation group ID.
Type	Type of the Aggregation group (Static or LACP).
Speed	Speed of the Aggregation group.
Configured ports	Configured member ports of the Aggregation group.
Aggregated ports	Aggregated member ports of the Aggregation group.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.6.2 LACP

3.6.2.1 System Status

This page provides a status overview for all LACP instances. LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol, allows bundling several physical ports together to form a single logical port.

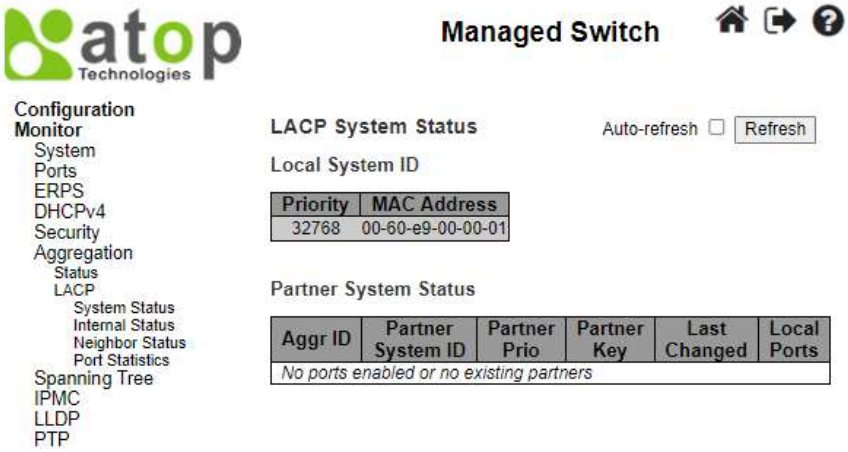


Figure 3.37 Webpage to Monitor LACP System Status

Table 3.31 Monitoring Descriptions of LACP System Status

Label	Description
Aggr ID	The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id'
Partner System ID	The system ID (MAC address) of the aggregation partner.
Partner Key	The Key that the partner has assigned to this aggregation ID.
Last changed	The time since this aggregation changed.
Local Ports	Shows which ports are a part of this aggregation for this switch.

Check **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.6.2.2 Internal Status

This page provides a status overview for the LACP internal (i.e. local system) status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters please refer to IEEE 801.AX-2014.

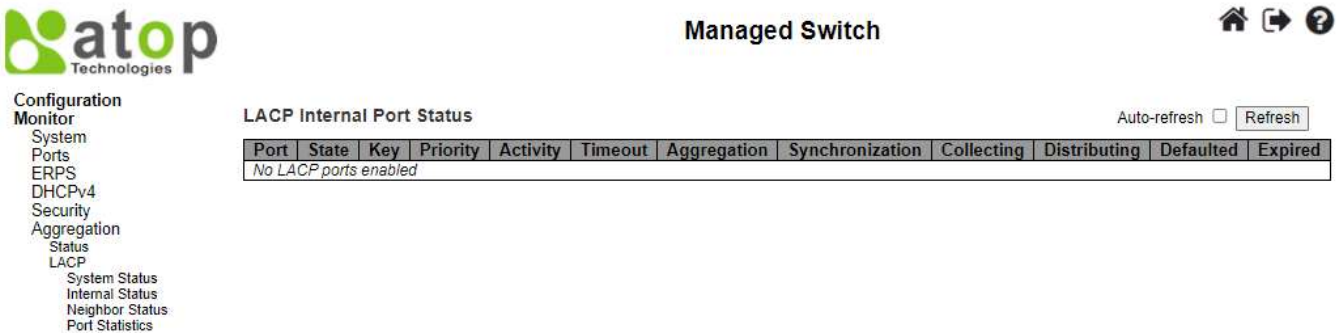


Figure 3.38 Webpage to Monitor LACP Internal Port Status

Table 3.32 Monitoring Descriptions of LACP Internal Port Status

Label	Description
Port	The switch port number.
State	The current port state: • **Down:** The port is not active. • **Active:** The port is in active state. • **Standby:** The port is in standby state.
Key	The key assigned to this port. Only ports with the same key can aggregate together.
Priority	The priority assigned to this aggregation group.
Activity	The LACP mode of the group (Active or Passive).
Timeout	The timeout mode configured for the port (Fast or Slow).
Aggregation	Show whether the system considers this link to be "aggregable"; i.e., a potential candidate for aggregation.
Synchronization	Show whether the system considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.
Collecting	Show if collection of incoming frames on this link is enabled.
Distributing	Show if distribution of outgoing frames on this link is enabled.
Defaulted	Show if the Actor's Receive machine is using Defaulted operational Partner information.
Expired	Show if that the Actor's Receive machine is in the EXPIRED state.

Check **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.6.2.3 Neighbor Status

This page provides a status overview for the LACP neighbour status for all ports. Only ports that are part of an LACP group are shown. For details on the shown parameters please refer to IEEE 801.AX-2014.

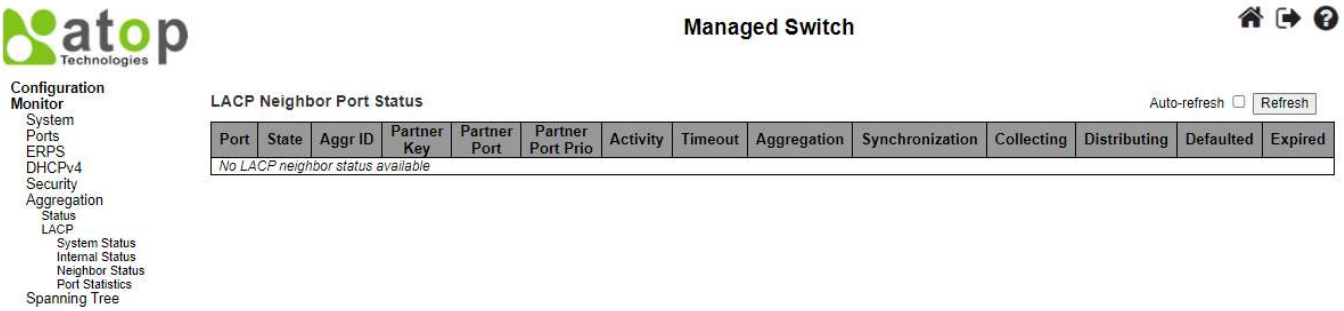


Figure 3.39 Webpage to Monitor LACP Neighbour Port Status

Table 3.33 Monitoring Descriptions of LACP Neighbour Port Status

Label	Description
Port	The switch port number.
State	The current port state: • **Down:** The port is not active. • **Active:** The port is in active state. • **Standby:** The port is in standby state.
Aggr ID	The aggregation group ID which the port is assigned to.
Partner Key	The key assigned to this port by the partner.
Partner Port	The partner port number associated with this link.
Partner Port Priority	The priority assigned to this partner port.
Activity	The LACP mode of the group (Active or Passive).
Timeout	The timeout mode configured for the partner port (Fast or Slow).
Aggregation	Show whether the partner considers this link to be "aggregable"; i.e., a potential candidate for aggregation.
Synchronization	Show whether the partner considers this link to be "IN_SYNC"; i.e., it has been allocated to the correct LAG, the group has been associated with a compatible Aggregator, and the identity of the LAG is consistent with the System ID and operational Key information transmitted.
Collecting	Show if collection of incoming frames on this link is enabled.
Distributing	Show if distribution of outgoing frames on this link is enabled.
Defaulted	Show if the partners Receive machine is using Defaulted operational Partner information.
Expired	Show if that the partners Receive machine is in the EXPIRED state.

Check **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.6.2.4 Port Statistics

This page provides an overview for LACP statistics for all ports.

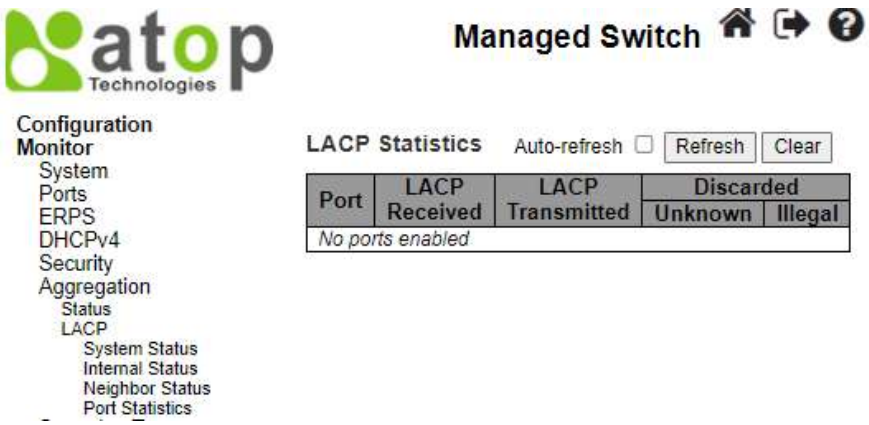


Figure 3.40 Webpage to Monitor LACP Statistics

Table 3.34 Monitoring Descriptions of LACP Statistics

Label	Description
Port	The switch port number.
LACP Received	Shows how many LACP frames have been received at each port.
LACP Transmitted	Shows how many LACP frames have been sent from each port.
Discarded	Shows how many unknown or illegal LACP frames have been discarded at each port.

Check **Auto-refresh** box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately. Click **Clear button** to clear the counters for the selected server. The "Pending Requests" counter will not be cleared by this operation

3.7 Spanning Tree

3.7.1 Bridge Status

This page provides a status overview of all STP bridge instances.

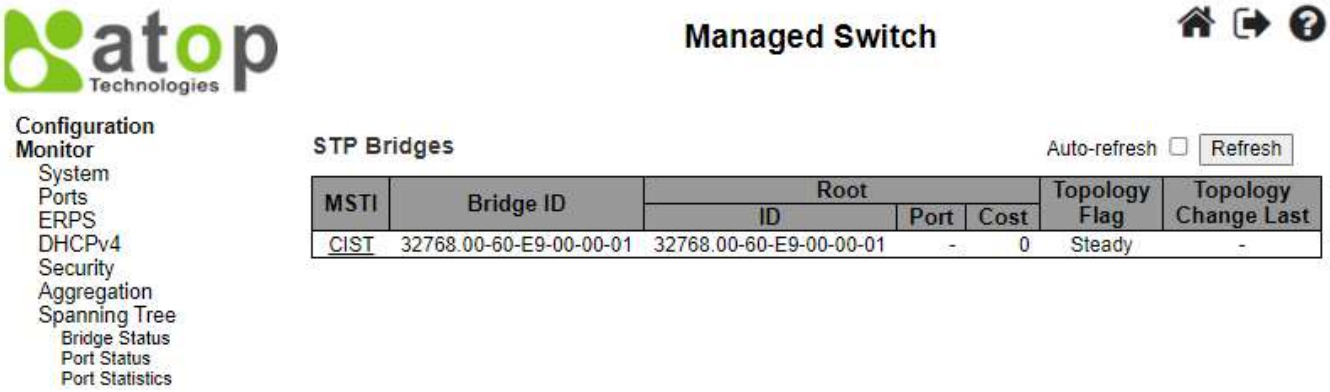


Figure 3.41 Webpage to Monitor STP Bridges

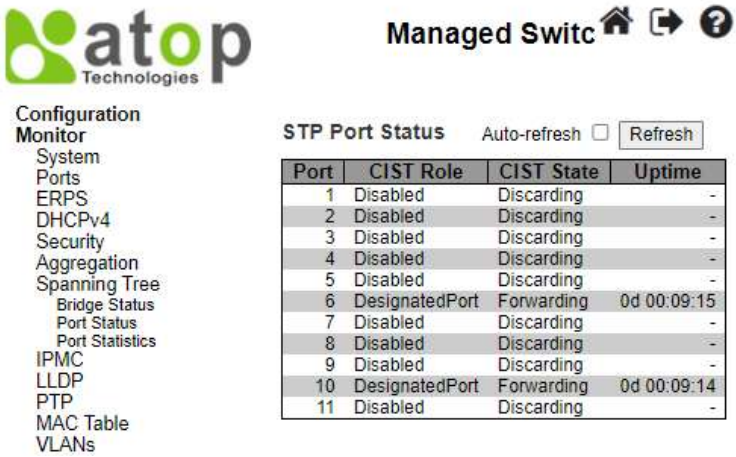
Table 3.35 Monitoring Descriptions of STP Bridges

Label	Description
Bridge ID	The Bridge ID of this Bridge instance.
Root ID	The Bridge ID of the currently elected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root Path Cost. For the Root Bridge it is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag of this Bridge instance.
Topology Change Last	The time since last Topology Change occurred.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.7.2 Port Status

This page displays the STP CIST port status for physical ports of the switch.



Port	CIST Role	CIST State	Uptime
1	Disabled	Discarding	-
2	Disabled	Discarding	-
3	Disabled	Discarding	-
4	Disabled	Discarding	-
5	Disabled	Discarding	-
6	DesignatedPort	Forwarding	0d 00:09:15
7	Disabled	Discarding	-
8	Disabled	Discarding	-
9	Disabled	Discarding	-
10	DesignatedPort	Forwarding	0d 00:09:14
11	Disabled	Discarding	-

Figure 3.42 Webpage to Monitor STP Port Status

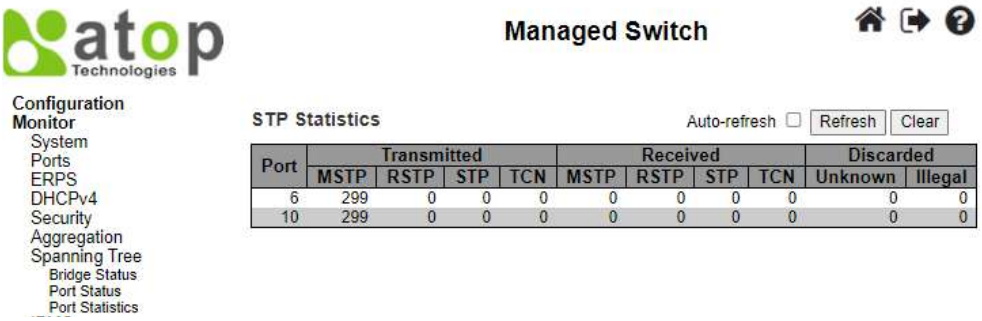
Table 3.36 Monitoring Descriptions of STP Port Status

Label	Description
Port	The switch port number of the logical STP port.
CIST Role	The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort Disabled.
CIST State	The current STP port state of the CIST port. The port state can be one of the following values: Discarding Learning Forwarding.
Uptime	The time since the bridge port was last initialized.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.7.3 Port Statistics

This page displays the STP port statistics counters of bridge ports in the switch.



Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
6	299	0	0	0	0	0	0	0	0	0
10	299	0	0	0	0	0	0	0	0	0

Figure 3.43 Webpage to Monitor STP Statistics

Table 3.37 Monitoring Descriptions of STP Statistics

Label	Description
Port	The switch port number of the logical STP port.
Transmitted/Received MSTP	The number of MSTP BPDU's received/transmitted on the port.
Transmitted/Received RSTP	The number of RSTP BPDU's received/transmitted on the port.

Transmitted/Received STP	The number of legacy STP Configuration BPDU's received/transmitted on the port.
Transmitted/Received TCN	The number of (legacy) Topology Change Notification BPDU's received/transmitted on the port.
Discarded Unknown	The number of unknown Spanning Tree BPDU's received (and discarded) on the port.
Discarded Illegal	The number of illegal Spanning Tree BPDU's received (and discarded) on the port.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.8 IPMC

3.8.1 IGMP Snooping

Figure 3.44 IGMP Snooping Submenu under Configuration->IPMC Main Menu

3.8.1.1 Status

This page provides IGMP Snooping status.

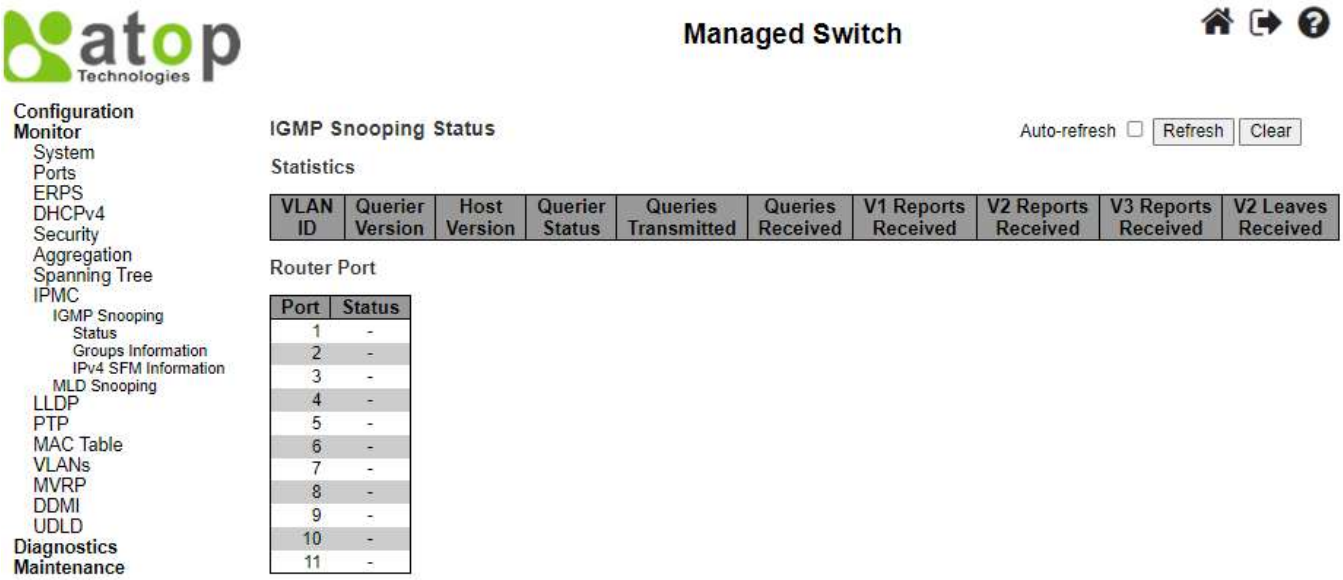


Figure 3.45 Webpage to Monitor DHCP Server Statistics

Table 3.38 Descriptions of DHCP Server Statistics Monitoring

Label	Description
Statistics	
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
Queries Transmitted	The number of Transmitted Queries.
Queries Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports.
V3 Reports Received	The number of Received V3 Reports.
V2 Leaves Received	The number of Received V2 Leaves.
Router Port Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.	
Port	Switch port number.
Status	Indicate whether specific port is a router port or not.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately. Click **Clear button** to clear all Statistics counters.

3.8.1.2 Groups Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the IGMP Group table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table. The "Start from VLAN", and "group" input fields allow the user to select the starting point in the IGMP Group Table. Clicking the **Refresh button** will update the displayed table starting from that or the closest next IGMP Group Table match. In addition, the two input fields will - upon a **Refresh button** click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> will use the last

entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

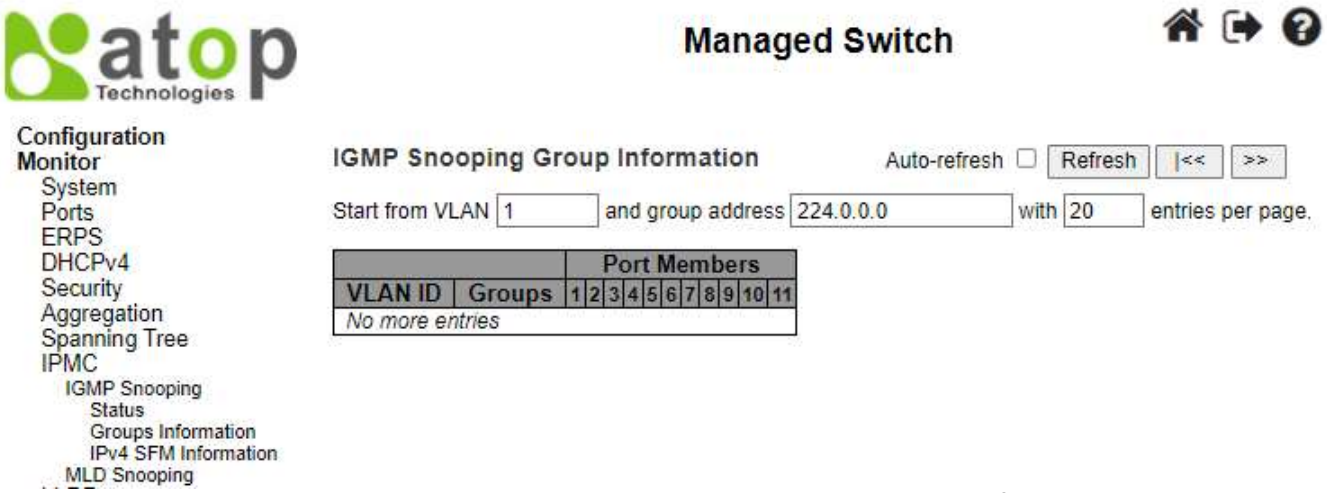


Figure 3.46 Webpage to Monitor IGMP Snooping Group Information

Table 3.39 Monitoring Descriptions of IGMP Snooping Group Information

Label	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

Check the Auto-refresh box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click Refresh button to refresh the displayed table starting from the input fields. Click |<< to update the table starting from the first entry in the MVR Channels (Groups) Information Table. Click >> to updates the table, starting with the entry after the last entry currently displayed.

3.8.1.3 IPv4 SFM Information

Entries in the IGMP SFM Information Table are shown on this page. The IGMP SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

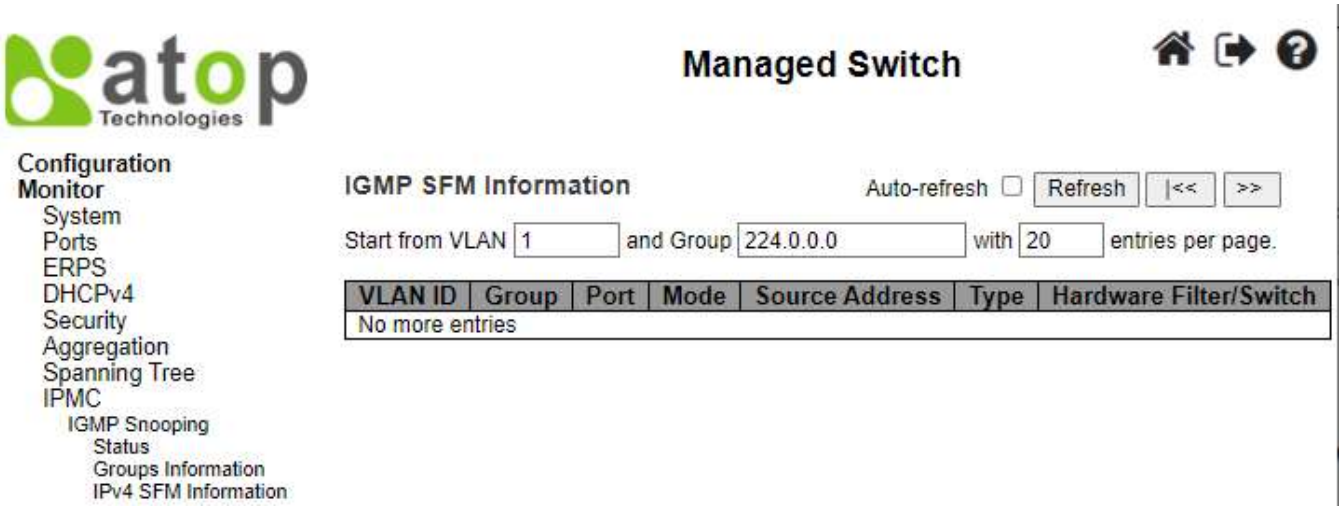


Figure 3.47 Webpage to Monitor IGMP SFM Information

Table 3.40 Monitoring Descriptions IGMP SFM Information

Label	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, the maximum number of IPv4 source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv4 address could be handled by chip or not.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the displayed table starting from the input fields. Click |<< to update the table starting from the first entry in the IGMP SFM Information Table. Click >> to update the table, starting with the entry after the last entry currently displayed

3.8.2 MLD Snooping

3.8.2.1 Status

This page provides MLD Snooping status.

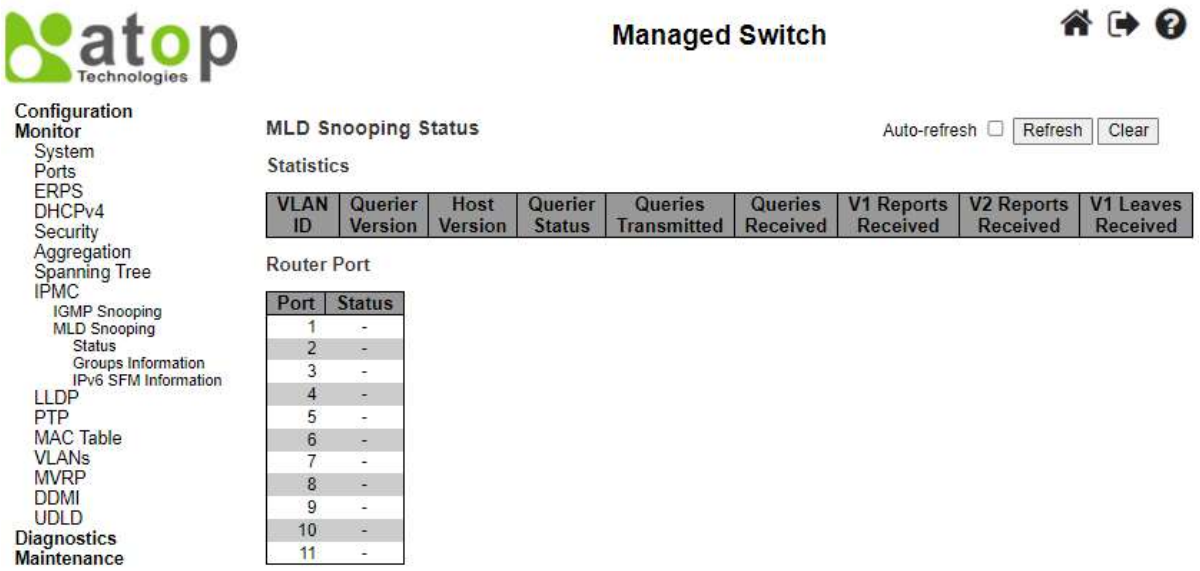


Figure 3.48 Webpage to Monitor MLD Snooping Status

Table 3.41 Monitoring Descriptions of MLD Snooping Status

Label	Description
VLAN ID	The VLAN ID of the entry.
Querier Version	Working Querier Version currently.
Host Version	Working Host Version currently.
Querier Status	Shows the Querier status is "ACTIVE" or "IDLE". "DISABLE" denotes the specific interface is administratively disabled.
Queries Transmitted	The number of Transmitted Queries.

Queries Received	The number of Received Queries.
V1 Reports Received	The number of Received V1 Reports.
V2 Reports Received	The number of Received V2 Reports. V1 Leaves Received
V1 Leaves Received	The number of Received V1 Leaves.
Router Port: Display which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or MLD querier. Static denotes the specific port is configured to be a router port. Dynamic denotes the specific port is learnt to be a router port. Both denote the specific port is configured or learnt to be a router port.	
Port	Switch port number.
Status	Indicate whether specific port is a router port or not.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately. Click **Clear button** to clear all Statistics counters.

3.8.2.2 Groups Information

Entries in the MLD Group Table are shown on this page. The MLD Group Table is sorted first by VLAN ID, and then by group.

