Atop Technologies, Inc.

Industrial Managed Layer-3 Switch

User Manual

V2.3

September 27th, 2022

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. Thecontents are designed to help users manage the switchand 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 networkoperations, andmight 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. Ifthey 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 Ethernetswitches.

Documentation Control

Author:	Matteo Tabarelli
Revision:	2.3
Revision History:	sFlow
Creation Date:	2 November 2016
Last Revision Date:	21 October 2022
Product Reference:	Layer-3 Managed Switch – RHG96XX
Document Status:	Released

Table of Contents

1 Introduction 15

1.1 Introduction toIndustrial Managed Switch 15
1.2 Software Features 16

2 Configuring with a Web Browser 17

2.1 Web-based Management Basics 17
2.1.1 Default Factory Settings 17
2.1.2 Login Process and Main Window Interface 18
2.2 Basic Information 19
2.2.1 Sys Info 19
2.2.2 Device InformationSetting 20
2.2.3 Console Setting 20
2.2.4 Protocols Status 21
2.2.5 Power Status 22
2.2.6 Temperature Log 22
2.3 Administration 23
2.3.1 Password 24
2.3.2 IP Setting 26
2.3.3 IPv6 Setting 28
2.3.4 Ping 30
2.3.5 Ping6 31
2.3.6 Mirror Port 31
2.3.7 System Time 32
2.3.8 Modbus Setting 33
2.3.9 Precision Time Protocol (PTP) 41
2.3.10 Secure Shell - SSH 44
2.3.11 Telnet 45
2.3.12 HTTPS 45
2.3.13 sFlow 46
2.4 Forwarding 47
2.4.1 QoS 48
2.4.2 Rate Control 52
2.4.3 Storm Control 53
2.5 Redundancy 55
2.5.1 Setting 55
2.6 Port-related settings 56
2.6.1 Port Setting 57
2.6.2 Port Status 58
2.6.3 Mini-GBIC Port Status 59
2.6.4 Port Statistics 60
2.7 Trunking 61
2.7.1 Trunking Setting 61
2.7.2 LACP Status 63
2.8 Unicast/Multicast MAC 65
2.8.1 Add Static MAC 66
2.8.2 Black-List MAC 67
2.8.3 MAC Aging Time 67
2.8.4 MAC Table 68
2.9 GARP/GVRP/GMRP 69
2.9.1 Multicast Group Table 69
2.9.2 GARP Setting 70
2.9.3 GVRP Setting 70
2.9.4 GMRP Setting 72
2.10 IP Multicast 74

2.10.1 IGMP 75
2.10.2 MLD 79
2.10.3 DVMRP 82
2.10.4 PIM 88
2.10.5 Static IP Multicast 105
2.11 SNMP 106
2.11.1 SNMP Agent 107
2.11.2 SNMP V1/V2c Community Setting 108
2.11.3 Trap Setting 108
2.11.4 SNMPv3 Auth. Setting 109
2.12 Spanning Tree 111
2.12.1 Spanning Tree Setting 112
2.12.2 Bridge Info 114
2.12.3 Port Setting 115
2.12.4 MSTP Instance 118
2.13 BGP 119
2.13.1 BGP Setting 119
2.13.2 BGP Neighbor Setting 121
2.13.3 BGP Proto Setting 129
2.13.4 BGP IP Setting 138
2.14 VLAN 143
2.14.1 VLAN Setting 144
2.14.2 802.1Q VLAN 144
2.14.3 Port-Based VLAN 148
2.14.4 MAC-Based VLAN 149
2.14.5 IP Subnet-Based VLAN 150
2.14.6 Protocol-Based VLAN 150
2.14.7 QinQ 151
2.15 VRRP 153
2.15.1 VRRP 154
2.15.2 Setting 155
2.15.3 Restart 157
2.16 DHCP Server 158
2.16.1 Setting 159
2.16.2 Clients 160
2.16.3 Restart 161
2.17 Security 161
2.17.1 Port Security 162
2.17.2 802.1X 164
2.17.3 IP Source Guard 168
2.17.4 ARP Spoof Prevention 170
2.17.5 DHCP Snooping 171
2.17.6 ACL (Access Control List) 172
2.17.7 Dynamic ARP Inspection with DHCP 177
2.18 ERPS Ring 178
2.18.1 ESRP Setting 180
2.18.2 iA-Ring Settings 185
2.18.3 C-Ring(Compatible-Ring) Settings 187
2.18.4 U-Ring 188
2.18.5 Compatible-Chain Settings 191
2.18.6 MRP 193
2.19 LLDP 195
2.19.1 LLDPSettings 196
2.19.2 LLDP Neighbors 197
2.20 UDLD 198
2.20.1 UDLD's Setting 199
2.20.2 UDLD's Port-info 200
2.20.3 UDLD's Reset 200

2.21 IP Routing (Layer-3 Switching Features) 201
2.21.1 IP Routing's Setting 201
2.21.2 IPv4 Static Routing 201
2.21.3 RIP Setting 202
2.21.4 OSPF Settings 203
2.22 Client IP Setting 210
2.22.1 DHCP Relay Agent 210
2.22.2 DHCP Mapping IP 211
2.23 SyncE 212
2.23.1 SyncE Setting 213
2.23.2 SyncE Status 214
2.24 System 214
2.24.1 System Log 216
2.24.2 Warning/Alarm 217
2.24.3 Denial of Service 222
2.24.4 Backup/Restore Config 224
2.24.5 Firmware Update 226
2.24.6 Factory Default Setting 227
2.24.7 Reboot 227
2.24.8 Logout 227
3 Configuring with a Serial Console 228
3.1 Serial Console Setup 228
3.2 Command Line Interface Introduction 229
3.3 General Commands 230
3.4 Command Example 230
3.4.1 Administration Setup using Serial Console 231
3.4.2 Spanning Tree Setup using Serial Console 232
3.4.3 VRRP Setup using Serial Console 232
3.4.4 DHCP Server Setup using Serial Console 234
3.4.5 PIM SM Setup using Serial Console 235
3.4.6 PIM SSM Setup using Serial Console 236
3.4.7 PIM DM Setup using Serial Console 237
3.4.8 BGP Setup using Serial Console 238
4 Configuring with a Telnet Console 248
4.1 Telnet 248
4.2 Telnet Log-in 248
4.3 Command Line Interface for Telnet 249
4.4 Commands in the Privileged Mode 249
4.5 Commands in the Configuration Mode 250
5 Device Management Utility 254
5.1 Network Setting 255
5.2 Topology Diagram 256
5.3 Firmware Update 258
6 Glossary 259
7 Modbus Memory Map 261

Table of Figures

Figure 2.1 IP Address for Web-based Setting 18

Figure 2.2Default Web Interface 18
Figure 2.3Basic Information Dropdown Menu 19
Figure 2.4Details of Sys Info Webpage 19
Figure 2.5Details of Device InformationSettings Webpage 20
Figure 2.6Setting Parameters for the Console Method 21
Figure 2.7Protocol Status Webpage 21
Figure 2.8Power Status Webpage 22
Figure 2.9User Temperature Log 23
Figure 2.10 System Temperature Log 23
Figure 2.11Administration DropdownMenu 24
Figure 2.12Password Setting Webpage 24
Figure 2.13 Authentication Server Setting 25
Figure 2.14 IP Setting under IP Setting Webpage 27
Figure 2.15 IP Interface Part under IP Setting Webpage 27
Figure 2.16 IPv6 Setting Partof IPv6 Setting Webpage 28
Figure 2.17 IP Interface for IPv6 Part of IPv6 Setting Webpage 29
Figure 2.18Ping Webpage 30
Figure 2.19Example of Ping Command 30
Figure 2.20Example of successful ping command result 30
Figure 2.21Example of unsuccessful ping command result 30
Figure 2.22Ping6 Webpage 31
Figure 2.23Example of Successful Ping6 Result 31
Figure 2.24Mirror Port Webpage 31
Figure 2.25Webpage for Setting System Time and SNTP 32
Figure 2.26Webpage for Setting the Modbus Address 34
Figure 2.27Mapping Table of Modbus Address for Switch's IP Address 34
Figure 2.28Entering Connection Setup Menu of the Modbus Poll 35
Figure 2.29Modbus Poll Connection Setup 35
Figure 2.30 Multiple Cell Section in Modbus Poll 36
Figure 2.31 Set Display Mode to Hex in Modbus Poll 36
Figure 2.32 Modbus Poll Setup Read/Write Definition 37
Figure 2.33Slave ID in the Modbus Poll Function is set to 1 37
Figure 2.34 Set Code 03 in the Modbus Poll Function 38
Figure 2.35 Setup Starting Address and Quantity in Modbus Poll 38
Figure 2.36 Modbus Memory Address 81 and 82 are the location of RHG96xx's IP Address 39
Figure 2.37Mapping Table of Modbus Address for Clearing Port Statistics 39
Figure 2.38 Port Count in Port Statistics Webpage 39
Figure 2.39 Click on Function 06 in the Modbus Poll 40
Figure 2.40 Use Modbus Poll to Clear Switch's Port Count 40
Figure 2.41 Cleared Port Statistics 40
Figure 2.42 PTP's Submenu 41
Figure 2.43 PTP Setting Webpage, example taken from RHG96XX series 42
Figure 2.44Output Module Setting 44
Figure 2.45 SSH Setting Webpage 45
Figure 2.46 Telnet Setting Webpage 45
Figure 2.47 HTTPS Setting Webpage 46
Figure 2.48 sFlow setting Webpage 46
Figure 2.49 sFlow working sample 47
Figure 2.50 Forwarding Dropdown Menu 48
Figure 2.51 QoS Dropdown Menu 48
Figure 2.52 QoS Setting Webpage 50
Figure 2.53Mapping Table of CoS Webpage 51
Figure 2.54 Mapping Table of DSCP and ECN Webpage 52
Figure 2.55 Rate Control Webpage 53
Figure 2.56 Storm Control Webpage 54
Figure 2.57Setting Webpage under Redundancy Section 56
Figure 2.58 Port Dropdown Menu 56