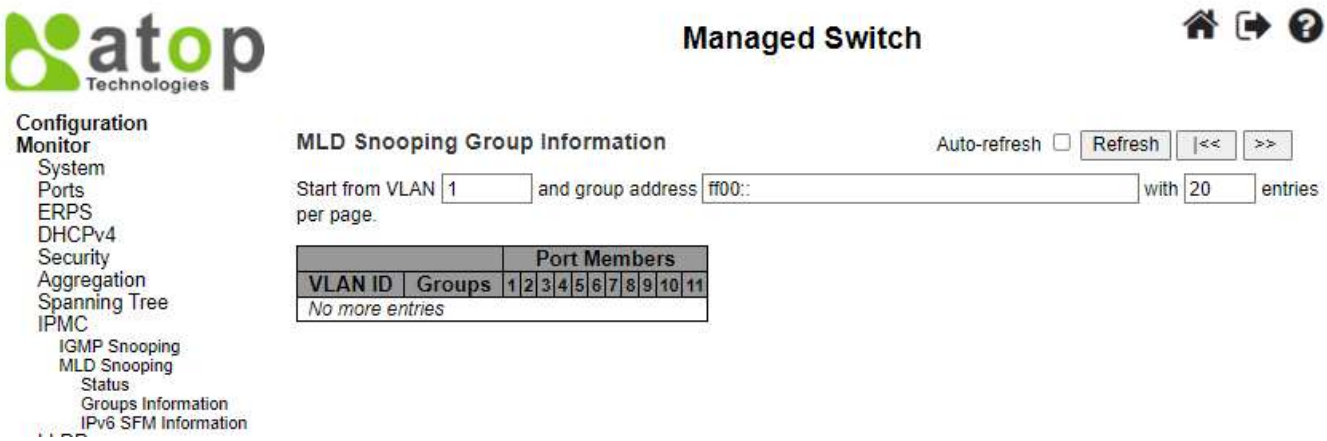


Figure 3.49 Webpage to Monitor MLD Snooping Group Information

Table 3.42 Monitoring Descriptions of MLD Snooping Group Information

Label	Description
VLAN ID	VLAN ID of the group.
Groups	Group address of the group displayed.
Port Members	Ports under this group.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the displayed table starting from the input fields. Click |<< to update the table starting from the first entry in the MLD Group Table. Click >> to update the table, starting with the entry after the last entry currently displayed

3.8.2.3 IPv6 SFM Information

Entries in the MLD SFM Information Table are shown on this page. The MLD SFM (Source-Filtered Multicast) Information Table also contains the SSM (Source-Specific Multicast) information. This table is sorted first by VLAN ID, then by group, and then by Port. Different source addresses belong to the same group are treated as single entry.

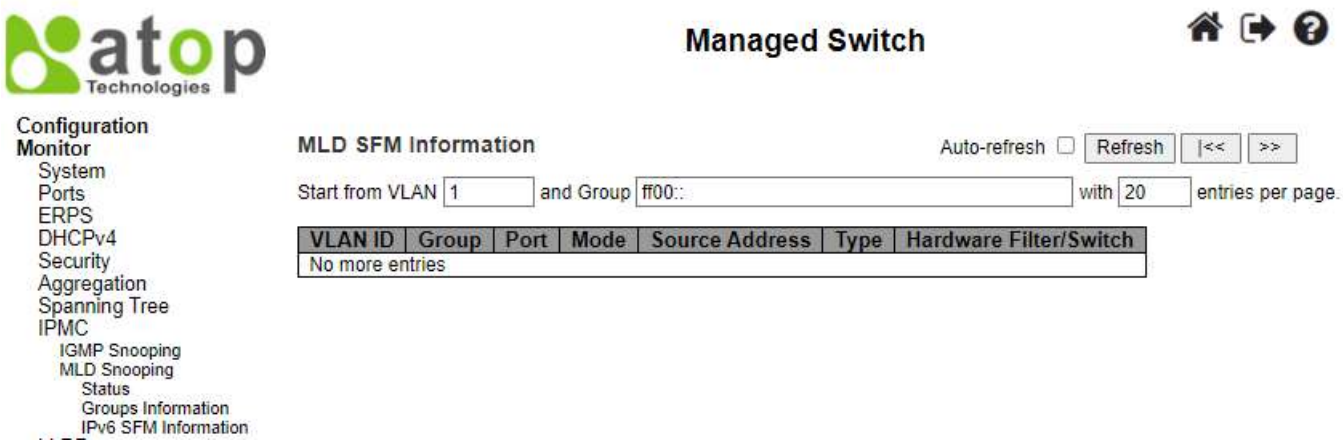


Figure 3.50 Webpage to Monitor

Table 3.43 Monitoring Descriptions of MLD SFM Information

Label	Description
VLAN ID	VLAN ID of the group.
Group	Group address of the group displayed.
Port	Switch port number.
Mode	Indicates the filtering mode maintained per (VLAN ID, port number, Group Address) basis. It can be either Include or Exclude.
Source Address	IP Address of the source. Currently, the maximum number of IPv6 source address for filtering (per group) is 8. When there is no any source filtering address, the text "None" is shown in the Source Address field.
Type	Indicates the Type. It can be either Allow or Deny.
Hardware Filter/Switch	Indicates whether data plane destined to the specific group address from the source IPv6 address could be handled by chip or not.

Check the Auto-refresh box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the displayed table starting from the input fields: Click |<< to update the table starting from the first entry in the MLD SFM Table. Click >> to update the table, starting with the entry after the last entry currently displayed

3.9 LLDP

3.9.1 Neighbors

This page provides a status overview for all LLDP neighbours. The displayed table contains a row for each interface on which an LLDP neighbour is detected. The columns hold the following information.

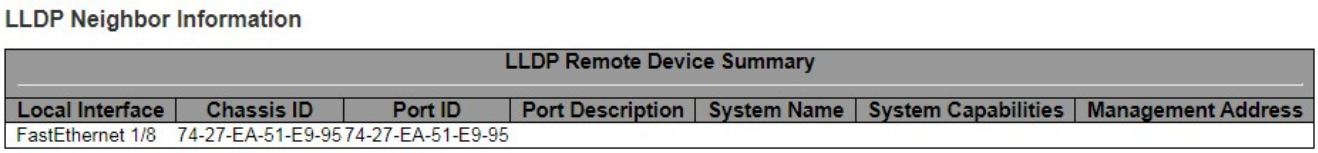


Figure 3.51 Webpage to Monitor LLDP Neighbour Information

Table 3.44 Monitoring Descriptions of LLDP Neighbour Information

Label	Description
Local Interface	The interface on which the LLDP frame was received.
Chassis ID	The identification of the neighbour's LLDP frames.
Port ID	The identification of the neighbour port.
Port Description	The port description advertised by the neighbour unit.
System Name	The name advertised by the neighbour unit.

Label	Description
System Capabilities	Describes the neighbour unit's capabilities. The possible capabilities are: 1. Other 2. Repeater 3. Bridge 4. WLAN Access Point 5. Router 6. Telephone 7. DOCSIS cable device 8. Station only 9. Reserved When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-).
Management Address	The neighbour unit's address that is used for higher layer entities to assist discovery by the network management. This could for instance hold the neighbour's IP address.

Check the Auto-refresh box to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh this page.

3.9.2 Port Statistics

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters are counters that refer to the whole switch, while local counters refer to per interface counters for the currently selected switch.

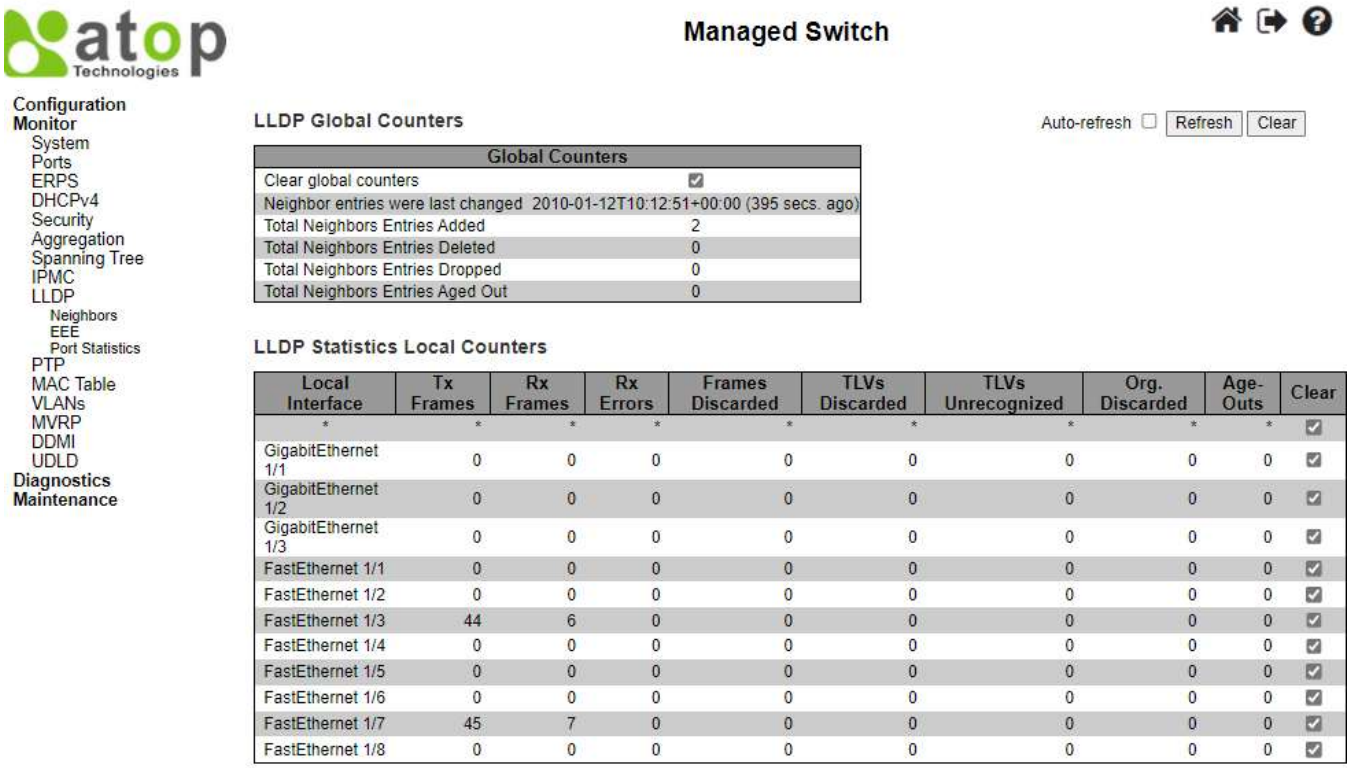


Figure 3.52 Webpage to Monitor LLDP Global and Statistics Local Counters

Table 3.45 Monitoring Descriptions of LLDP Global and Statistics Local Counters

Label	Description
LLDP Global Counters	
Clear global counters	If checked the global counters are cleared when Clear button is pressed.
Neighbor entries were last changed	Shows the time when the last entry was last deleted or added. It also shows the time elapsed since the last change was detected.
Total Neighbors Entries Added	Shows the number of new entries added since switch reboot.
Total Neighbors Entries Deleted	Shows the number of new entries deleted since switch reboot.
Total Neighbors Entries Dropped	Shows the number of LLDP frames dropped due to the entry table being full.

Label	Description
LLDP Global Counters	
Total Neighbors Entries Aged Out	Shows the number of entries deleted due to Time-To-Live expiring.
LLDP Statistics Local Counters	
Local Interface	The interface on which LLDP frames are received or transmitted.
Tx Frames	The number of LLDP frames transmitted on the interface.
Rx Frames	The number of LLDP frames received on the interface.
Rx Errors	The number of received LLDP frames containing some kind of error.
Frames Discarded	If a LLDP frame is received on an interface, and the switch's internal table has run full, the LLDP frame is counted and discarded. This situation is known as "Too Many Neighbours" in the LLDP standard. LLDP frames require a new entry in the table when the Chassis ID or Remote Port ID is not already contained within the table. Entries are removed from the table when a given interface's link is down, an LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (TLV is short for "Type Length Value"). If a TLV is malformed, it is counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value.
Org. Discarded	If LLDP frame is received with an organizationally TLV, but the TLV is not supported the TLV is discarded and counted.
Age-Outs	Each LLDP frame contains information about how long time the LLDP information is valid (age out time). If no new LLDP frame is received within the age out time, the LLDP information is removed, and the Age-Out counter is incremented.
Clear	If checked the counters for the specific interface are cleared when Clear button is pressed.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately. Click **Clear button** to clear all Statistics counters.

3.10 PTP

3.10.1 PTP

This page allows the user to inspect the current PTP clock settings.