Figure 2.59 Port Setting Webpage 57
Figure 2.60 Port Status Webpage 59
Figure 2.61 Mini-GBIC Port Status Webpage 60
Figure 2.62 Port Statistics Webpage 60
Figure 2.63Trunking Dropdown Menu 61
Figure 2.64Trunking Setting Webpage, example with RHG9628-410GSFP-BC-DC 62
Figure 2.65LACP Webpage 64
Figure 2.66Unicast vs. Multicast 65
Figure 2.67Unicast/Multicast Dropdown Menu 66
Figure 2.68Add Static MAC Webpage 66
Figure 2.69Black-List MACSetting Webpage 67
Figure 2.70MAC Aging TimeWebpage 68
Figure 2.71MAC Table Webpage 68
Figure 2.72 GARP/GVRP/GMRP Dropdown Menu 69
Figure 2.73Multicast Group Table 69
Figure 2.74GARP Setting Webpage 70
Figure 2.75GVRP Setting Box with Port Enabling 71
Figure 2.76GVRP Statistics 71
Figure 2.77 GMRP Setting Box 72
Figure 2.78GMRP Statistics 73
Figure 2.79IP Multicast Dropdown Menu 74
Figure 2.80 IGMP's Options 75
Figure 2.81IGMP Setting Webpage 75
Figure 2.82Example of IGMP Proxy 76
Figure 2.83 IGMP's IP Multicast Table Webpage 76
Figure 2.84 Example of IGMP's IP Multicast Table 77
Figure 2.85 IGMP's Statistics Webpage 78
Figure 2.86 Example of IGMP's Statistics 78
Figure 2.87 MLD's Submenus 79
Figure 2.88 MLD's Setting 80
Figure 2.89Error: No vlans configured for MLD 81
Figure 2.90 MLD's IPv6 Multicast Table 81
Figure 2.91 MLD's Statistics 82
Figure 2.92 Example of Setting 802.1Q VLAN Interface for Multicast Routing 83
Figure 2.93 Example of Setting Port VLAN ID (PVID) for Multicast Routing 84
Figure 2.94 Example of IP Address Setting for VLAN Interfaces used in Multicast Routing 85
Figure 2.95 DVMRP Running Status Web Page 85
Figure 2.96 Error Message When Enabling DVMRP with no DVMRP VLANs 86
Figure 2.97 DVMRP Setting Web Page 86
Figure 2.98 DVMRP Restart Web Page 87
Figure 2.99 DVMRP Statistics Web Page 87
Figure 2.100 Error Message on DVMRP Statistics Web Page 87
Figure 2.101 PIM Menu and Its Submenus 88
Figure 2.102 Example of Setting 802.1Q VLAN Interface for PIM Protocol 89
Figure 2.103 Example of Setting Port VLAN ID (PVID) for PIM 89
Figure 2.104 Example of IP Address Setting for VLAN Interfaces used in PIM 90
Figure 2.105 Enabling of IP Routing Function in Layer-3 Managed Switch for PIM 90
Figure 2.106 Example of Adding Static Routes for PIM 91
Figure 2.107 PIM's IGMP Query Interval Setting Web Page 91
Figure 2.108 IGMP Join/Leave Web Page 92
Figure 2.109 Menu and Submenus of PIM Sparse Mode 92
Figure 2.110 PIM Sparse Mode Running Status Web Page 93
Figure 2.111 Error Message when IP Routing function is not enabled 93
Figure 2.112 Error Message when no Sparse-Mode VLAN was configured 93
Figure 2.113 PIM Sparse Mode Setting Web Page 94
Figure 2.114 PIM Sparse Mode Statistics Web Page 95
Figure 2.115 Error Message when PIM Sparse Mode was not enabled 96

Figure 2.116 PIM Sparse Mode Restart Web Page 96
Figure 2.117 Rendezvous Point Bootstrap Settings Web Page 97
Figure 2.118 Rendezvous Point Static Setting Web Page 97
Figure 2.119 Menu and Submenus of PIM SSM 98
Figure 2.120 PIM Source Specific Mode Running Status Web Page 98
Figure 2.121 Error Message when no PIM SSM VLAN was configured 98
Figure 2.122 PIM Source Specific Mode (SSM) Setting Web Page 99
Figure 2.123 PIM Source Specific Mode Restart Web Page 99
Figure 2.124 Example of Sending IGMP Join to an SSM Source Address 100
Figure 2.125 PIM Source Specific Mode (SSM) Statistics Web Page 101
Figure 2.126 Error Message on Statistics web page when PIM SSM was not enabled 101
Figure 2.127 PIM Dense Mode Menus 102
Figure 2.128 PIM Dense Mode's Running Status Web Page 102
Figure 2.129 Error Message when IP Routing is Disabled 102
Figure 2.130 Error Message when It has insufficient configured VLANs 102
Figure 2.131 PIM Dense Mode Settings Web Page 103
Figure 2.132 PIM Dense Mode Restart Web Page 103
Figure 2.133 PIM Dense Mode Statistics Web Page 104
Figure 2.134 Error Message when PIM Dense Mode is not enabled. 104
Figure 2.135 Static IP Multicast Setting Webpage 105
Figure 2.136Example of Static IP Multicast Setting 106
Figure 2.137 SNMP Dropdown Menu 107
Figure 2.138 SNMP Enabling Box 107
Figure 2.139 SNMP Community Strings 108
Figure 2.140Example of Trap Receiver Setting 109
Figure 2.141 SNMPv3 Users' Options 110
Figure 2.142 Spanning Tree Dropdown Menu 111
Figure 2.143 Spanning Tree Mode Setting 112
Figure 2.144 Spanning Tree Main Setting for STP and RSTP 112
Figure 2.145 Spanning Tree Main Setting for MSTP 113
Figure 2.146 Spanning Tree Per-port Setting for STP and RSTP 114
Figure 2.147Bridge Information Webpage 114
Figure 2.148Spanning Tree Port SettingWebpage 116
Figure 2.149 MSTP Instance Webpage 118
Figure 2.150 BGP Dropdown Menu 119
Figure 2.151 BGP Setting Submenu 119
Figure 2.152Setting inside the BGP-> BGP Setting Submenu 120
Figure 2.153BGP Restart inside BGP->BGP Setting Submenu 121
Figure 2.154 Error Message of BGP Restart 121
Figure 2.155BGP Neighbor Setting Menu 122
Figure 2.156Remote ASSubmenu inside the BGP Neighbor Setting 122
Figure 2.157Local ASSubmenu inside the BGP Neighbor Setting 123
Figure 2.158Description Submenu inside the BGP Neighbor Setting 123
Figure 2.159Route Map Submenu inside the BGP Neighbor Setting 124
Figure 2.160Prefix List Submenu inside the BGP Neighbor Setting 124
Figure 2.161 Advertisement Interval Submenu inside the BGP Neighbor Setting 125
Figure 2.162 Timers Submenu inside the BGP Neighbor Setting 126
Figure 2.163Allow AS INSubmenu inside the BGP Neighbor Setting 126
Figure 2.164Peer Group Submenu inside the BGP Neighbor Setting 127
Figure 2.165Shutdown Submenu inside the BGP Neighbor Setting 127
Figure 2.166Activate Submenu inside the BGP Neighbor Setting 128
Figure 2.167Route Reflector Client Submenu inside the BGP Neighbor Setting 128
Figure 2.168Remove Private AS Submenu inside the BGP Neighbor Setting 129
Figure 2.169BGP Proto Setting Menu 129
Figure 2.170BGP Router ID Submenu inside the BGP Proto Setting 130
Figure 2.171Router BGP ASN Submenu inside the BGP Proto Setting 131
Figure 2.172Set AS Path Prepend Submenu inside the BGP Proto Setting 131

Figure 2.173BGP Timers Submenu inside the BGP Proto Setting 132
Figure 2.174Dampening Submenu inside the BGP Proto Setting 133
Figure 2.175Route Map Submenu Inside the BGP Proto Setting 133
Figure 2.176Network IP Submenu inside the BGP Proto Setting 134
Figure 2.177Confed. Peers Submenu inside the BGP Proto Setting 134
Figure 2.178Confed. Identifier Submenu inside the BGP Proto Setting 135
Figure 2.179Aggregate IP Submenu inside the BGP Proto Setting 136
Figure 2.180Maximum Path Submenu inside the BGP Proto Setting 136
Figure 2.181Redistribute Submenu inside the BGP Proto Setting 137
Figure 2.182AS Path Submenu inside the BGP Proto Setting ->Match Setting 137
Figure 2.183Community Range Submenu inside the BGP Proto Setting ->Match Setting 138
Figure 2.184Match Prefix List Submenu inside the BGP Proto Setting ->Match Setting 138
Figure 2.185Submenus inside the BGP IP Setting 139
Figure 2.186Expaned Submenus inside the BGP IP Setting ->IP Community List 139
Figure 2.187Standard Submenu inside the BGP IP Setting -> IP Community List 140
Figure 2.188Expanded Submenu inside the BGP IP Setting ->IP Ext. Community List 140
Figure 2.189Standard Submenu inside the BGP IP Setting ->IP Ext. Community List 141
Figure 2.190List Name IP Submenu inside the BGP IP Setting ->Prefix List 142
Figure 2.191List Name Submenu inside the BGP IP Setting ->Prefix List 142
Figure 2.192Example of VLAN Configuration 143
Figure 2.193 VLAN Dropdown Menu 144
Figure 2.194 VLAN Setting Webpage 144
Figure 2.195 802.1Q VLAN Dropdown Menu 145
Figure 2.196 802.1Q VLAN's Setting Webpage 146
Figure 2.197 802.1Q VLAN PVID Setting Webpage 147
Figure 2.198 802.1Q VLAN Table Webpage 148
Figure 2.199 Example of 802.1Q VLAN Table 148
Figure 2.200 Port-based VLAN Setting Webpage 149
Figure 2.201 MAC-Based VLAN Setting Webpage 149
Figure 2.202 IP Subnet-Based VLAN Setting Webpage 150
Figure 2.203 Protocol to Group Setting Webpage 150
Figure 2.204 Group to VLAN Setting Webpage 151
Figure 2.205 Example of QinQ Deployment 152
Figure 2.206 QinQ Setting Webpage 153
Figure 2.207 Overview of the VRRP 154
Figure 2.208VRRP Dropdown Menu 154
Figure 2.209 VRRP Running Status 155
Figure 2.210Setting in VRRPMenu 155
Figure 2.211 VRRP Virtual Interface Box under VRRP's Setting 156
Figure 2.212 Setting in VRRP Menu after Adding Virtual Router ID (Front part) 156
Figure 2.213 Setting in VRRP Menu after Adding Virtual Router ID (Ending part) 156
Figure 2.214 Restart in VRRP Menu 157
Figure 2.215Multiple VLANs for a DHCP Server 158
Figure 2.216DHCP Server Dropdown Menu 158
Figure 2.217Status of theDHCP Server 158
Figure 2.218DHCP Server's Setting Submenu 159
Figure 2.219 Add Dynamic IP Address in DHCP Server's Setting Submenu 159
Figure 2.220Add Static IP Address in DHCP Server's Setting Submenu 160
Figure 2.221Modify DHCP Server Configuration in DHCP Server's Setting Submenu 160
Figure 2.222Client Menu in DHCP Server's Dropdown Menu 161
Figure 2.223Restart Menu in DHCP Server's Dropdown Menu 161
Figure 2.224 Security Dropdown Menu 162
Figure 2.225 Port Security Setting Webpage 163
Figure 2.226 White-List MAC Webpage 163
Figure 2.227RADIUS Authentication Sequence 164
Figure 2.228 802.1X Setting Webpage 165