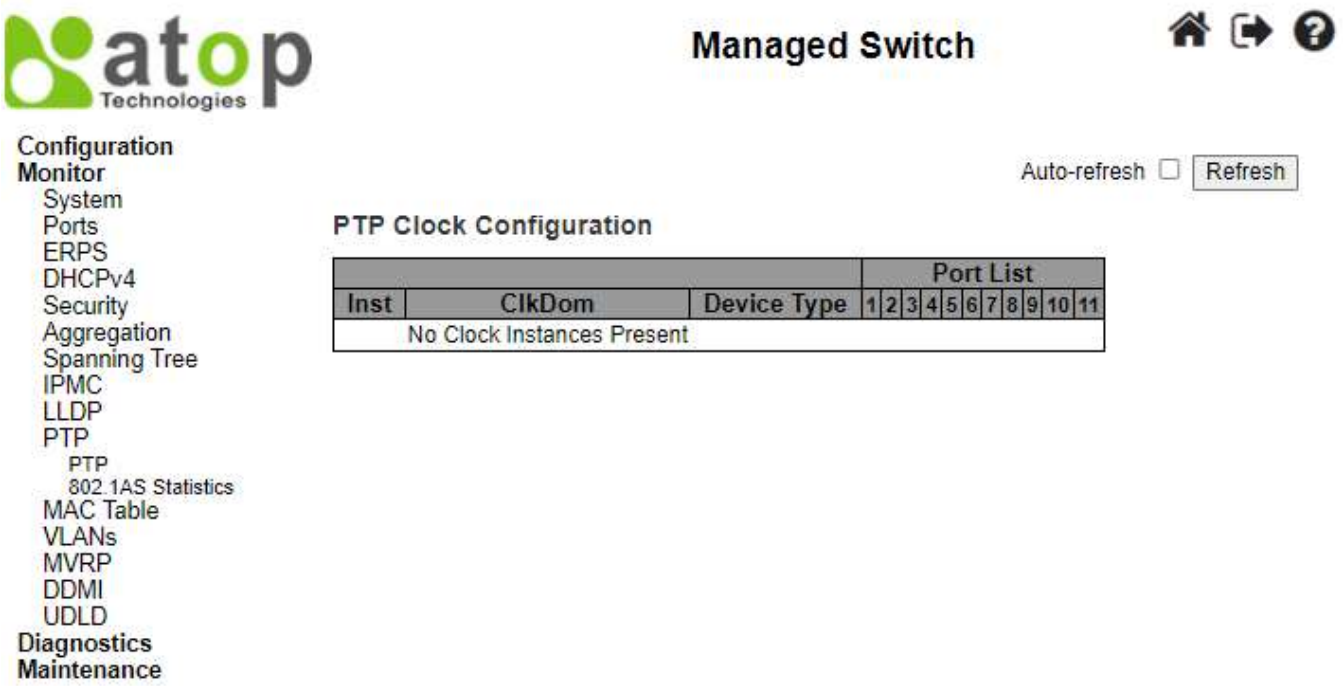


Figure 3.53 Webpage to Monitor PTP External Clock Mode and Clock Configuration

Table 3.46 Monitoring Descriptions of PTP External Clock Mode and Clock Configuration

Label	Description
PTP Clock Configuration	
Inst	Indicates the Instance of a particular Clock Instance [0..3]. Click on the Clock Instance number to monitor the Clock details.
ClkDom	Indicates the Clock domain used by the Instance of a particular Clock Instance [0..3].
Device Type	Indicates the Type of the Clock Instance. There are five Device Types. 1. Ord-Bound - Clock's Device Type is Ordinary-Boundary Clock. 2. P2p Transp - Clock's Device Type is Peer to Peer Transparent Clock. 3. E2e Transp - Clock's Device Type is End to End Transparent Clock. 4. Master Only - Clock's Device Type is Master Only. 5. Slave Only - Clock's Device Type is Slave Only.
Port List	Shows the ports configured for that Clock Instance.

Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately

3.10.2 802.1AS Statistics

This page allows the user to inspect the current PTP configurations, and possibly change them as well.

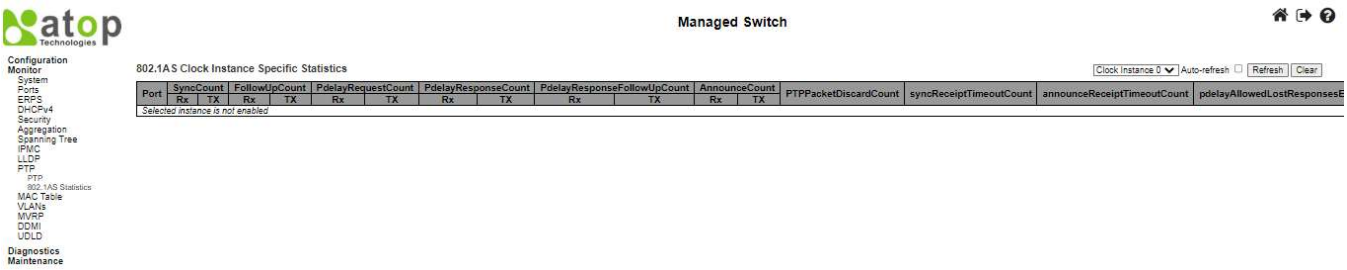


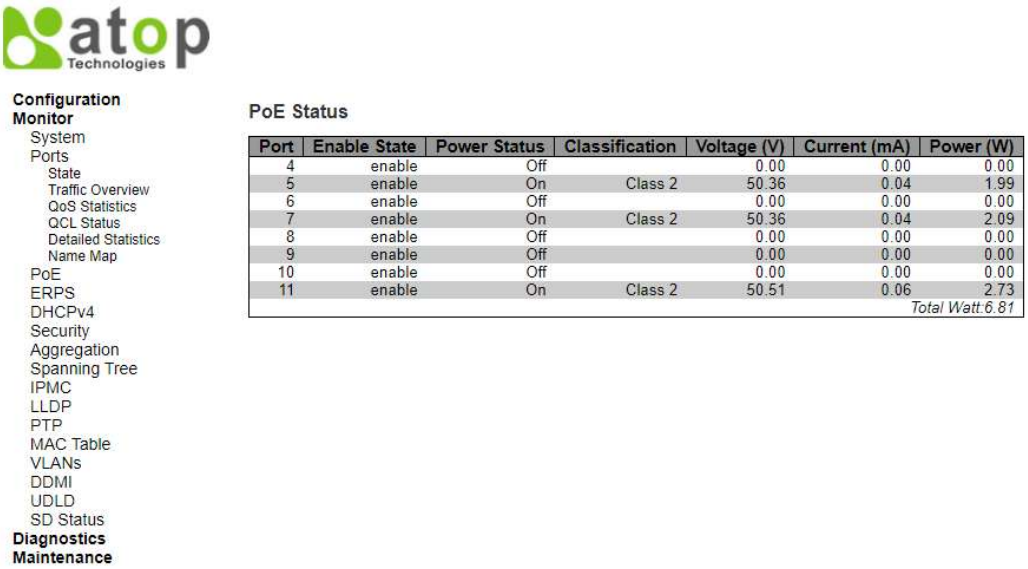
Figure 3.54 Webpage to Monitor 802.1AS Statistics

Table 3.47 Monitoring Descriptions of 802.1AS Statistics

Label	Description
SyncCount	A counter that increments every time when synchronization information is received.
FollowUpCount	A counter that increments every time when a Follow Up message is received.
PdelayRequestCount	A counter that increments every time when a Pdelay_Req message is received.
PdelayResponseCount	A counter that increments every time when a Pdelay_Resp message is received.
PdelayResponseFollowUpCount	A counter that increments every time when a Pdelay_Resp_Follow_Up message is received.
AnnounceCount	A counter that increments every time when an Announce message is received.
PTPPacketDiscardCount	A counter that increments every time when announce receipt timeout occurs.
pdelayAllowedLostResponsesExceededCount	A counter that increments every time the value of the variable lostResponses exceeds the value of the variable allowedLostResponses.
802.1As Transmit Counters	
SyncCount	A counter that increments every time synchronization information is transmitted.
FollowUpCount	A counter that increments every time a Follow_Up message is transmitted.
PdelayRequestCount	A counter that increments every time a Pdelay_Resp message is transmitted.
PdelayResponseFollowUpCount	A counter that increments every time a Pdelay_Resp_Follow_Up message is transmitted.
AnnounceCount	A counter that increments every time an Announce message is transmitted.
PTPPacketDiscardCount	A counter that increments every time when a PTP message is discarded.
syncReceiptTimeoutCount	A counter that increments every time when sync receipt timeout occurs.
announceReceiptTimeoutCount	A counter that increments every time when announce receipt timeout occurs.
pdelayAllowedLostResponsesExceededCount	A counter that increments everytime the value of the variable lostResponses exceeds the value of the variable allowedLostResponses.

3.11 PoE

This webpage summarizes the status of each PoE port. For example, in Figure 3.17, Port5, 7 and 11 were enabled and are supplying power to a Class 2 Powered Device (PD) indicated under the Classification column. The PD device is rated at 50V and 0.04~0.06mA. The total power consumption for this PD is 6.81W. To check the status of the PoE port, please click on the Refresh button. Table 3.11 provides descriptions of each column in the table of PoE Status.



Port	Enable State	Power Status	Classification	Voltage (V)	Current (mA)	Power (W)
4	enable	Off		0.00	0.00	0.00
5	enable	On	Class 2	50.36	0.04	1.99
6	enable	Off		0.00	0.00	0.00
7	enable	On	Class 2	50.36	0.04	2.09
8	enable	Off		0.00	0.00	0.00
9	enable	Off		0.00	0.00	0.00
10	enable	Off		0.00	0.00	0.00
11	enable	On	Class 2	50.51	0.06	2.73

Figure 3.55 Webpage to PoE Status

Table 3.48 Monitoring Descriptions of QoS Control List Status

Label	Description
Port	On when there is a power device on the other end or Off when there is no PD on the other end.
Enable State	Enable or Disable PoE function.
Power Status	On when there is a power device on the other end or Off when there is no PD on the other end.
Classification	Display the classification of power device on the other end.
Voltage (V)	Display the voltage supplied to this port in Volts.
Current (mA)	Display the current supplied to this port in milli-Amperes.
Power (W)	Display the power supplied to this port in Watts.
Total Watt	Display the power supplied to all ports in Watts.

3.12 MAC Table

Entries in the MAC Table are shown on this page. The MAC Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Navigating through the MAC table, users will realize the followings. Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table. The "Start from MAC address" and "VLAN" input fields allow the user to select the starting point in the MAC Table. Clicking the **Refresh button** will update the displayed table starting from that or the closest next MAC Table match. In addition, the two input fields will - upon a **Refresh button** click - assume the value of the first displayed entry, allowing for continuous refresh with the same start address. The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the |<< button to start over.

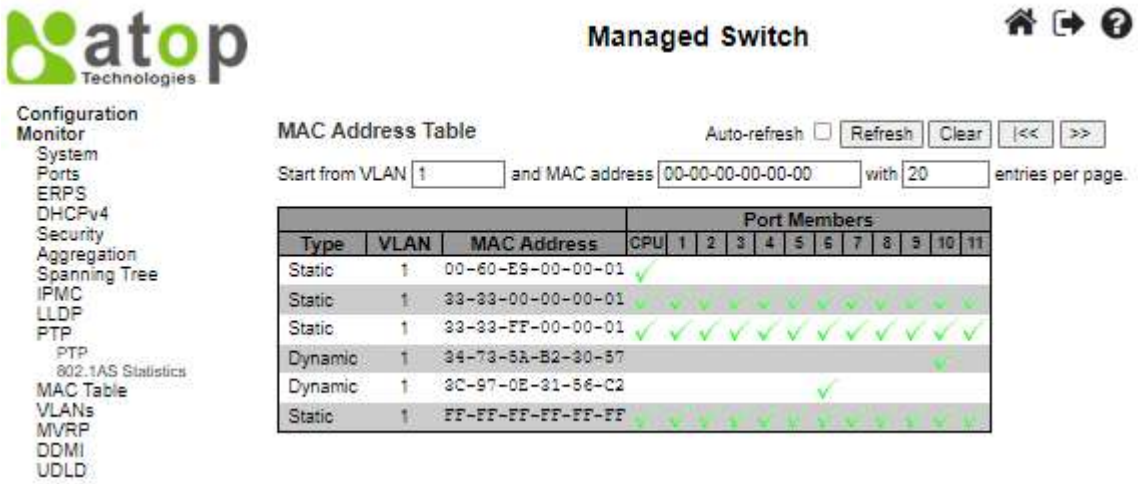


Figure 3.56 Webpage to Monitor MAC Address Table

Table 3.49 Monitoring Descriptions of MAC Address Table

Label	Description
Type	Indicates whether the entry is a static or a dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.

3.13 VLANs

3.13.1 Membership

This page provides an overview of membership status of VLAN users.

The following describes how to navigate the VLAN Membership Status page. Each page shows up to 99 entries from the VLAN table (default being 20), selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table. The "VLAN" input field allows the user to select the starting point in the VLAN Table.

Clicking the **Refresh button** will update the displayed table starting from that or the closest next VLAN Table match. The >> will use the last entry of the currently displayed VLAN entry as a basis for the next lookup. When the end is reached, the text "No data exists for the selected user" is shown in the table. Use the |<< button to start over.

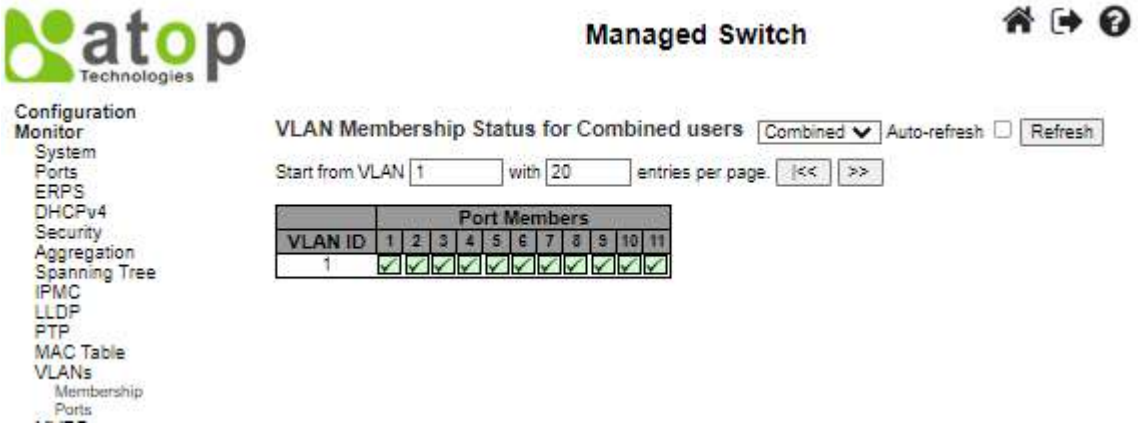


Figure 3.57 Webpage to Monitor VLAN Membership Status for Combined Users

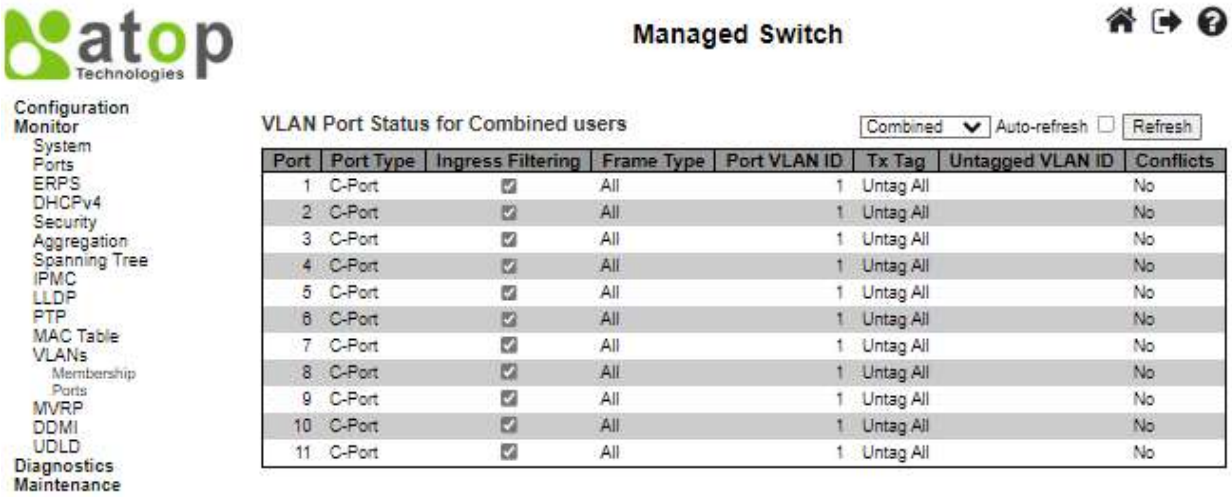
Table 3.50 Monitoring Descriptions of VLAN Membership Status for Combined Users

Label	Description
VLAN User	Various internal software modules may use VLAN services to configure VLAN memberships on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware.
VLAN ID	VLAN ID for which the Port members are displayed.
Port Members	A row of check boxes for each port is displayed for each VLAN ID. If a port is included in a VLAN, the following image will be displayed: ☑. If a port is in the forbidden port list, the following image will be displayed: ☒ . If a port is in the forbidden port list and at the same time attempted included in the VLAN, the following image will be displayed: ☒ . The port will not be a member of the VLAN in this case.

Click Combined Buttons to select VLAN Users from this drop-down list. Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately.

3.13.2 Ports

This page provides VLAN Port Status.



Port	Port Type	Ingress Filtering	Frame Type	Port VLAN ID	Tx Tag	Untagged VLAN ID	Conflicts
1	C-Port	☑	All	1	Untag All		No
2	C-Port	☑	All	1	Untag All		No
3	C-Port	☑	All	1	Untag All		No
4	C-Port	☑	All	1	Untag All		No
5	C-Port	☑	All	1	Untag All		No
6	C-Port	☑	All	1	Untag All		No
7	C-Port	☑	All	1	Untag All		No
8	C-Port	☑	All	1	Untag All		No
9	C-Port	☑	All	1	Untag All		No
10	C-Port	☑	All	1	Untag All		No
11	C-Port	☑	All	1	Untag All		No

Figure 3.58 Webpage to Monitor VLAN Port Status for Combined Users

Table 3.51 Monitoring Descriptions of VLAN Port Status for Combined Users

Label	Description
VLAN User	Various internal software modules may use VLAN services to configure VLAN port configuration on the fly. The drop-down list on the right allows for selecting between showing VLAN memberships as configured by an administrator (Admin) or as configured by one of these internal software modules. The "Combined" entry will show a combination of the administrator and internal software modules configuration, and basically reflects what is actually configured in hardware. If a given software modules hasn't overridden any of the port settings, the text "No data exists for the selected user" is shown in the table.
Port	The logical port for the settings contained in the same row.
Port Type	Shows the port type (Unaware, C-Port, S-Port, S-Custom-Port.) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
Ingress Filtering	Shows whether a given user wants ingress filtering enabled or not. The field is empty if not overridden by the selected user.

Label	Description
Frame Type	Shows the acceptable frame types (All, Tagged, Untagged) that a given user wants to configure on the port. The field is empty if not overridden by the selected user.
Port VLAN ID	Shows the Port VLAN ID (PVID) that a given user wants the port to have. The field is empty if not overridden by the selected user.
Tx Tag	Shows the Tx Tag requirements (Tag All, Tag PVID, Tag UVID, Untag All, Untag PVID, Untag UVID) that a given user has on a port. The field is empty if not overridden by the selected user.
Untagged VLAN ID	If Tx Tag is overridden by the selected user and is set to Tag or Untag UVID, then this field will show the VLAN ID the user wants to tag or untag on egress. The field is empty if not overridden by the selected user.
Conflicts	Two users may have conflicting requirements to a port's configuration. For instance, one user may require all frames to be tagged on egress while another requires all frames to be untagged on egress. Since both users cannot win, this gives rise to a conflict, which is solved in a prioritized way. The Administrator has the least priority. Other software modules are prioritized according to their position in the drop-down list: The higher in the list, the higher priority. If conflicts exist, it will be displayed as "Yes" for the "Combined" user and the offending software module. The "Combined" user reflects what is actually configured in hardware.

Click Combined Buttons to select VLAN Users from this drop-down list. Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately

3.14 DDMI

3.14.1 Overview

Display DDMI overview information on this page.

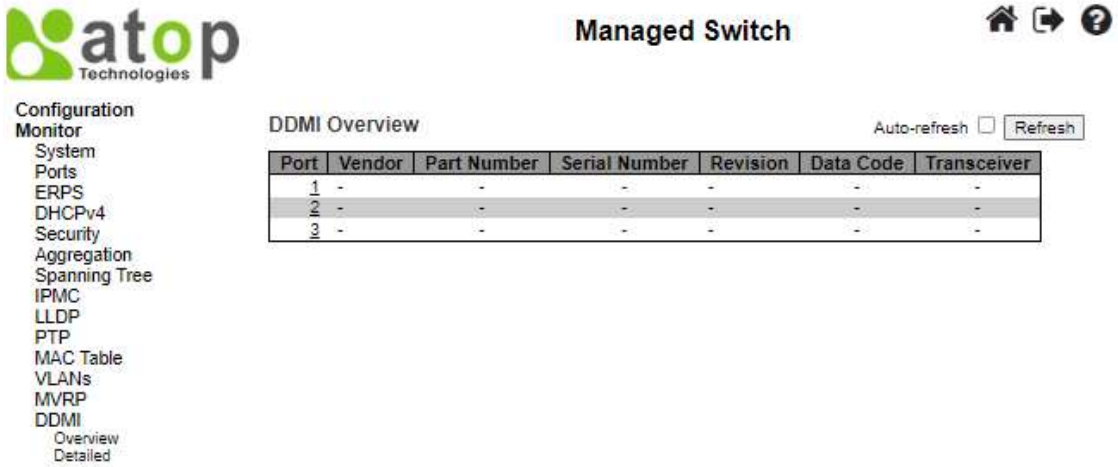


Figure 3.59 Webpage to Monitor DDMI Overview

Table 3.52 Monitoring Descriptions of DDMI Overview

Label	Description
Port	DDMI port.
Vendor	Indicates Vendor name SFP vendor name.
Part Number	Indicates Vendor PN Part number provided by SFP vendor.
Serial Number	Indicates Vendor SN Serial number provided by vendor.

Revision	Indicates Vendor rev Revision level for part number provided by vendor.
Data Code	Indicates Date code Vendor's manufacturing date code.
Transceiver	Indicates Transceiver compatibility.

3.14.2 Detailed

Display DDMI detailed information on this page. DDMI is an acronym for Digital Diagnostics Monitoring Interface. It provides an enhanced digital diagnostic monitoring interface for optical transceivers which allows real time access to device operating parameters.

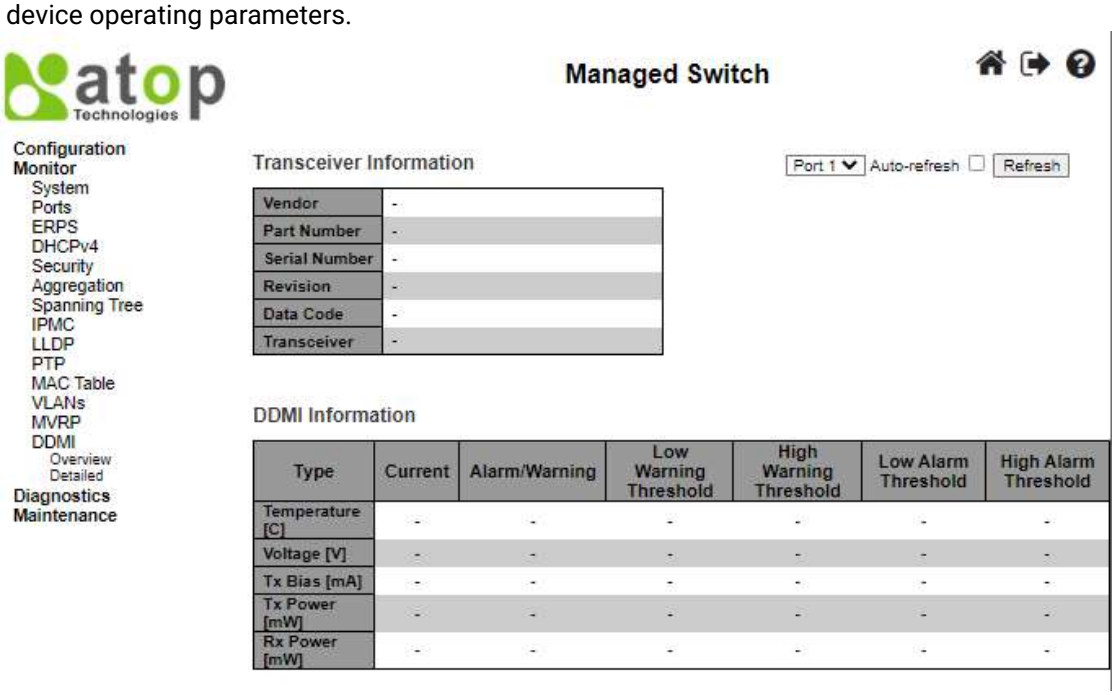


Figure 3.60 Webpage to Monitor DDMI Detailed

Table 3.53 Monitoring Descriptions of DDMI Detailed

Label	Description
Transceiver Information	
Vendor	Indicates SFP vendor name.
Part Number	Indicates part number provided by SFP vendor.
Serial Number	Indicates serial number provided by SFP vendor.
Revision	Indicates revision level for part number provided by SFP vendor.
Data Code	Indicates vendor's manufacturing date code.
Transceiver	Indicates SFP transceiver compatibility.
DDMI Information	
Current	The current value of temperature, voltage, Tx bias, Tx power, and Rx power.
Alarm/Warning	Indicates whether there is an alarm or warning.
Low Warning Threshold	The low warning threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.
High Warning Threshold	The high warning threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.
Low Alarm Threshold	The low alarm threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.
High Alarm Threshold	The high alarm threshold value of temperature, voltage, Tx bias, Tx power, and Rx power.

3.15 UDLD

This page displays the **UDLD** status of the ports. UDLD is an acronym for **U**ni **D**irectional **L**ink **D**etection. UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. It detects the existence of unidirectional links. Its functionality is to provide mechanisms useful for detecting one-way connections before they create a loop or other protocol malfunction. RFC 5171 specifies a way at data link layer to detect Uni directional link.

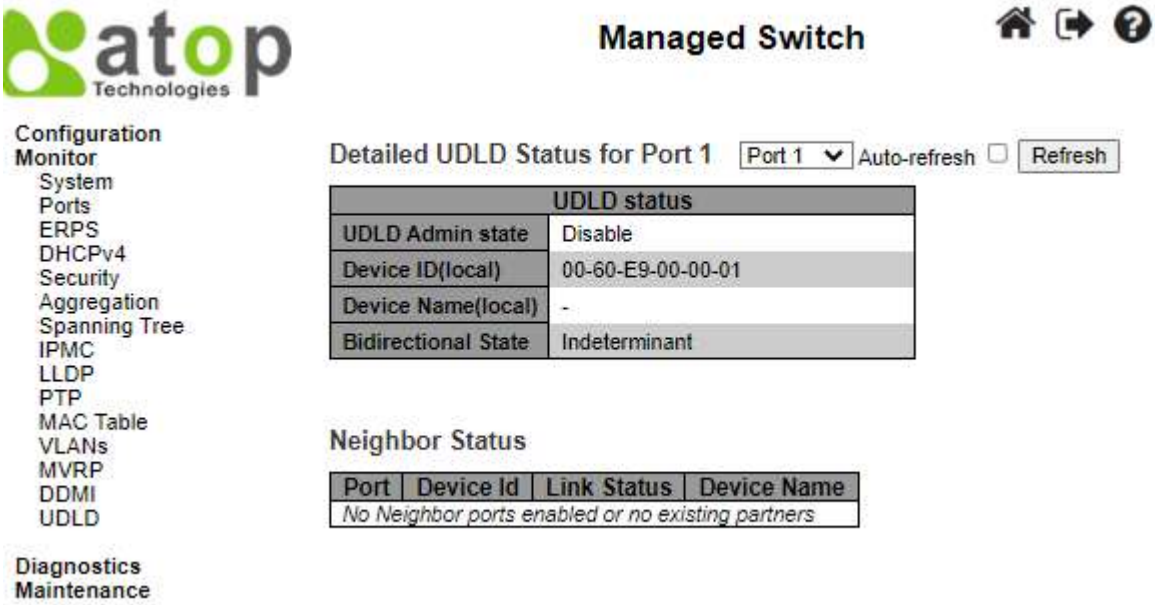


Figure 3.61 Webpage to Monitor Detailed UDLD Status for Port 1 and Neighbour Status

Table 3.54 Monitoring Descriptions of Detailed UDLD Status for Port 1 and Neighbour Status

Label	Description
Detailed UDLD Status	
UDLD Admin State	The current port state of the logical port. Enabled if any of state (Normal, Aggressive) is Enabled.
Device ID (local)	The ID of Device.
Device Name(local)	Name of the Device.
Bidirectional State	The current state of the port.
Neighbour Status	
Port	The current port of neighbour device.
Device ID	The current ID of neighbour device.
Link Status	The current link status of neighbour port.
Device Name	Name of the Neighbour Device.