Figure 2.229 802.1X's Parameters Setting Webpage 166
Figure 2.230802.1x Port Setting Webpage 167
Figure 2.231 IP Source Guard Drop-down Menu 168
Figure 2.232 IP Verify Source's Setting Webpage 168
Figure 2.233 IP Verify Source's Status Webpage 169
Figure 2.234 IP Source Binding's Setting Webpage 170
Figure 2.235 IP Source Binding's Status Webpage 170
Figure 2.236 ARP Spoof Prevention Webpage 171
Figure 2.237 DHCP Snooping Webpage 172
Figure 2.238 Security Access Control List Information Webpage(MAC Based Filtering) 173
Figure 2.239 Security Access Control List Information Webpage (for IPv4 Based Filtering) 174
Figure 2.240 Security Access Control List Information Webpage (for IPv6 Based Filtering) 175
Figure 2.241 Dynamic ARP Inspection (DAI) with DHCP Webpage 178
Figure 2.242Error Message for Dynamic ARP Inspection when DHCP Snooping was disabled 178
Figure 2.243An Example of Ring Topology (Example made on EH7520) 179
Figure 2.244 ERPS/Ring Drowdown Menu 180
Figure 2.245ERPS Setting Webpage 181
Figure 2.246ERPS RAPS VLAN Setting Webpage 182
Figure 2.247Example of Ring Topology for ERPS Setup (Example made on EH7520) 183
Figure 2.248Example of Switch A's ERPS settings 184
Figure 2.249Example of SwitchA's RAPS VLAN Settings 184
Figure 2.250Example of Switch B's RAPS VLAN Setting 185
Figure 2.251Switch A's ERPS state 185
Figure 2.252iA-Ring Example Topology (Example made on EH7520) 186
Figure 2.253iA-Ring Setting Webpage 187
Figure 2.254Compatible-Ring (C-Ring) Setting Webpage 188
Figure 2.255 Example 1 of Two Wireless Bridge U-ring (Example made on EH7520) 189
Figure 2.256 Example 2 of Two Wired Bridge U-ring (Example on EH7520) 190
Figure 2.257U-Ring Setting Webpage 191
Figure 2.258 Compatible-Chain Setting Webpage 192
Figure 2.259 MRP Setting Webpage 194
Figure 2.260 Example of PROFINET's MRP VLAN Entry 194
Figure 2.261 MRP Ring Setting Webpage 195
Figure 2.262 MRP Ring Setting Error Message 195
Figure 2.263 LLDP Dropdown Menu 196
Figure 2.264LLDP Setting Webpage 196
Figure 2.265LLDP Neighbors Webpage 197
Figure 2.266Example of LLDP NeighborsWebpage 198
Figure 2.267 UDLD Menu 199
Figure 2.268 UDLD Setting Webpage 199
Figure 2.269 Error Message when No UDLD VLAN was configured 200
Figure 2.270 UDLD's Port-info Webpage with an Example 200
Figure 2.271 UDLD's Reset Webpage 200
Figure 2.272 IP Routing Menu 201
Figure 2.273 IP Routing Webpage 201
Figure 2.274 Error message when IP Routing is disabled. 201
Figure 2.275 IPv4 Static Routing Webpage 202
Figure 2.276 Example ofan Entry in IPv4 Static Routing Table 202
Figure 2.277 RIP Setting Webpage 203
Figure 2.278 OSPF Setting Submenu 204
Figure 2.279 OSPF's Global Setting Webpage 204
Figure 2.280 OSPF's Area Setting Webpage 205
Figure 2.281 OSPF Interface Setting Webpage 206
Figure 2.282 OSPF Virtual Link Setting Webpage 208
Figure 2.283 OSPF Area Aggregation Setting Webpage 209
Figure 2.284 OSPF Routing Table Webpage 210
Figure 2.285 Client IP Setting Dropdown Menu 210

Figure 2.286 DHCP Relay Agent Webpage 211
Figure 2.287 DHCP Mapping IP Webpage 211
Figure 2.288How SyncE works in RHG9628 212
Figure 2.289SyncE Submenus in RHG96xx 213
Figure 2.290SyncE Setting submenus in RHG96xx 213
Figure 2.291SyncE Status submenus in RHG96xx 214
Figure 2.292 System Dropdown Menu 215
Figure 2.293System Log SettingWebpage 216
Figure 2.294Event Log Webpage 217
Figure 2.295 Webpage ofWarning Event Selection 218
Figure 2.296 SMTP Setting Webpage 220
Figure 2.297 Example of SMTP Setting 221
Figure 2.298 Warning/Alarm Log Webpage 222
Figure 2.299Example of Warning Events 222
Figure 2.300 Denial of Service Setting Webpage 223
Figure 2.301Backup/Restore Config.Dropdown Menu 224
Figure 2.302 Backup/Restore Configuration via HTTP 225
Figure 2.303 Backup/Restore Configuration via TFTP 226
Figure 2.304Firmware Update Webpage 227
Figure 2.305Factory Default Setting Webpage 227
Figure 2.306Reboot Webpage 227
Figure 2.307 Logout Webpage 227
Figure 3.1Setting of New Connection in Tera Term Program 228
Figure 3.2Setup Menu 228
Figure 3.3Setting for the Serial Port 229
Figure 3.4Modes, privileges, and prompts 230
Figure 3.5Example of Commands 231
Figure 3.6 Example of Virtual Routers Configuration for VRRP 234
Figure 3.7 Example of CLI for VLAN Configurations in DHCP Server 235
Figure 3.8 Example of PIM SM Configuration 236
Figure 3.9 Example of PIM Source Specific Mode Configuration 237
Figure 3.10 Examples of CLI for Neighbor Bestpath AS-Path Confed Configuration in BGP 242
Figure 3.11 Examples of CLI for Neighbor Bestpath Compare-Routerid Configuration in BGP 242
Figure 3.12 Examples of CLI for Neighbor Port Configuration in BGP 242
Figure 3.13 Examples of CLI for Neighbor Weight Configuration in BGP 242
Figure 3.14 Examples of CLI for Neighbor Version Configuration in BGP 242
Figure 3.15 Examples of CLI for Neighbor EBGP-Multihop Configuration in BGP 243
Figure 3.16 Examples of CLI for Neighbor Interface Configuration in BGP 243
Figure 3.17 Examples of CLI for Show Filter-List Configuration in BGP 243
Figure 3.18 Examples of CLI for Neighbor Distribute-List Name Configurations in BGP 243
Figure 3.19 Examples of CLI for Neighbor Peer-Group Configuration in BGP 243
Figure 3.20 Examples of CLI for Neighbor Send-Community Extended Configuration in BGP 244
Figure 3.21 Examples of CLI for Neighbor Attribute-Unchanged AS-Path Configuration in BGP 244
Figure 3.22 Examples of CLI for Neighbor Capability ORF Prefix-List Configuration in BGP 244
Figure 3.23 Examples of CLI for Neighbor Unsuppress-Map Configuration in BGP 244
Figure 3.24 Examples of CLI for Neighbor Capability Route-Fresh Configuration in BGP 244
Figure 3.25 Examples of CLI for Neighbor Don't Capability Negotiate Configuration in BGP 244
Figure 3.26 Examples of CLI for Neighbor Next-Hop-Self Configuration in BGP 245
Figure 3.27 Examples of CLI for Neighbor Override Capability Configuration in BGP 245
Figure 3.28 Examples of CLI for Neighbor Passive Configuration in BGP 245
Figure 3.29 Examples of CLI for Neighbor Route Server Client Configuration BGP 245
Figure 3.30 Examples of CLI for Neighbor Soft-Reconfiguration Inbound Configuration in BGP 245
Figure 3.31 Examples of CLI for Cluster-ID Configuration in BGP 246
Figure 3.32 Examples of CLI for Set Local-Preference Configuraion in BGP 246
Figure 3.33 Examples of CLI for Default Local Preference Configurations in BGP 246
Figure 3.34 Examples of CLI for Distance Configuration in BGP 246
Figure 3.35 Examples of CLI for Set Metric Configuration in BGP 246

Figure 3.36 Examples of CLI for Best Path Med Configuration in BGP 247
Figure 3.37 Examples of CLI for IP AS-PATH Access List Configuration in BGP 247
Figure 4.1Telnet Command 248
Figure 4.2Log-in Screen using Telnet 249
Figure 4.3Commands in the Privileged Mode 249
Figure 4.4Commands in the Configuration Mode 251
Figure 5.1 Device Management Utility 254
Figure 5.2Rescan (Search) Icon 254
Figure 5.3 Authentication to Login to RHG9XXX switch 255
Figure 5.4 Network Configure Icon 255
Figure 5.5 Network Setting Dialog 255
Figure 5.6 Administration Verification before Changing the Network Setting 256
Figure 5.7 Warning Dialog before the Device Restart 256
Figure 5.8 Topology Diagram 257
Figure 5.9 Show Information on Topology Diagram 257
Figure 5.10 Upgrade from Disk (Firmware Update)Icon 258
Figure 5.11 Dialog Window for Download Firmware from Disk 258

Table of Tables

Table 2.1Descriptions of the Basic information 19
Table 2.2Descriptions of Password Setting 24
Table 2.3Authentication Server Settings 25
Table 2.4Comparison of Authentication Server Settings between RADIUS and TACACS+ 26
Table 2.5Descriptions of IP Settings 27
Table 2.6Description of IPv6 Setting 29
Table 2.7Description of Port Mirroring Options 32
Table 2.8Descriptions of the System Time and the SNTP 33
Table 2.9Description of PTP Setting 43
Table 2.10Description of PTP Port Setting 43
Table 2.11Description of Output Module 44
Table 2.12 Descriptions of sFlow Setting 47
Table 2.13 Descriptions of QoS Setting 48
Table 2.14Priority queue descriptions 51
Table 2.15 Descriptions of Rate Control Setting 53
Table 2.16 Descriptions of Storm Control 54
Table 2.17 Descriptions of Limiting Parameters 55
Table 2.18Descriptions of Port Settings 58
Table 2.19Descriptions of Trunking Settings 63
Table 2.20Descriptions of LACP Status 64
Table 2.21Description of fields inAdd Static MAC Webpage 67
Table 2.22Descriptions ofMAC Filtering Webpage 67
Table 2.23Descriptions ofMAC Address Table 68
Table 2.24Descriptions of GARP Timer Settings 70
Table 2.25GVRP Setting Descriptions 72
Table 2.26 Descriptions of GMRP Settings and Statistics 73
Table 2.27Descriptions of IGMP'sSettings 75
Table 2.28 Descriptions of IGMP Statistics 78
Table 2.29 Description of MLD's Statistics 82
Table 2.30 Descriptions of PIM Sparse Mode Settings 94
Table 2.31Description of SNMP Setting 107
Table 2.32Descriptions of Community String Settings 108
Table 2.33Descriptions of Trap Receiver Settings 109
Table 2.34Descriptions of SNMP V3 Settings 110
Table 2.35 Descriptions of Spanning Tree Parameters 113

Table 2.36Bridge Root Information 115
Table 2.37Bridge Topology Information 115
Table 2.38 Descriptions of Spanning Tree Port Setting 116
Table 2.39 Default Path Cost for STP and RSTP 117
Table 2.40 Description of MSTP Information 118
Table 2.41 Description of each Feature inside the BGP-> BGP Setting Submenu 120
Table 2.42Meanings of the Special Character Field 139
Table 2.43Meanings of the Special Character Field 141
Table 2.44Description of VLAN Setting 144
Table 2.45Setting Descriptions of 802.1Q VLAN Settings 146
Table 2.46 Setting Descriptions of 802.1Q VLAN PVID 147
Table 2.47 Descriptions of 802.1Q VLAN Table 148
Table 2.48Description of Fields in White-List MAC Webpage 164
Table 2.49Descriptions of 802.1X Setting 165
Table 2.50Descriptions of 802.1X Parameters 166
Table 2.51Descriptions of 802.1X Port Setting 167
Table 2.52 Descriptions of Main ACL Entries for L2 Filtering in ACL Webpage 173
Table 2.53 Description of Main ACL Entries for L3 Filtering in ACL Webpage 175
Table 2.54 Summary of Label, Description, and Factory Default for Both ACL Filtering Method 176
Table 2.55Descriptions of ERPSSetting 181
Table 2.56Description of ERPS VLAN Setting 182
Table 2.57Setting Configuration for Switch A, B, C and D 183
Table 2.58Descriptions of iA-Ring Setting 187
Table 2.59Descriptions of Compatible-Ring Setting 188
Table 2.60Descriptions of U-Ring Setting 191
Table 2.61 Descriptions of Compatible-Chain Setting 193
Table 2.62 Description of MRP Setting Webpage 194
Table 2.63Descriptions of LLDP Setting 197
Table 2.64Descriptions of LLDP Neighbors Webpage 198
Table 2.65 Descriptions of IPv4 Static Routing Settings 202
Table 2.66 Descriptions of OSPF's Global Setting Webpage 204
Table 2.67 Descriptions of OSPF Area Setting Webpage 205
Table 2.68 Descriptions of OSPF Interface Setting Webpage 207
Table 2.69 Descriptions of OSPF Virtual Link Setting Webpage 208
Table 2.70 Descriptions of OSPF Area Aggregation Setting Webpage 209
Table 2.71 Option and Default Setting of the SyncE Status 214
Table 2.72Descriptions of System Log Settings 216
Table 2.73Descriptions of Event Log 217
Table 2.74 Descriptions of Link Status Alarm Event Selection 218
Table 2.75 Descriptions of Power Status Alarm Event Selection 219
Table 2.76 Descriptions of System Log Alarm Event Selection 219
Table 2.77Descriptions of SMTP Setting 221
Table 2.78Descriptions of Warning/AlarmLog 222
Table 2.79 Descriptions of Denial of Service Setting 224
Table 2.80Descriptions of TFTP Settings 226
Table 3.1Command Description 230
Table 3.2Descriptions of Administrative Commands for Setting Up 231
Table 3.3Descriptions of Commands for Setting up Spanning Tree 232
Table 3.4 Descriptions of Commands for Setting up VRRP 233
Table 3.5 Descriptions of Commands for Setting up DHCP Server 234
Table 3.6Descriptions of Commands for PIMSM Configuration 236
Table 3.7 Descriptions of Commands for PIM SSM Configuration 237
Table 3.8 Descriptions of Commands for PIM DM Configuration 237
Table 3.9 Descriptions of Commands for Setting up BGP Function 238
Table 4.1Commands in the Configuration Mode 251

1 Introduction

1.1 Introduction toIndustrial Managed Switch

Atop's RHG (Router Switching Hub Full Gigabit) 96XXseriesareproduct lines of powerful industrial managed switch whichare referred to asOpen Systems Interconnection (OSI) Layer 3bridging/routing devices. Unlike an "**unmanaged**" switch, which is normally found in homes or in Small Office/Home Office (SOHO) environments and runs in "auto-negotiation" mode, each port on a "**managed switch**" can be configured for its link bandwidth, priority, security, and duplex settings. The managed switches can be managed bySimple Network Management Protocol (SNMP) software, web browsers, Telnet, or serial console. Since every single port can be configured to specific settings, network administrators can better control the network and maximize network functionality.

Atop's managed switchisalso an industrial switch and not a commercial switch. A commercial switch simply works in a comfortable office environment. However, an industrial switch is designed to perform in harsh industrial environments, i.e., extreme temperature, high humidity, dusty air, potential high impact, or the presence of potentially high static charges. Atop's managed switch works fine even in these environments.

Atop'smanaged switchis designed to provide faster, secure, and more stable network. One advantage that makes it a powerful switch is that it supports network redundancy protocols/technologiessuch asEthernet Ring Protection Switching (ERPS), iA-Ring, Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and Media Redundancy Protocol (MRP). These protocols provide better network reliability and decrease recovery time down to less than 20 ms.

Atop's managed Layer-3 switches add to all these features above mentioned, typically present into a Layer-2 managed switch, also Routing capability through IPv4 static routing, RIPv1/v2 and OSPFv2 dynamic routing. Unlike Switching (where packet addressing is made based on the MAC address), Layer-3 switches route the packet based on the IP address.

Atop'smanaged switchsupports a wide range of IEEE standard protocols. This switch is excellent for keeping systems running smoothly, reliable for preventing system damage or losses, and friendly to all levels of users. The goal of this innovative product is to bring users an enhanced networkmanagement experience.

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 industrialLayer-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 usedin 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)Server/Relay/Client with Option 66/67
- Time Synchronization
  - Network Time Protocol (NTP)Server/Client
  - Simplified Network Time Protocol (SNTP)
  - IEEE 1588 Precision Clock Synchronization Protocol(PTP)v2 hw- E2E TC and sw-Boundary Clock
- Port Mirroring
- Quality of Service (QoS) Traffic Regulation
- Link Aggregation Control Protocol (LACP)
- Link Layer Discovery Protocol (LLDP)
- Medium Access Control (MAC) Filtering
- Generic Attribute Registration Protocol (GARP) / GARP Multicast Registration Protocol (GMRP)/GARP VLAN Registration Protocol (GVRP)
- Internet Group Management Protocol(IGMP),
- Protocol Independent Multicast (PIM), PIM Sparse Mode (SM), PIM Dense Mode (DM), PIM Source Specific Mode (SSM)
- Distance Vector Multicasting Routing Protocol (DVMRP)
- Simple Network Management Protocol (SNMP) v1/v2/v3 (with MD5 Authentication and DES encryption)
- SNMP Inform
- Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol(MSTP)/Media Redundancy Protocol (MRP)
- 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 (selected models only)
  - MACsec
  - 802.1AE authentication and key exchange
- Ring
  - Ethernet Ring Protection Switching (ERPS)
  - iA-Ring
  - Compatible-Ring
  - Compatible-Chain
  - U-Ring
- Alarm System (with E-mail Notification or Relay Output)
- Industrial Protocols
  - Modbus/TCP
  - Profinet (including MRP Ring)
- Layer-3 Switching:
  - IP Routing
  - IPv4 Routing
  - Routing Information Protocol (RIP)v1/v2
  - OSPFv2 (Open Shortest Path First Protocol for IPv4)
- Virtual Router Routing Protocol (VRRP)

2 Configuring with a Web Browser

Chapter 2 explains how to access the industrial managed switchfor the first time. There are three ways to configure this Ethernet Switch:

1. Web browser
2. Telnet console
3. Serial console

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 consoleand the switch.There are only a few differences among these three methods. Users are recommended to use the web browser method to configure the system because of its user-friendly interface.

2.1 Web-based Management Basics

Users can access the managed switch easily usingtheir web browsers (Internet Explorer 8 or 11, Firefox44, Chrome 48 or later versions are recommended). We will proceed to use a web browser to introduce the managed switch's functions.

2.1.1 Default Factory Settings

Belowis a list of default factory settings. This information will be used during the login process. Make sure that the computer accessing the switch has an IP address in the same subnet and the subnet mask is the same.

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

2.1.2 Login Process and Main Window Interface

Beforeuserscan access the configuration,they have to log in. This can simply be done in two steps.

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

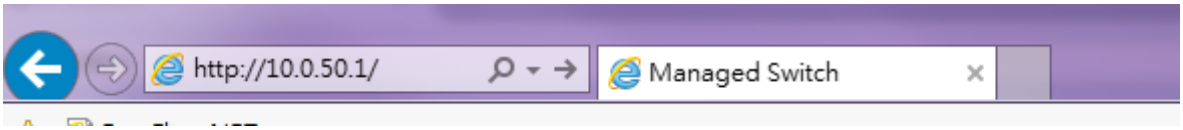


Figure 2.1IP Address for Web-based Setting

After the login process, the main interface will show up, as shown in Figure 2.2. The main menu (left side of the screen)provides the links at the top-level links of the menu hierarchy and by clicking each item allows lower-level links to be displayed. Note that in this case the Port 5 is highlighted in green, indicating that the port is being connected. Detailed explanations of each subsection will be addressed later as necessary.