The port select box Port 1 determines which port is affected by clicking the buttons. Check the **Auto-refresh box** to refresh the page automatically. Automatic refresh occurs every 3 seconds. Click **Refresh button** to refresh the page immediately

4 Diagnostics

The **Diagnostics** menu is a collection of software tools that can be used to check the network connection for your managed switch. The submenus under the **Diagnostics** menu are shown in Figure 4.1. The available network diagnostic tools are **Ping (IPv4)**, **Ping (IPv6)**, **Traceroute (IPv4)**, and **Traceroute (IPv6)**.

Figure 4.1 Diagnostics Menu

4.1 Ping (IPv4)

Atop's managed switch provides a network tool called **Ping** for testing network connectivity in this subsection. Ping is a network diagnostic utility for testing reachability between a destination device and the managed switch. It utilizes ICMP (Internet Control Message Protocol) packet to troubleshoot IP connectivity issues. Note that this utility is only for IPv4 address. The Ping utility for IPv6 will be provided in the next subsection. Figure 4.2 shows the user interface for using the Ping command for IP version 4. The user must at least enter the **Hostname or IP Address** for the destination to be checked with Ping tool. Description of each parameter for Ping tool is summarized in Table 4.1.

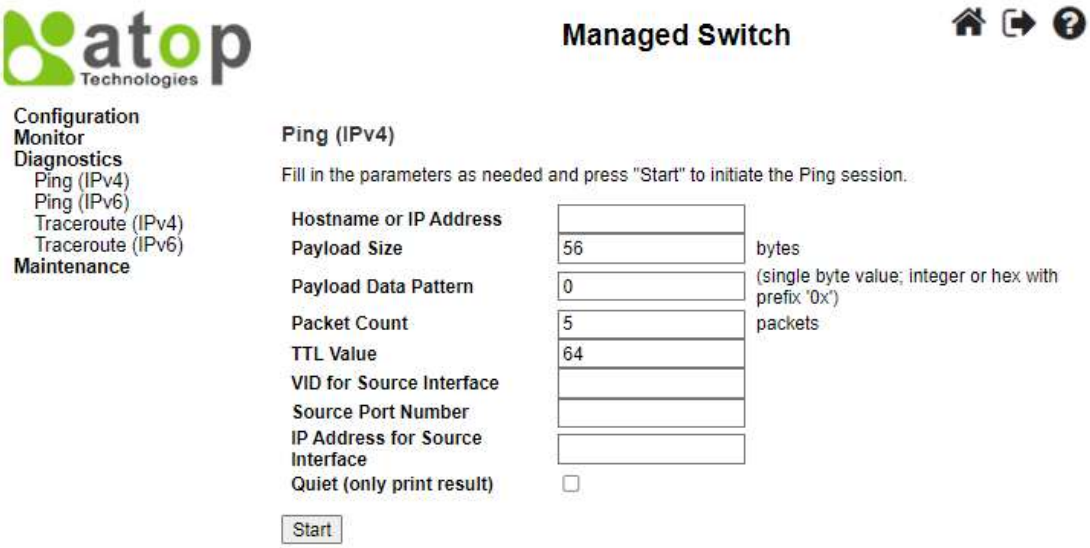


Figure 4.2 Diagnostics Webpage using IPv4 Ping

Table 4.1 Descriptions of Options for Ping (IPv4) Diagnostic Tool

Label	Description
Hostname or IP Address	The address of the destination host, either as a symbolic hostname or an IP Address.

Label	Description
Payload Size	Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.
Payload Data Pattern	Determines the data pattern used in the ICMP data payload in single byte value. The default value is 0. The valid range is 0-255.
Packet Count	Determines the number of PING requests (ICMP packets) to be sent to the destination. The default value is 5. The valid range is 1-60.
TTL Value	Determines the Time-To-Live (TTL) field value in the IPv4 header. This is the integer value to be set for the number of hops that the ping packet can traverse the network. If TTL reaches zero (deducted by a host after it reached a host), the ping packet will be discarded. The default value is 64. The valid range is 1-255.
VID for source Interface	This field can be used to force the Ping test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Source Port Number	This field can be used to force the Ping test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.
IP Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Quiet (only print result)	Checking this option will enable the quiet mode which only print the ping's final results without the result of each ping request.

After the user enters an IP address or a domain name into the field to verify network connectivity. Click **Start** button to run the ping tool. After you press **Start**, ICMP packets are transmitted, and the sequence number and round-trip-time are displayed upon reception of a reply. The amount of data received inside of an IP packet of type ICMP ECHO_REPLY will always be 8 bytes more than the requested payload data size (the difference is the ICMP header). The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

An example of successful ping to an IPv4 address is shown in Figure 4.3 while an example of a failure ping is depicted in Figure 4.4. Note that the user can initiate another ping command by clicking the **New Ping** button at the end of the **Ping (IPv4) Output** webpage.

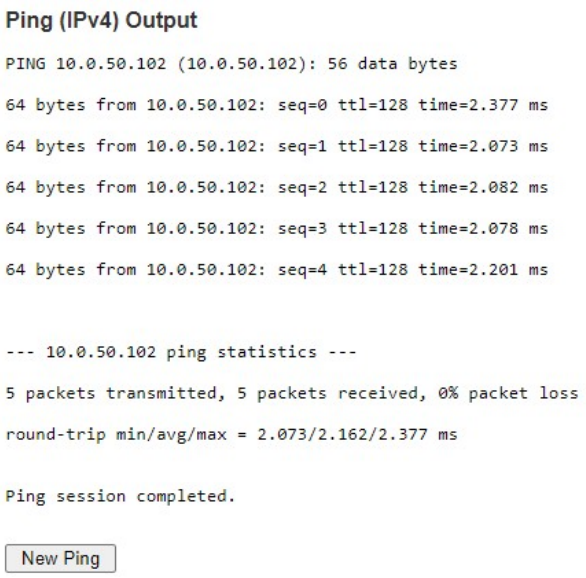


Figure 4.3 Result of successful IPv4 ping

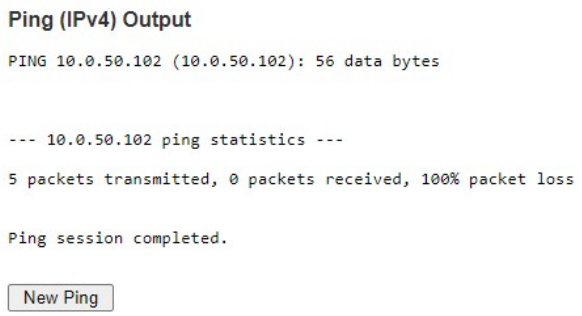


Figure 4.4 Result of failure IPv4 ping

4.2 Ping (IPv6)

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues. The user can enter an IP address or a domain name into the Hostname or IP Address field to verify network connectivity for IP version 6 network as shown in Figure 4.5. After entering the IP address or hostname, click **Start** button to run the Ping (IPv6) function. An example of successful ping result is shown in Figure 4.6 while a failure ping result is depicted in Figure 4.6. Note that the user can initiate another ping command by clicking the **New Ping** button at the end of the Ping (IPv6) Output webpage. Description of each parameter for Ping (IPv6) tool is summarized in Table 4.2

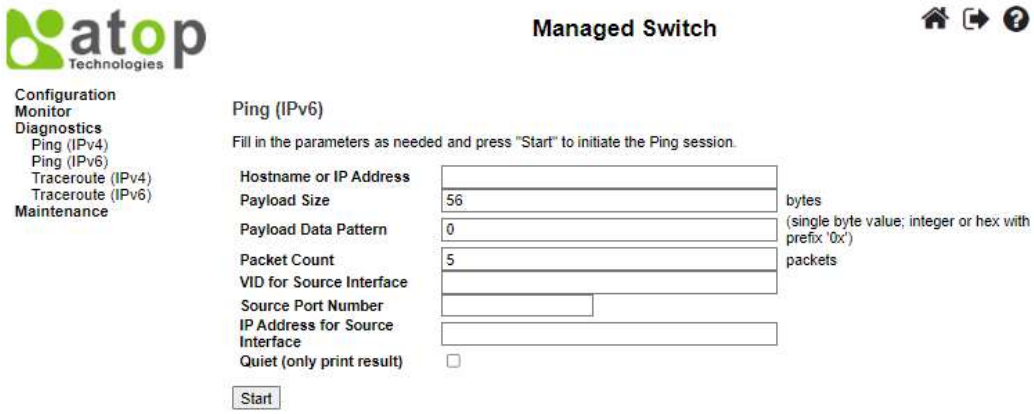


Figure 4.5 Diagnostics Webpage using IPv6 Ping

Ping (IPv6) Output

```
PING fe80::c0a3:98e6:54b3:c9fa (fe80::c0a3:98e6:54b3:c9fa): 56 data bytes
64 bytes from fe80::c0a3:98e6:54b3:c9fa: seq=0 ttl=128 time=6.678 ms
64 bytes from fe80::c0a3:98e6:54b3:c9fa: seq=1 ttl=128 time=2.200 ms
64 bytes from fe80::c0a3:98e6:54b3:c9fa: seq=2 ttl=128 time=2.216 ms
64 bytes from fe80::c0a3:98e6:54b3:c9fa: seq=3 ttl=128 time=2.255 ms
64 bytes from fe80::c0a3:98e6:54b3:c9fa: seq=4 ttl=128 time=3.134 ms

--- fe80::c0a3:98e6:54b3:c9fa ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.200/3.296/6.678 ms

Ping session completed.
```

New Ping

Figure 4.6 Result of successful IPv6 ping

Ping (IPv6) Output

```
PING fe80::c0a3:98e6:54b3:c9fb (fe80::c0a3:98e6:54b3:c9fb): 56 data bytes

--- fe80::c0a3:98e6:54b3:c9fb ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss

Ping session completed.
```

New Ping

Figure 4.7 Result of failure IPv6 ping

Table 4.2 Descriptions of Options for Ping (IPv6) Diagnostic Tool

Label	Description
Hostname or IP Address	The address of the destination host, either as a symbolic hostname or an IP Address.
Payload Size	Determines the size of the ICMP data payload in bytes (excluding the size of Ethernet, IP and ICMP headers). The default value is 56 bytes. The valid range is 2-1452 bytes.
Payload Data Pattern	Determines the data pattern used in the ICMP data payload in single byte value. The default value is 0. The valid range is 0-255.
Packet Count	Determines the number of PING requests (ICMP packets) to be sent to the destination. The default value is 5. The valid range is 1-60.
VID for source Interface	This field can be used to force the Ping test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Source Port Number	This field can be used to force the Ping test to use a specific local interface with the specified port number as the source interface. The specified port must be configured with a suitable IP address. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the Source Port Number or the IP Address for the source interface.
IP Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration.

Label	Description
	Note: You may only specify either the VID or the IP Address for the source interface.
Quiet (only print result)	Checking this option will enable the quiet mode which only print the ping's final results without the result of each ping request.

4.3 Traceroute (IPv4)

Traceroute (IPv4) is another diagnostic tool that allows the user to check the path or route that packets take from the managed switch to a destination host or IP address. This tool could provide information about host or gateway along the path to the specified destination. It can measure transit delays of packets across the IPv4 network. Figure 4.8 shows the webpage for **Traceroute (IPv4)** tool on the managed switch. Table 4.3 provides brief descriptions of all parameters on the webpage. The only required parameter to start the **Traceroute (IPv4)** is the **Hostname or IP Address**. An example of traceroute result is shown in Figure 4.9. Note that the user can initiate another traceroute command by clicking the **New Traceroute** button at the end of the **Traceroute (IPv4) Output** webpage.

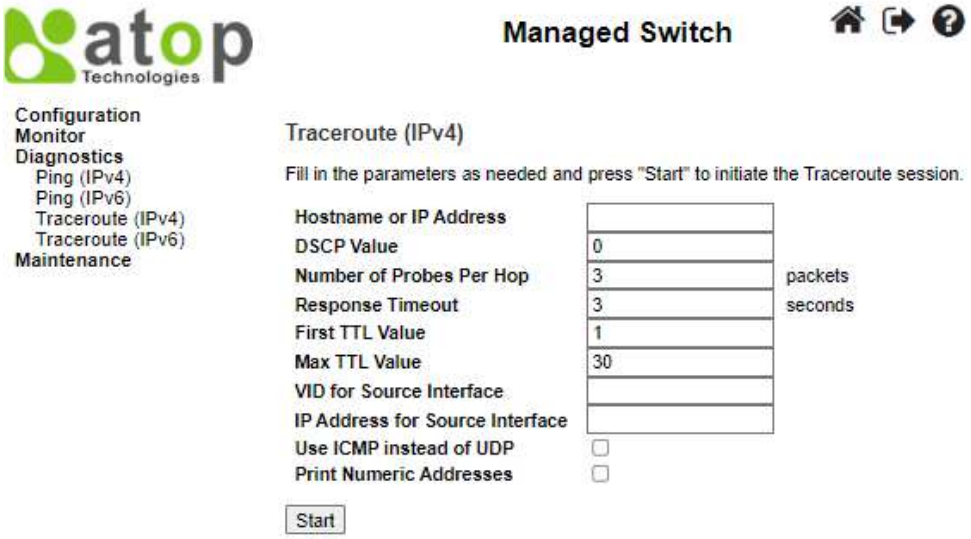


Figure 4.8 Diagnostics Webpage using IPv4 Traceroute

Table 4.3 Description of each parameter for Traceroute (IPv4)

Label	Description
Hostname or IP Address	Specifies the hostname or IP Address of the destination
DSCP Value	Specifies the DSCP (DiffServ Code Point) priority (value) in packets. The value is an integer that has a range from 0 to 63.
Number of Probes Per Hop	Specifies the number of probe packets sent for each hop which is the number of queries per intermediate host or gateway. The default value is 3 packets. The valid range is 1 – 60.
Response Timeout	Specifies the timeout for the response message or ICMP echo reply after an ICMP echo request message is sent to an intermediate host or gateway. This is the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1 – 86400.
First TTL Value	Specifies the initial Time to Live (TTL) value. This is a field in the IPv4 header in the first packet sent. The default value is 1. The valid range is 1 – 30.
Max TTL Value	Specifies the maximum number of hops traceroute will try to probe. If this value is reached before the specified remote host is reached, the test stops. The default value is 30. The valid range is 1 – 255.
VID for source Interface	This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration.