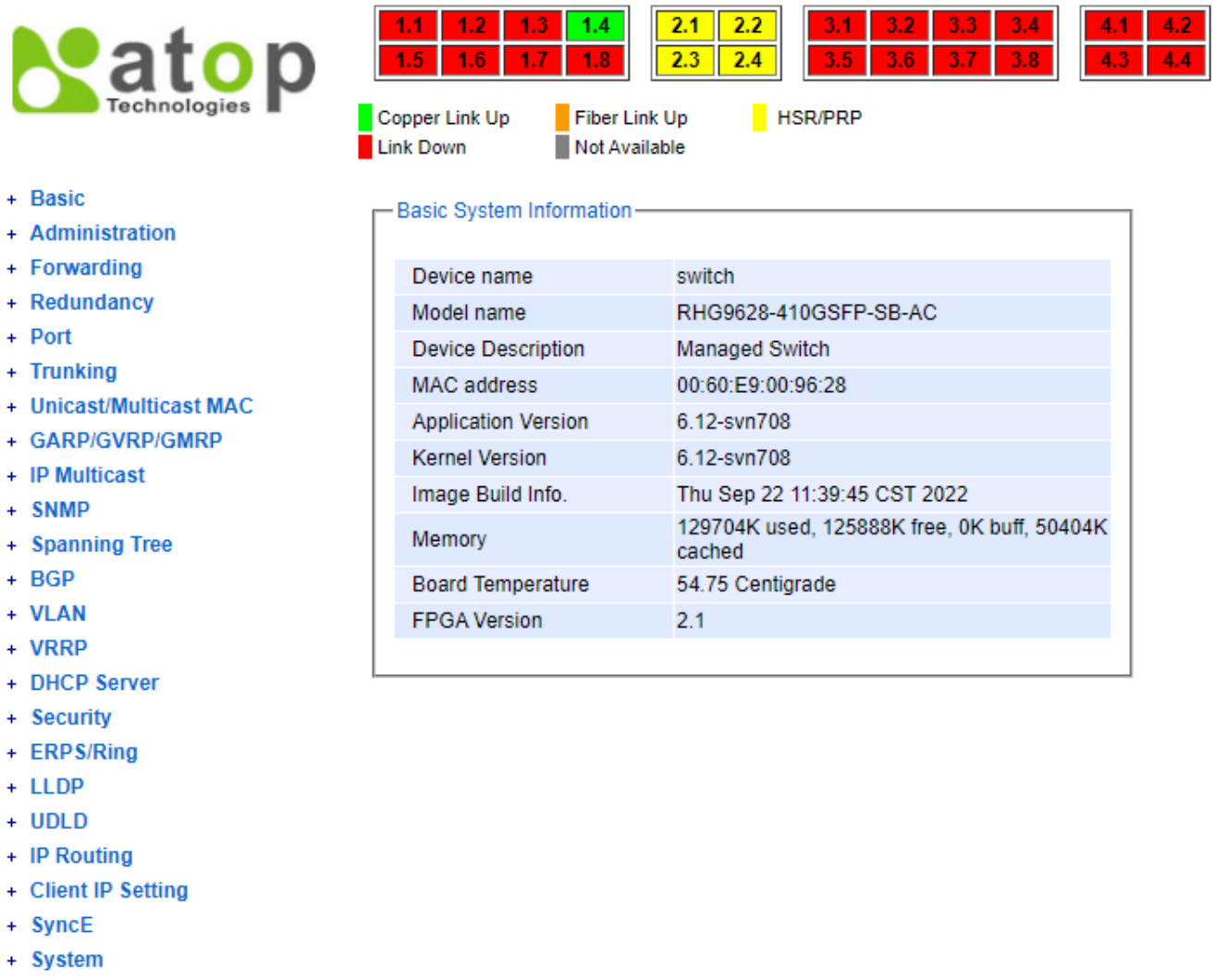


Figure 2.2Default Web Interface

2.2 Basic Information

To help users become familiar with the device, the **Basic**section provides important details of the switch. This is also the main welcome screen once the user has logged in. The details make it easier to identify different switches connected to the network. The Basic section is categorized into sixsubsections as shown in the left panel of Figure 2.3.

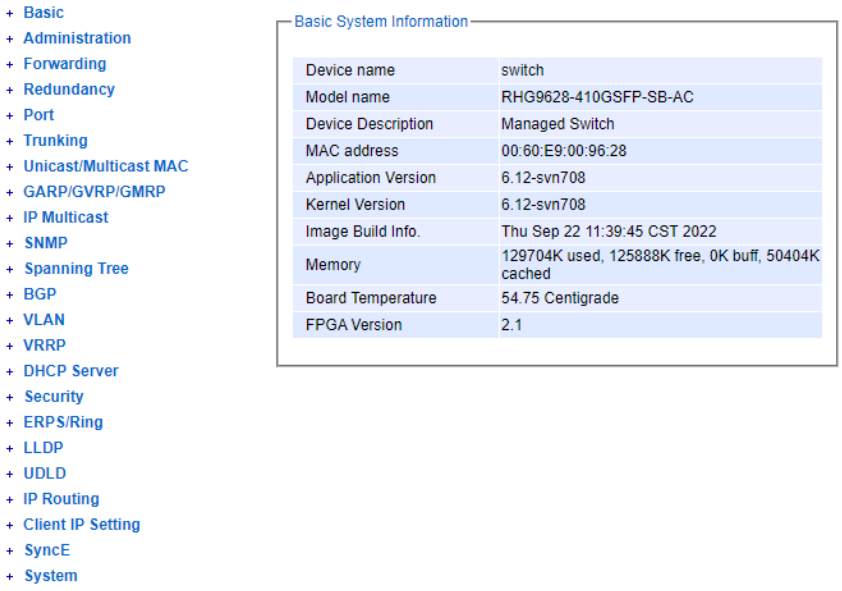


Figure 2.3Basic Information Dropdown Menu

2.2.1 Sys Info

This subsection provides basic system information of Atop's industrial managed switch. The user can check the device name, model name,device description, MAC address, firmware version (application version & kernel version),image build information, memory usage of the switch, and current board's temperature. Note that Atop's firmwaregenerally consists of applicationversionand kernel version. Figure 2.4 depicts an example of Basic System Information of RHG9628-410GSFP-BC-DC. Table 2.1summarizes the description of each basic information.

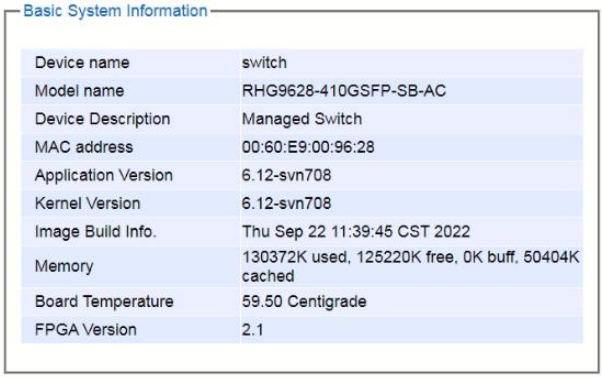


Figure 2.4Details of Sys Info Webpage

Table 2.1Descriptions of the Basic information

Label	Description
Device name	The alias of the device used to distinguish it among different devices
Model name	The device's complete model name

Device Description	The model type of thedevice
MAC address	TheMAC address of the device
Application Version	The current application version of the device
Kernel Version	The current kernel version of the device
Image Build Info.	Information about the firmware image such as date of creation
Memory	The current RAM'savailability and the size of cached and shared memory
Board Temperature	The current temperature of the board inside the chassis in degree Celsius(a.k.a.Centigrade)
FPGA Version	The current FPGA version of the device

2.2.2 Device InformationSetting

Users can assign device's details to Atop's switch in this subsection. By entering unique and relevant system information such as device name, device description, location, and contact, this information can help identify one specific switch among allother devices in the network that supports SNMP. Please click on the "**Update**" button to update the information on the switch. Figure 2.5shows Device Information Setting page of an RHG9628 managed switch model.Table2. summarizes the device information setting descriptions and corresponding default factory settings.

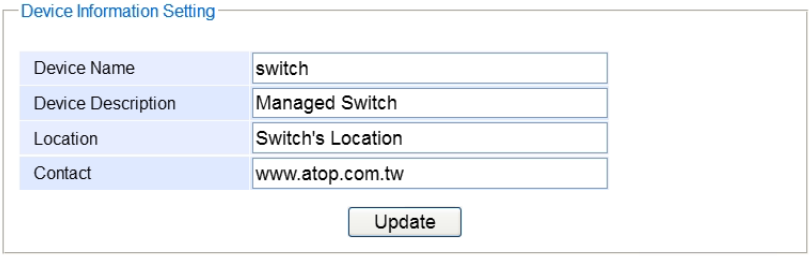


Figure 2.5Details of Device InformationSettings Webpage

Table2. Descriptions of the System Settings

Label	Description	Factory Default
Device Name	Specifies a particular role or application of different switches. The name entered here will also be shown inAtop's Device Management Utility. Max. 63 Char.	switch
Device Description	Detailed description of the unit. Max. 63 Characters.	Managed Switch
Location	Location of the switch. Max. 63 Characters.	Switch Location
Contact	Provides contact information for maintenance. Enter the name of whom to contact in case a problem occurs. Max. 63 Characters.	www.atop.com.tw

2.2.3 Console Setting

In this chapter, we use a web browser for configuring the switch. For the serial console method, please go to Chapter 3 Configuring with Serial Consolefor more detail on how to connect console to the switch. The **Console Setting** here only shows thesetting parameters of a serial console's connection, which can be used by a console software such as Tera Term. Figure 2.6below shows an example of the serial console'sconnection parameters.

Console

Baud Rate	115200 bits/second
Stop	1 bit
Data	8 bits
Parity	None
Flow Control	None

Figure 2.6Setting Parameters for the Console Method

2.2.4 Protocols Status

Protocols Status subsection reports status of all protocols in the switch. While users can view status of all protocols at once in this webpage, the detailed explanation of each protocol and method will be provided in the following sections. Figure 2.7 shows the web interface for the Protocol Status page.

Protocol Status

Protocol	Status
SNTP	Disabled
PTP	Disabled
LACP	Disabled
GVRP	Disabled
GMRP	Disabled
IGMP	Disabled
SNMP	Disabled
STP	Disabled
RSTP	Disabled
MSTP	Disabled
802.1x	Disabled
ERPS	Disabled
IA-Ring	Disabled
Compatible-Ring	Disabled
U-Ring	Disabled
LLDP Tx	Enabled
LLDP Rx	Enabled
Compatible-Chain	Disabled
MRP	Disabled
NTP Server	Disabled
Telnet	Enabled
SSH	Enabled
MLD	Disabled
DHCP Server	Disabled
VRRP	Disabled
PIM Sparse Mode	Disabled
PIM SSM	Disabled
PIM Dense Mode	Disabled
DVMRP	Disabled
UDLD	Disabled

Figure 2.7Protocol Status Webpage

2.2.5 Power Status

Atop'smanaged switch features dual VDC powersupply inputs. For Non-PoE models, 9-57VDC can be supplied to Power Input 1 (V1+ and V1- pins)and/or Power Input 2 (V2+and V2- pins).For PoE models, 45-57VDC should be supplied under 802.3af mode and 51-57VDC should be supplied under 802.3at mode. For instance, the RHG9628-410GSFP-BC-DC has the following three power ratings: 9-57VDC with a maximum current of 2.8 Amperes (No PoE mode), 45-57VDC with a maximum current of 1.7 Amperes (802.3af mode), and 51-57VDC with a maximum current of 2.3 Amperes (802.3at mode).Figure 2.8shows the status of each power input. A "**Not Connected**" status means that the power on that supply input is either not connected or a "**Fault**" status means that the power is not supplied properly.

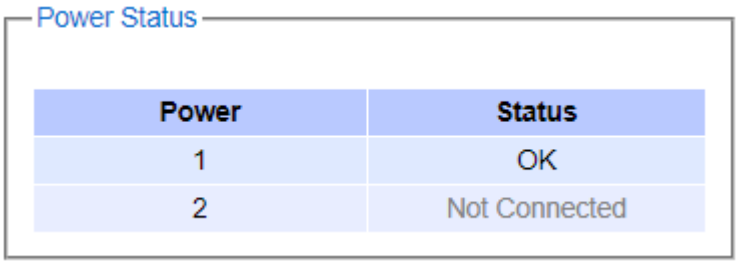
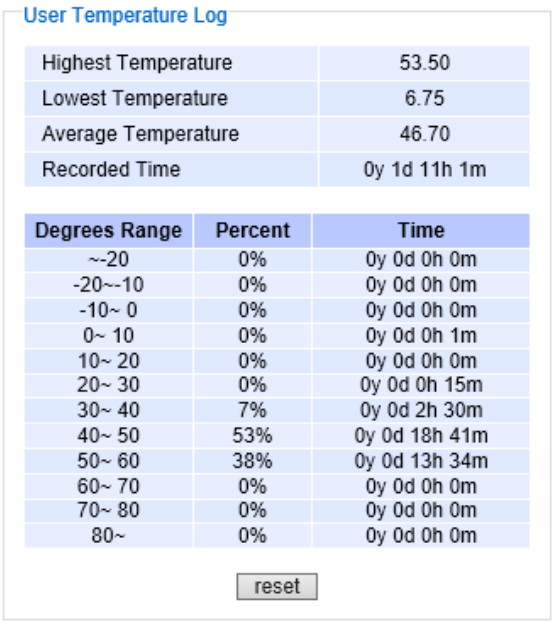


Figure 2.8Power Status Webpage

2.2.6 Temperature Log

This subsection provides user and system temperature logs. There are summary statistics and distribution of temperature information for each log. The highest temperature, the lowest temperature and the average temperature are reported in degree Celsius. Additionally, there is a recorded time which shows the time since the temperature log were recorded. Under the summary statistics, there is a table showing the ranges of temperature, percentages of time in each range, and amount of time in each range. The user can reset the user statistics by clicking on the **Reset**button at the bottom of User Temperature Log. However, the system temperature log cannot be reset by the users.Note that the information is not automatically update. Information provided in this webpage will help the users to monitor the status of the industrial managed switch in harsh environment. The users have to click reload on the web browser to update for the latest statistics. Figure 2.9shows the **User Temperature Log**box and Figure 2.10 shows the System Temperature Log box.

Note that there is a sensor component in the industrial managed switch which can detect the inside temperature. The software inside the switch can read the sensor's data and transform it into temperature in a unit of degree Celsius. Because the device is airtight, the inside temperature will be higher than the outside temperature around 20 degrees.For the industry level switches, the lowest operating temperature (outside) will be around-20 to -40 degreesCelsius and the highest operating temperature (outside) will be around 70 to85 degrees Celsius.



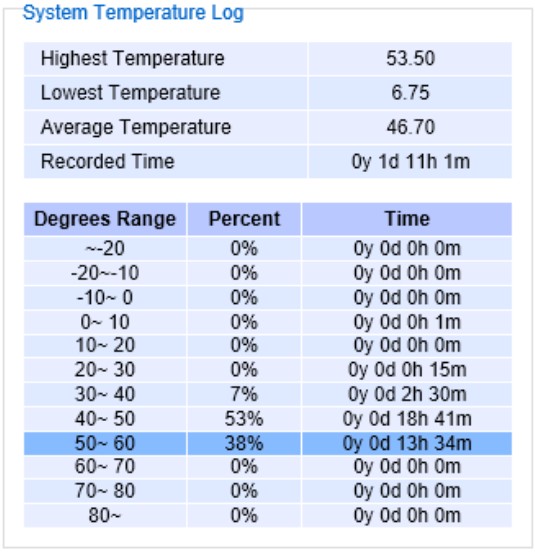
User Temperature Log

Highest Temperature	53.50
Lowest Temperature	6.75
Average Temperature	46.70
Recorded Time	0y 1d 11h 1m

Degrees Range	Percent	Time
~-20	0%	0y 0d 0h 0m
-20~-10	0%	0y 0d 0h 0m
-10~ 0	0%	0y 0d 0h 0m
0~ 10	0%	0y 0d 0h 1m
10~ 20	0%	0y 0d 0h 0m
20~ 30	0%	0y 0d 0h 15m
30~ 40	7%	0y 0d 2h 30m
40~ 50	53%	0y 0d 18h 41m
50~ 60	38%	0y 0d 13h 34m
60~ 70	0%	0y 0d 0h 0m
70~ 80	0%	0y 0d 0h 0m
80~	0%	0y 0d 0h 0m

reset

Figure 2.9User Temperature Log



System Temperature Log

Highest Temperature	53.50
Lowest Temperature	6.75
Average Temperature	46.70
Recorded Time	0y 1d 11h 1m

Degrees Range	Percent	Time
~-20	0%	0y 0d 0h 0m
-20~-10	0%	0y 0d 0h 0m
-10~ 0	0%	0y 0d 0h 0m
0~ 10	0%	0y 0d 0h 1m
10~ 20	0%	0y 0d 0h 0m
20~ 30	0%	0y 0d 0h 15m
30~ 40	7%	0y 0d 2h 30m
40~ 50	53%	0y 0d 18h 41m
50~ 60	38%	0y 0d 13h 34m
60~ 70	0%	0y 0d 0h 0m
70~ 80	0%	0y 0d 0h 0m
80~	0%	0y 0d 0h 0m

Figure 2.10 System Temperature Log

2.3 Administration

In this section, users will be able to configure**Password**, **IP Settings**, **IPv6 Setting**,**Ping**, **Ping6**, **Mirror Port**, **System Time**, **Modbus Setting**, **PTP**, **SSH**, **Telnet**,and **DIP Switch**. Figure 2.11shows the Administration section with the list of its subsections on the left of the screen.

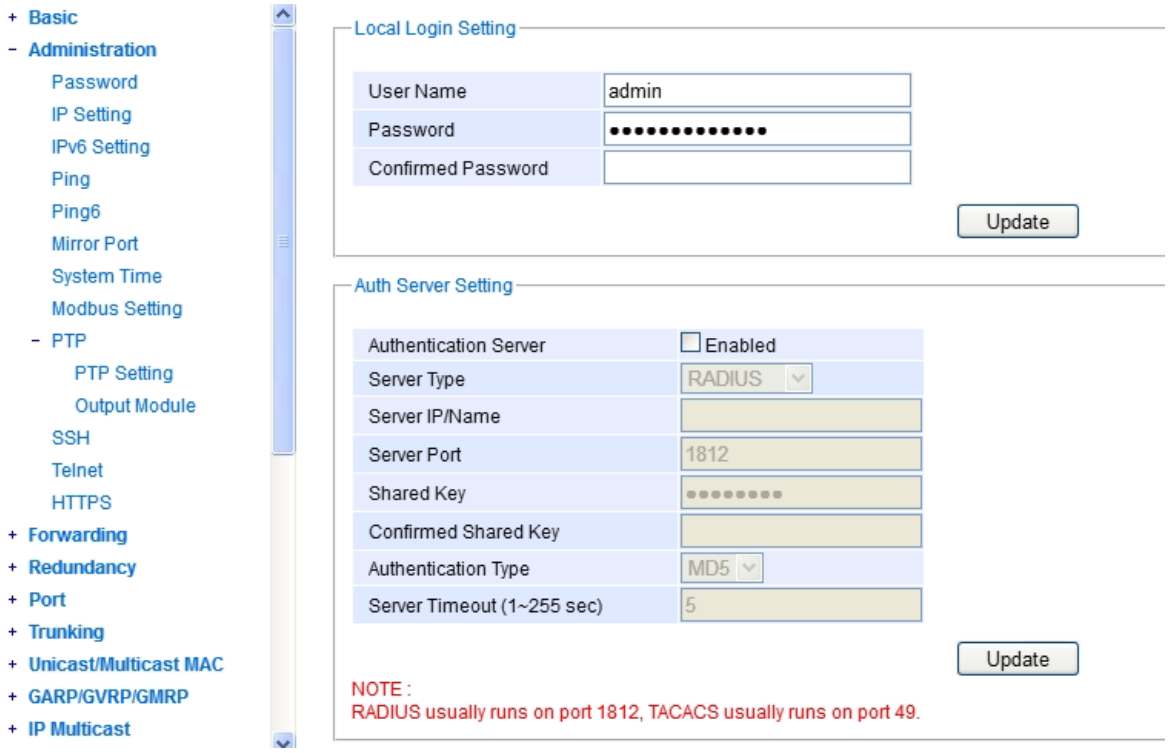


Figure 2.11Administration DropdownMenu

2.3.1 Password

Password "**default**" is set for the device when it is manufactured. Users can modify it password to ensure overall system security. The user name and password can be updated in this page as shown inFigure 2.12. Setting for a local authentication is introduced in this subsection, while setting for a remote authentication is described in later sections. The user name and password set here are applied to all types of access to Atop's switch: web management user interface (UI), secure shell (SSH), and command line interface (CLI). Please click on the "**Update**" button to update the user name and password information on the switch.
Table 2.2 summarizes the description of each field.

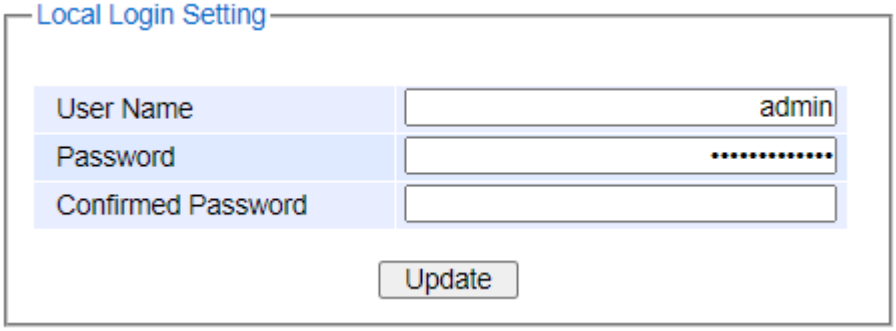


Figure 2.12Password Setting Webpage

Table 2.2Descriptions of Password Setting

Label	Description	Factory Default
User Name	User's Name. Max. 15 characters	admin
Password	Password to log-in. Max. 15 characters	default

Confirmed Password	Re-type the password. This has to be exactly the same as the password entered in the above field. Max. 15 characters	NULL

In addition to the local authentication, the switch can be configured to request for authentication through a centralized RADIUS or TACACS+ server when the local authentication fails. Figure 2.13shows the setting parameters for authentication server while Table 2.3 summarizes the authentication server settings. For theRADIUS and TACACS+comparison, please refer toTable 2.4 so that youcan choose the solution that best suits your needs.