Label	Description
	Note: You may only specify either the VID or the IP Address for the source interface.
IP Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Use ICMP instead of UDP	By default, the traceroute command will use UDP datagrams. Selecting this option forces it to use ICMP ECHO packets instead.
Print Numeric Addresses	By default, the traceroute command will print out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

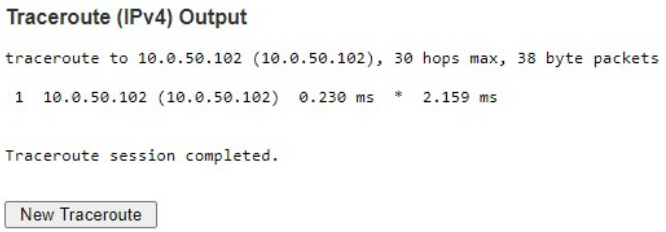


Figure 4.9 Example of traceroute (IPv4) output

4.4 Traceroute (IPv6)

Traceroute (IPv6) is another diagnostic tool that allows the user to check the path or route that packets take from the managed switch to a destination host or IP address in IP version 6 network. This tool could provide information about host or gateway along the path to the specified destination. It can measure transit delays of packets across the IPv6 network. Figure 4.10 shows the webpage for **Traceroute (IPv6)** tool on the managed switch. Table 4.4 provides brief descriptions of all parameters on this webpage.

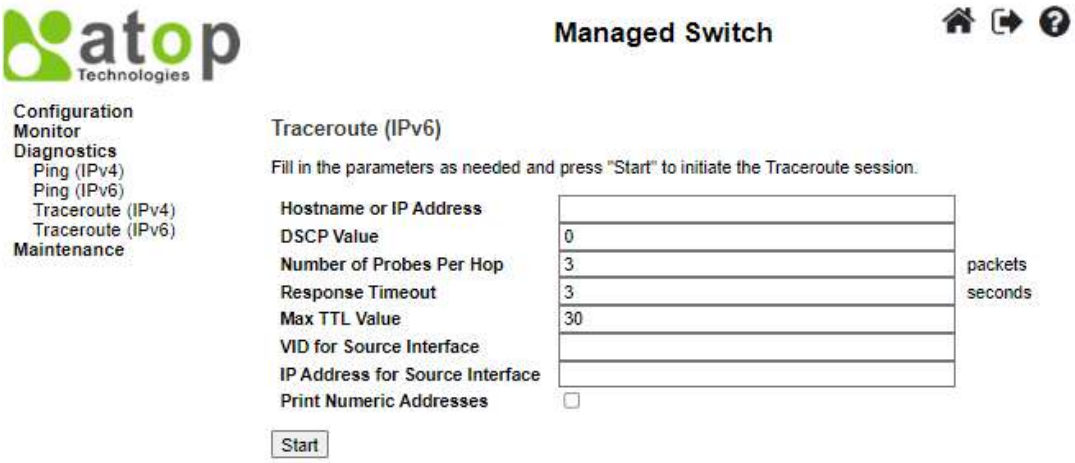


Figure 4.10 Diagnostics Webpage using IPv6 Traceroute

Table 4.4 Description of each parameter for Traceroute (IPv6)

Label	Description
Hostname or IP Address	Specifies the hostname or IP Address of the destination

Label	Description
DSCP Value	Specifies the DSCP (DiffServ Code Point) priority in packets. The value is an integer that has a range from 0 to 255.
Number of Probes Per Hop	Specifies the number of probe packets sent for each hop which is the number of queries per intermediate host or gateway. The default value is 3 packets. The valid range is 1 – 60.
Response Timeout	Specifies the timeout for the response message or ICMP echo reply after an ICMP echo request message is sent to an intermediate host or gateway. Determines the number of seconds to wait for a reply to a sent request. The default number is 3. The valid range is 1- 86400.
Max TTL Value	Specifies the maximum number of hops traceroute will try to probe. If this value is reached before the specified remote host is reached, the test stops. The default number is 255. The valid range is 1-255.
VID for source Interface	This field can be used to force the test to use a specific local VLAN interface as the source interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
IP Address for Source Interface	This field can be used to force the test to use a specific local interface with the specified IP address as the source interface. The specified IP address must be configured on a local interface. Leave this field empty for automatic selection based on routing configuration. Note: You may only specify either the VID or the IP Address for the source interface.
Print Numeric Addresses	By default, the traceroute command will print out hop information using a reverse DNS lookup for the acquired host IP addresses. This may slow down the display if the DNS information is not available. Selecting this option will prevent the reverse DNS lookup and force the traceroute command to print numeric IP addresses instead.

5 Maintenance

Maintenance menu is the last main menu on the WebUI on the RHG9728 Industrial Managed Ethernet Switch. Figure 5.1 shows all submenus under the **Maintenance** menu. Under this menu, the user can restart the device through the WebUI, reset the configuration of the device to the original factory default settings, upload new firmware image to update the device, and manage the configuration of the device. The following sections will describe each submenu under the **Maintenance** menu.

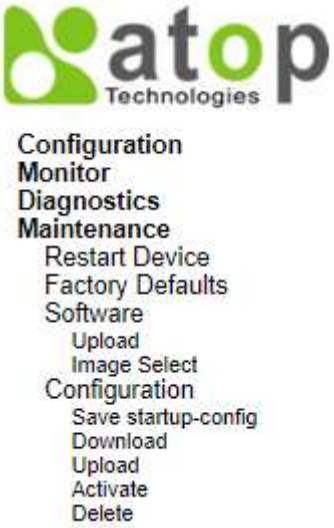


Figure 5.1 Maintenance Menu

5.1 Restart Device

To restart the managed switch (or device) through the WebUI, the user can select the **Maintenance→Restart Device** menu. The **Restart Device** webpage is showed in Figure 5.2. The user can click on the **Yes** button to restart the device. During the restarting process, the webpage will be displaying the progress of the restarting operation as shown in Figure 5.3. Note that if the user selects the **No** button, the web browser will return to the **Port State Overview** webpage without restarting.

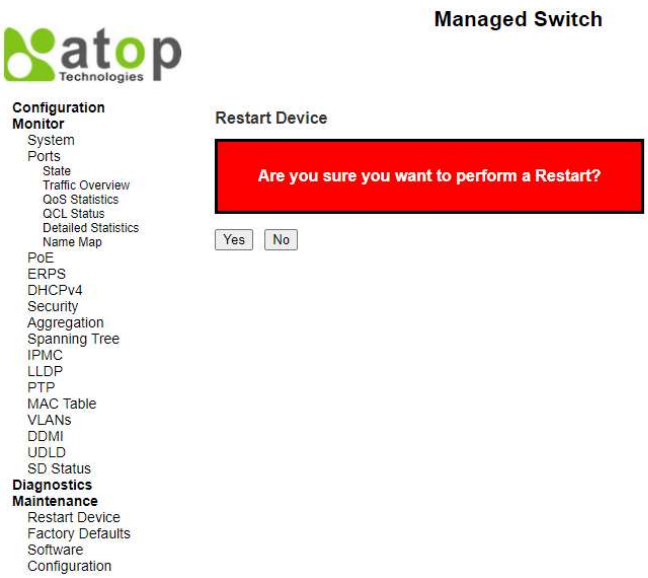


Figure 5.2 Webpage to Restart the Device

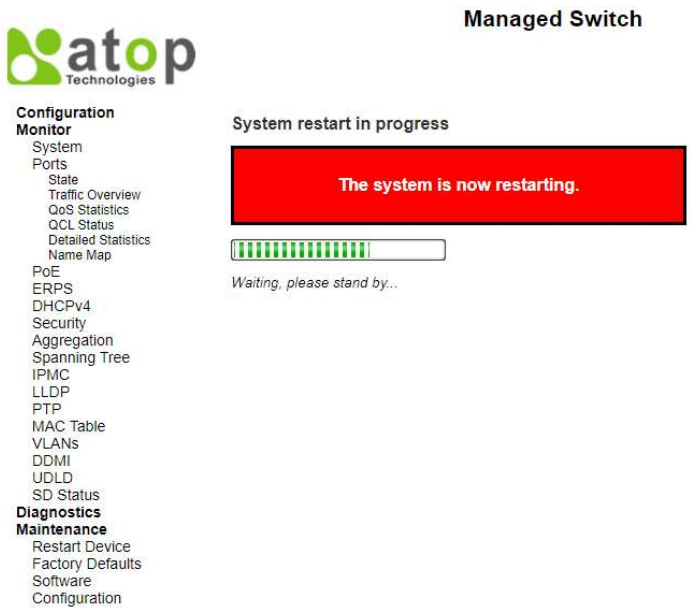


Figure 5.3 System restart in progress webpage

5.2 Factory Defaults

When the managed switch is not working properly, the user can reset it back to the original factory default settings by selecting **Maintenance→Factory Defaults** menu. Note that the IP configuration will not be changed after using this menu. The **Factory Defaults** webpage is shown in Figure 5.4. The user can click on the **Yes** button to reset the configuration to factory default settings. When the reset process is done the user will be presented with a message as showed in Figure 5.5. The new configuration will be available immediately and no restart is necessary. Note that if the user selects the **No** button, the web browser will be returned to the **Port State Overview** webpage.

Figure 5.4 Webpage to Reset Configuration to Factory Defaults

Figure 5.5 Message after the configuration factory reset is done.

Note: Restoring the factory default can also be performed by making a physical loopback between Port 1 and Port 2 within the first minute of switch rebooting. During the first minute after rebooting, "loopback" packets will be transmitted out of Port 1. If a "loopback" packet is received at Port 2, the switch will perform the restoration to factory default setting.

5.3 Software

This **Maintenance→Software** submenu allows the user to update the firmware for the device and check or select the current software/firmware image on the device.

5.3.1 Upload

The users can update the device firmware via web interface using **Upload** menu as shown in Figure 5.6. To update the firmware, the users can download a new firmware from Atop's website and save it on a local computer. Then, the users can click **Select File…** button and choose the firmware file that is already downloaded. The switch's firmware typically has a ".dld" extension such as RHG9728-KXXXAXXX.dld. After that, the users can click **Start Upgrade** button and wait for the update process to be done. After the software image is uploaded, a webpage will display a message stating that the firmware update is initiated. After a duration of approximately one minute, the firmware will finish update and the switch will be restarted.

Warning: While the firmware is being updated, web access will appear to be defuncted. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. **Do not restart or power off the device during this time** otherwise the switch may fail to function afterwards.

Note: please make sure that the switch is plug-in all the time during the firmware upgrade.

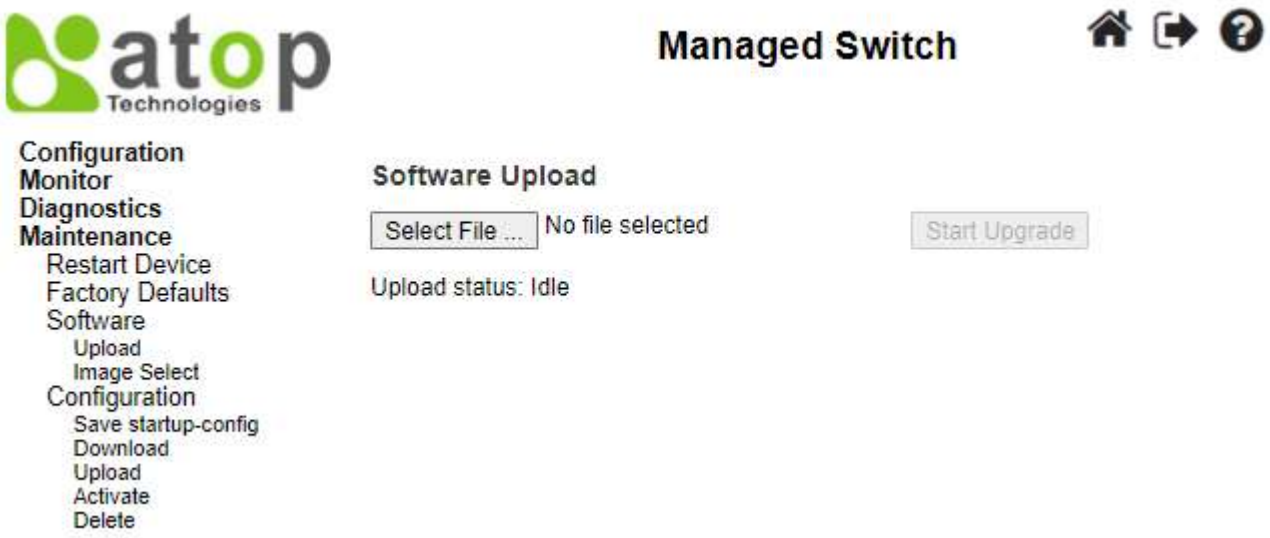


Figure 5.6 Webpage to Upload Software

5.4 Configuration

The managed switch stores its configuration in a number of text files in command line interface (CLI) format. The files are either virtual (RAM-based) or stored in flash on the switch. The available configuration files are:

- **running-config**: A virtual file that represents the currently active configuration on the switch. This file is volatile or disappeared when the power is off.
- **startup-config**: The start-up configuration for the switch which is read at boot time. If this file does not exist at boot time, the switch will start up in its default configuration.

- **default-config**: A read-only file with vendor-specific configuration. This file is read when the system is restored to default settings.
- Up to 31 other files, typically used for configuration backups or alternative configurations.

The **Configuration** menu enables the user to manage the configuration file on the switch. Under the **Maintenance→Configuration** menu, there are **Save startup-config**, **Download**, **Upload**, **Activate**, and **Delete** submenus as shown in Figure 5.7.

Figure 5.7 Submenus under Maintenance→Configuration menu

5.4.1 Save startup-config

The managed switch can save the start-up configuration inside the device. The webpage shown in Figure 5.8 allows the user to generate the start-up configuration file inside the managed switch. When the configuration file generation was finished, a message as shown in Figure 5.9 will be displayed on the webpage. This menu copies *running-config* to *startup-config*; therefore, ensuring that the current active configuration will be used at the next reboot.

Figure 5.8 Webpage to Save the Start-up Configuration

Figure 5.9 Message indicates the saving of startup-configuration file successfully

5.4.2 Download

The user can download different configuration files from the managed switch to the local computer using the web browser. There are **running-config**, **default-config**, and **startup-config** files that can be chosen as shown in Figure 5.10. To select the file name to be downloaded, check the radio button in front of the file name, then click on the **Download Configuration** button. The chosen configuration file will be downloaded by the web browser on to your local computer.

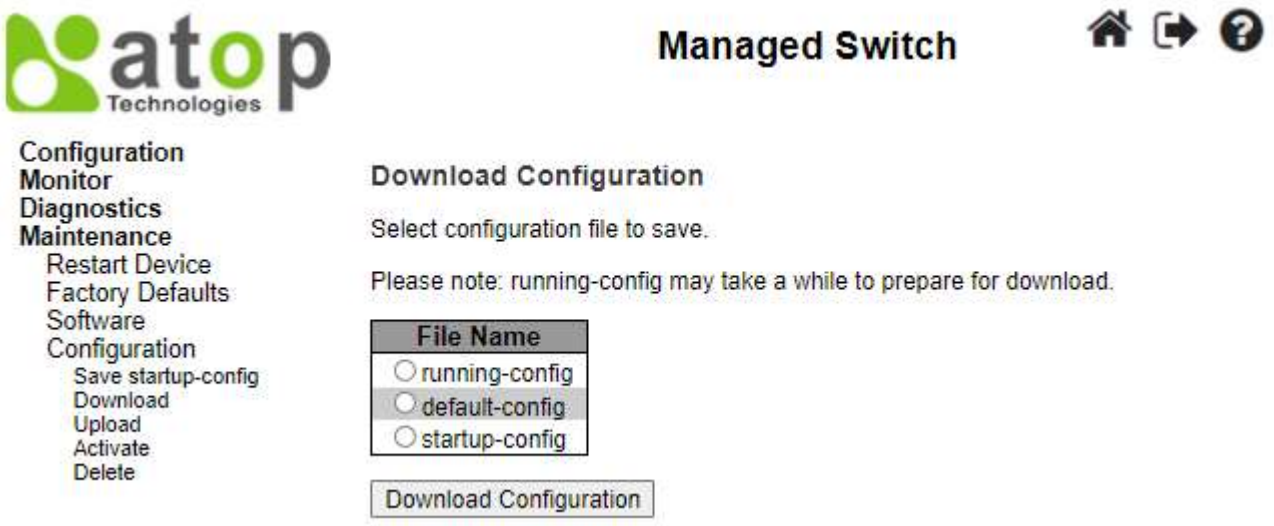


Figure 5.10 Webpage to Download the Current Configuration File

5.4.3 Upload

On this web page, the user can upload a local configuration file on the user's computer to the managed switch using web browser. This will be useful when the user would like to use a backup configuration file from another managed switch. To upload a configuration file, select the **Choose File** button as shown in Figure 5.11 to open a file chooser on the personal computer. Then, select a configuration file on your device. Next, the user can select the name of **Destination File** on the managed switch from the two given file names which are either **running-config** or **startup-config**. Note that the running-config file name also has two possible parameters or options that can be chosen which are **Replace** or **Merge**. Also, the default-config file is read-only; therefore, the user cannot choose it for uploading. That means the upload configuration file can be used to replace the running-config file on the managed switch or can be merged with the running-config file on the managed switch. The last option for the **File Name** is to create a new file by selecting the radio button in front of **Create new file** option in which the user can enter the new file name in the text field under the **Parameters** column. Finally click on the **Upload Configuration** button to start the upload process. A message "**Upload successfully completed**" will be displayed on the webpage.

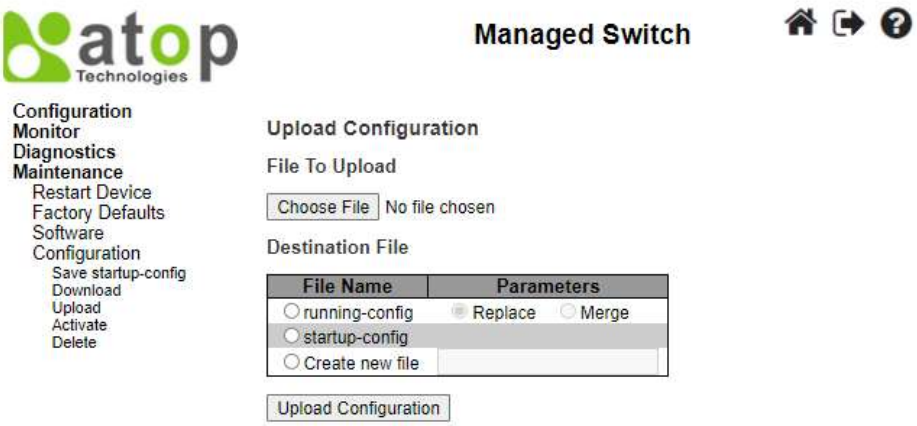


Figure 5.11 Webpage to Upload a Configuration File

If the destination is *running-config*, the file will be applied to the switch configuration. This can be done in two ways:

- Replace mode: The current configuration is fully replaced with the configuration in the uploaded file.
- Merge mode: The uploaded file is merged into *running-config*.

If the flash file system is full (i.e., contains *default-config* and 32 other files, usually including startup-config), it is not possible to create new files. Then, an existing file must be overwritten or another file must be deleted.

5.4.4 Activate

The user can activate different configuration files inside the managed switch, except for *running-config* which represents the currently active configuration. The **Configuration→Activate** submenu under the **Maintenance** menu as shown in Figure 5.12 can be used to perform this task. The user can select a configuration file from the list under the **File Name** table by checking on the radio button in front of that file name. Then, click on the **Activate Configuration** button. After the activation process is completed, the webpage will be updated to display the **Status** and **Output** as shown in Figure 5.13.

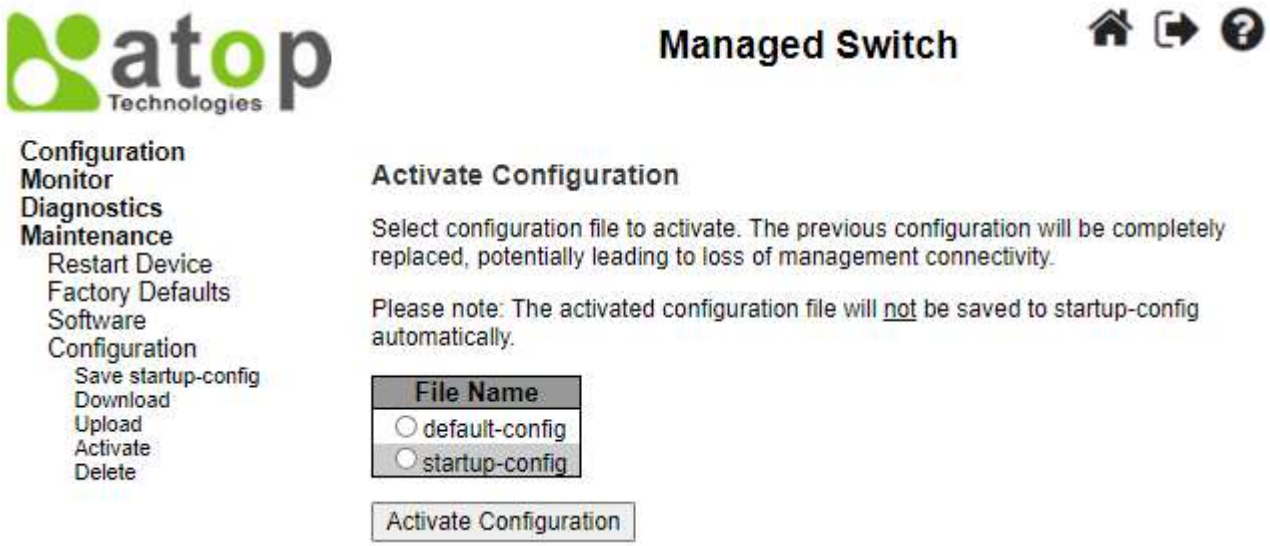


Figure 5.12 Webpage to Activate a Configuration File

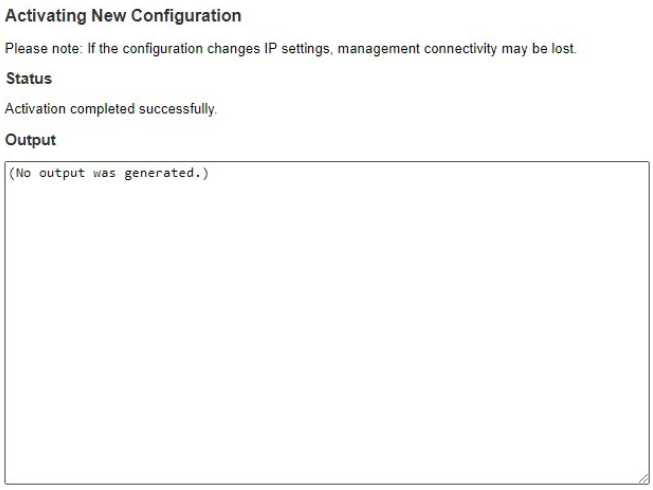


Figure 5.13 Activating New Configuration Webpage

5.4.5 Delete

The last submenu under the **Maintenance→Configuration** menu is **Delete**. This webpage allows the user to delete user-created configuration file stored in flash memory, including *startup-config*, as shown in Figure 5.14. Note that **default-config** cannot be deleted by this menu. For example, the **startup-config** file can be created by the **Save startup-config** menu and then can be deleted by this **Delete** menu. To remove a configuration file, select the file name by checking on the radio button in front of that file under the **File Name** table. Then, click on the **Delete Configuration File** button. Note that a pop-up window will be prompted for a confirmation by the user as shown in Figure 5.15. If the user really wants to delete the configuration, the user can click on the **OK** button. If the user wants to change the decision, the user can click on the **Cancel** button. When the deletion is completed, a message will be

presented on the webpage such as "**startup-config successfully deleted**". Note that if this is done and the switch is rebooted without a prior **Save** operation, this effectively resets the switch to default configuration.

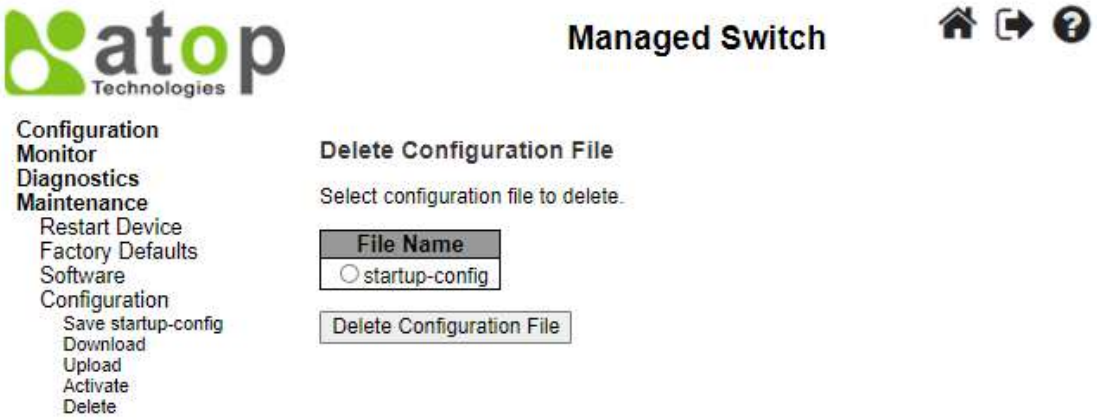


Figure 5.14 Webpage to Delete a Configuration File

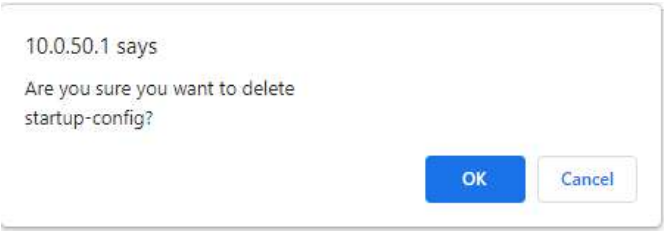


Figure 5.15 Confirmation for deleting a configuration file

Atop Technologies, Inc.

www.atoponline.com

TAIWAN HEADQUARTER and INTERNATIONAL SALES:

2F, No. 146, Sec. 1, Tung-Hsing Rd,
30261 Chupei City, Hsinchu County
Taiwan, R.O.C.
Tel: +886-3-550-8137
Fax: +886-3-550-8131
sales@atop.com.tw

ATOP CHINA BRANCH:

3F, 75th, No. 1066 Building,
Qingzhou North Road,
Shanghai, China
Tel: +86-21-64956231