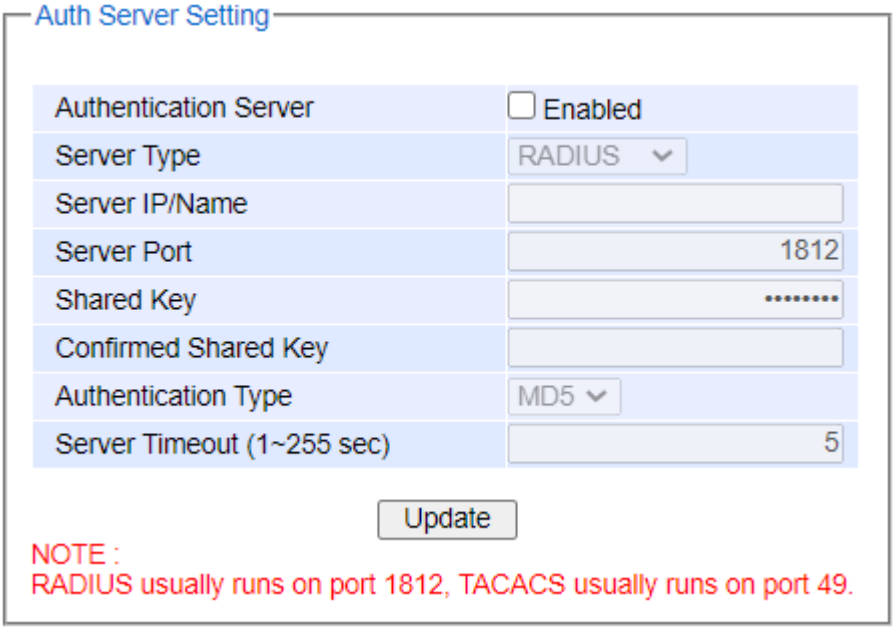


Figure 2.13 Authentication Server Setting

Table 2.3Authentication Server Settings

Label	Description	Factory Default
Authentication Server	Enable / disable authentication through a remote authentication server	Disabled
Server Type	ChooseAuthentication Server type: RADIUS or TACACS+. See notes below for a detailed explanation.	RADIUS
Server IP/Name	IP address of the authentication server	NULL
Server Port	Communication port of the authentication server	1812
Shared Key	The key used to authenticate with the server. Max. 15 characters.	12345678
Confirmed Shared Key	Re-type the shared key. Max. 15 characters.	NULL
Authentication Type	Authentication mechanism. For RADIUS: MD5. For TACACS+:ASCII, PAP, CHAP, MSCHAP.	RADIUS is MD5 TACACS+ is ASCII
Server Timeout (1~255 sec)	The time out period of waiting for a response from the authentication server. This will affect the time that the next login	5

Label	Description	Factory Default
	prompt shows up in case that the server is not available.	

***NOTE:**

RADIUS (Remote Authentication Dial in User Service):

RADIUS is an access server that uses authentication, authorization, and accounting(AAA) protocolfor authentication and authorization. It is a distributed security system that secures remote access to networks and network services against unauthorized access. TheRADIUS specification is described in RFC 2865, which obsoletes RFC 2138.

TACACS+ (Terminal Access Controller Access-Control System Plus):

TACACS+is a security application that provides centralized validation of users attempting to gain access to a router or network access server. The TACACS+specification is described inCisco's TACACS+RFC draft.

Table 2.4Comparison 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 passwordis encrypted	Entire packet is encrypted

2.3.2 IP Setting

In this subsection, users may modify network settings of Internet Protocol version 4 (IPv4) for the managed switch. Additionally, onindustrial managed switch, any virtual local area network (VLAN) group can be assigned an IP interface address. There are two types of IP setting that can be done in this subsection:1) setting managed (or management) interface IP address and 2) setting IP interface address for VLAN. Note that a VLAN group must be created first as described in Section **錯誤! 未知的選項引數。** before assigning an IP interface address in this section. Each IP interface address is a separated subnet. The user can configure multiple IP interface addresses on the switch. The IP interface of VLAN 1 is the default managed (or management) interface of the switch as configured in Section 2.14.1.

This subsection isdivided into two parts: **IP Setting**and **IP Interface**. The IP Setting part is depicted in Figure 2.14. The **Managed Interface VID** has a default value of 1. However, the **Gateway**, the **Primary DNS** and **Secondary DNS** can be entered. If the user set gateway or DNS on this page, the managed switch will not set the gateway or the DNS from DHCP server. After entering the desired information, please click **Update** button to change the IP Setting.

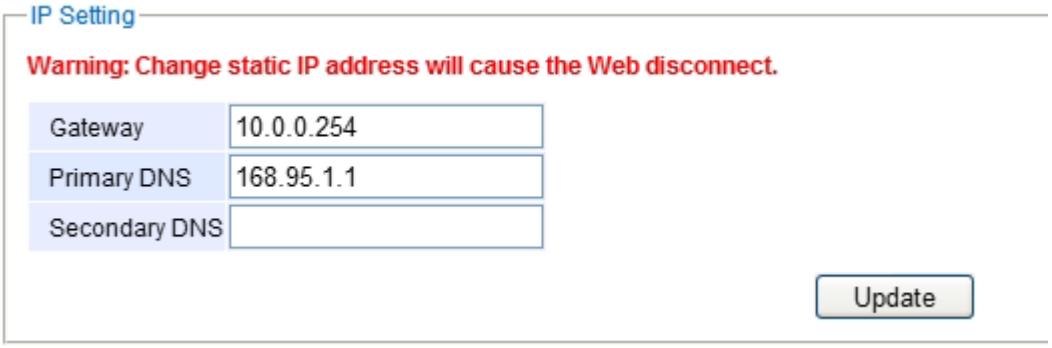


Figure 2.14 IP Setting under IP Setting Webpage

The second part of IP Setting section is the **IP Interface** part as shown in Figure 2.15. In this part, there is a table at the bottom that lists the IP interface information of each VLAN Identificationnumber (VID).The user can configure IP interface address for VLAN 1 to 4094 in this IP interface part. Note that the maximum number of IP interface is 32. The user can remove each entry in the table by clicking on the **Remove** button. The user can configure the IP Interface address for each VLAN ID (VID) in this part. To change the IPv4 address of the managed switch (default is 10.0.50.1), the user can enter a new **Static IP Address** and a new **Subnet Mask**, and select**VID = 1**from the drop-down list then clicking **Update** button. Note that 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.

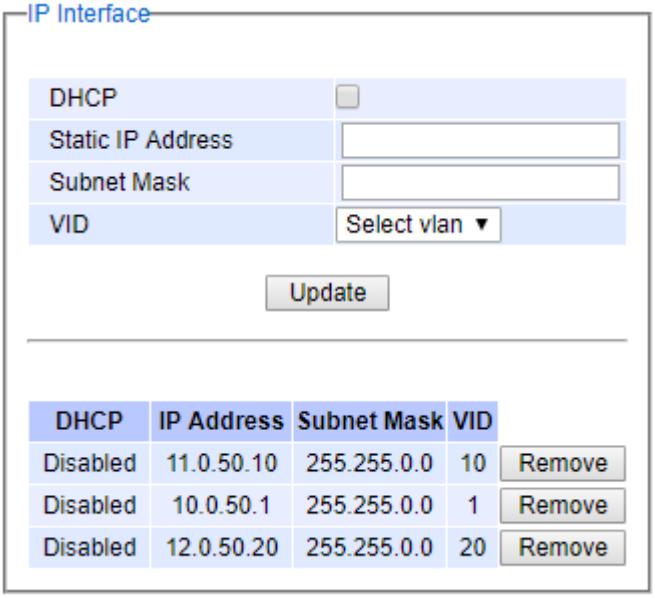


Figure 2.15 IP Interface Part under IP Setting Webpage

To configure IP interface address for other VLAN Identification number (VID), enter the desired **Static IP Address**and **Subnet Mask**, and select a**VID**from the drop-down list, and then click on the **Update** button.Additionally, each IP interface of the switch can enable the Dynamic Host Configuration Protocol (DHCP) by checking the **DHCP**box option to obtain an IP address and related information automaticallyfrom a DHCP server thus reducing the work for an administrator. Note that when checking the **DHCP** option, the **Static IP Address** and the **Subnet Mask**will be inactive. The only field that can be selected is the **VID** which means that the VID will obtain the IPv4 address automatically for its interface. Note that before deleting any VLAN group as described in Section2.14.2.1, please make sure that the VID does not establish an IP interface. The description of each field and its default value in IP Setting webpage are summarized in Table 2.5.

Table 2.5Descriptions of IP Settings

Label	Description	Factory Default
DHCP	By checking this box, an IP address and related fields will be automatically assigned. Otherwise, users can set up the static IP address and related fields manually.	Uncheck
Static IP Address	Display current IP address. Users can also set a new static IP address for the device.	10.0.50.1
Subnet Mask	Display current Subnet Mask or set a new subnet mask	255.255.0.0
Gateway	Show current Gateway or set a new one	0.0.0.0
Primary DNS	Set the primary DNS IP address to beused by your network	NULL
Secondary DNS	Set the secondary DNS IP address. The Ethernet switchwill locate the secondary DNS server if it fails to connect to the Primary DNS Server.	NULL
VID	Virtual local area network identification number is the ID value for VLAN that need to be configured with IPv4 address.	NULL

2.3.3 IPv6 Setting

This subsection enables Atop's industrial managed switch to operate in Internet Protocol version 6 (IPv6) network. The webpage is subdivided into two parts:**IPv6 Setting** and **IP interface for IPv6**. The first part called **IPv6 Setting** is shown in Figure 2.16. This part also provides the current IPv6 address information (**Link-Local Address**)and allows the users to configure the**Gateway** and the**Domain Name Service (DNS)**for IPv6 network. If the users change any DNS setting, please clicking on the **Update** button to allow the new configuration to take effect.

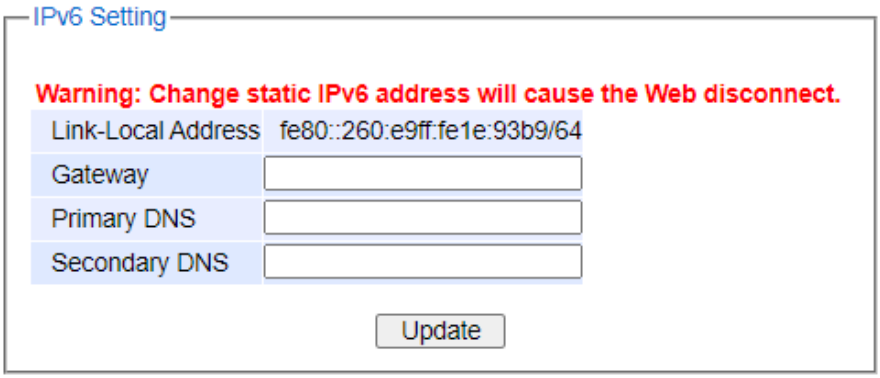


Figure 2.16 IPv6 Setting Partof IPv6 Setting Webpage

The second part called **IP Interface for IPv6** is shown in Figure 2.17. Similar to IPv4 Setting in previous subsection, the IPv6 Setting also allows the user to set IPv6 interface address for a virtual local area network (VLAN) group based on the **VLAN identification number (VID)**. For managed switch, the users haveoptions to enable Autoconfig, DHCPv6, or Manual setting. Note that in IPv6 network, there are three types of auto configuration: stateless, stateful, and a combination of both. The "**Autoconfig**" option here is the stateless configuration, while the "**DHCPv6**" option is the stateful configuration. If the users check both the **Autoconfig** and the **DHCPv6** options, the switch will use the combination of stateless and stateful configuration. When selecting the "**Manual**" option, the users will have toenterthe **Global Unicast Address**, **Prefix Length**, and **Gateway**. The users can select the VID from the drop-down list "**Select vlan**". After finishing the setting, please click on the **Update** button to allow the new configuration to take effect.

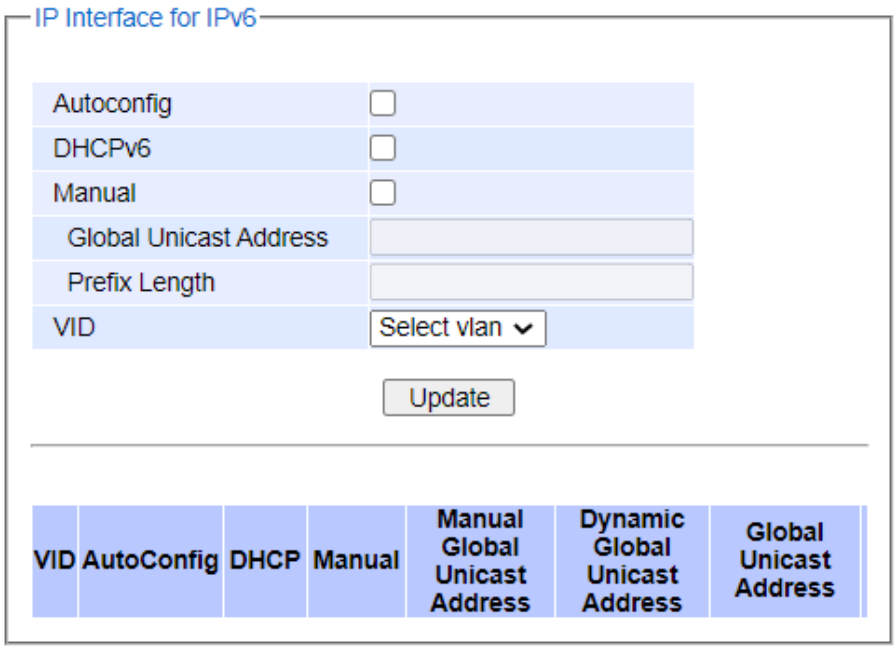


Figure 2.17 IP Interface for IPv6 Part of IPv6 Setting Webpage

At the bottom of this part as shown in Figure 2.17, there is also a list of IPv6 interface setting for each **VLAN identification number (VID)**. The users can click on the **Remove** button at the end of the line to remove any entry (or remove IPv6 interface address setting) from this list which is similar to the IPv4 Setting in previous subsection. Table 2.6explains each field in the **IPv6 Setting** webpage.

Table 2.6Description of IPv6 Setting

Label	Description	Factory Default
Autoconfig	By checking this box, all IPv6 setting will be automatically configured for the users. This option is based on the stateless autoconfiguration in which the switch uses information in router advertisement messages to configure an IPv6 address. The address will be a concatenation of first 64 bits from the router advertisement source address with the Extended Unique Identifier (EUI-64).	Uncheck
DHCPv6	By checking this box, an IPv6 address and related fields will be automatically assigned from a DHCPv6 server in the network. This is a stateful auto configuration in which the switch will generate a DHCP solicit message to the ALL-DHCP-Agents multicast address to find DHCPv6 server. Otherwise, users can set up the IPv6 address manually.	Uncheck
Manual	By checking this box, users must provide Global Unicast Address, Prefix Length, and Gateway address in the following fields. Note that when this option is checked, the next three fields will become active for setting.	Uncheck
Global Unicast Address	Set an IPv6 address that is routable across the Internet and its three high-level bits are 001. The IPv6 address is in the format 2XXX::/3.	NULL
Prefix Length	Set a prefix length for the IPv6 address in previous field.	NULL
Gateway	Set the IPv6 address of an IPv6 Gateway	NULL
Manual DNS	By checking this box, user must manually provide Primary and Secondary DNS addresses for IPv6. Note that when this option is checked, the next two fields will become active for setting.	Uncheck
Primary DNS	Set the primary DNS IPv6 address to beused by your network.	NULL

Label	Description	Factory Default
Secondary DNS	Set the secondary DNS IPv6 address. The Ethernet switchwill locate the secondary DNS server if it fails to connect to the Primary DNS Server.	NULL

2.3.4 Ping

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. Note that this utility is only for IPv4 address. The Ping utility for IPv6 will be provided in the next subsection. Figure 2.18shows the user interface for using the Ping command.

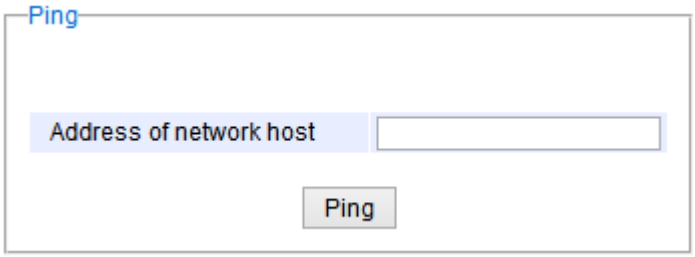


Figure 2.18Ping Webpage

Users can enter an IP address or a domain name into the field to verify network connectivity as shown in Figure 2.19. After entering the IP address/name, please click "**Ping**" button to run the ping function. Example of successfulping resultis shown inFigure 2.20while a failure ping result is depicted in

Figure 2.21.

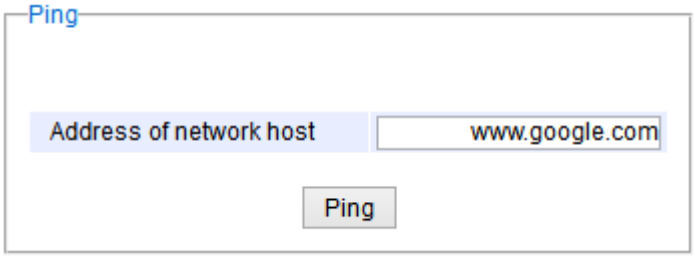


Figure 2.19Example of Ping Command

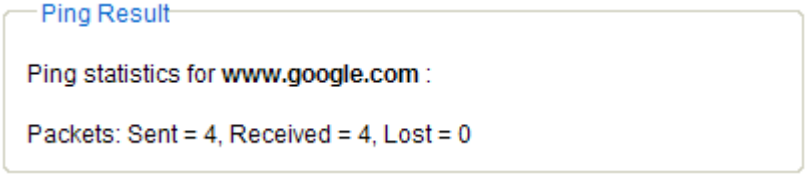


Figure 2.20Example of successful ping command result

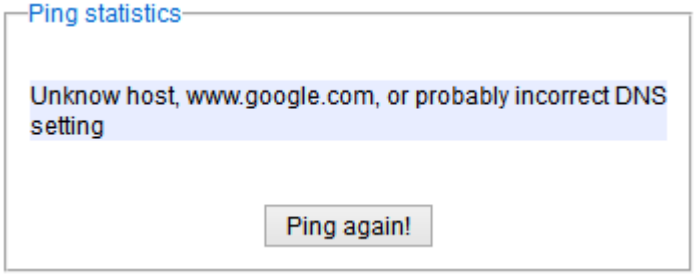


Figure 2.21Example of unsuccessful ping command result

***Note:**

If users entera domain name instead of an IP address, they should assign a DNS first. This can be done through **Administration→**IP Settingas shown in Section2.3.2.

2.3.5 Ping6

Ping6 is a corresponding network diagnostic utility for testing reachability between a destination device and the managed switch in IPv6 network. Figure 2.22shows the user interface for using the Ping command.

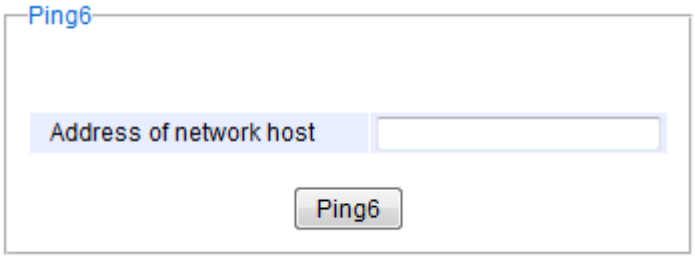


Figure 2.22Ping6 Webpage

Users can enter an IPv6 addressinto the field to verify network connectivity. After entering the IPv6 address, please click "**Ping6**" button to start the ping function. Examples of successful ping6 resultsare shown inFigure 2.23.

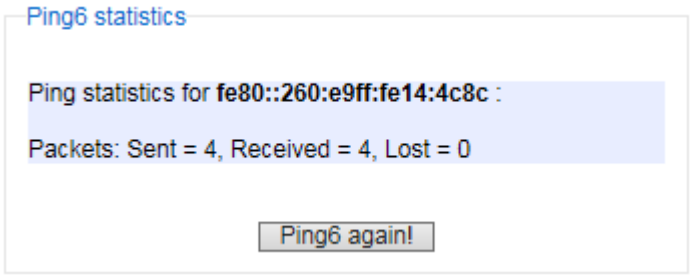


Figure 2.23Example of Successful Ping6 Result

2.3.6 Mirror Port

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 themirrored network traffic can be analyzed by a network analyzer or a sniffer for network performance or security monitoring purposes**.** Figure 2.24shows the Mirror Port webpage. Thedescriptions of port mirroring options are summarized in Table 2.7.

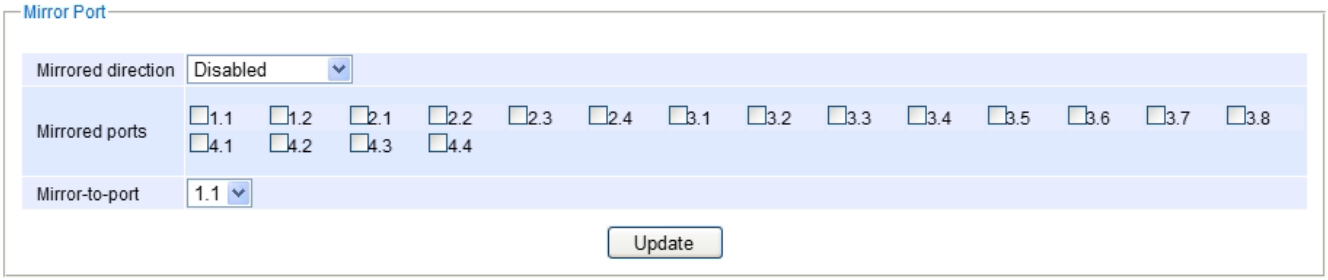


Figure 2.24Mirror Port Webpage

***Note:**
Overflow will occur if the total throughput of the monitoring ports exceeds what the mirror port can support.

Table 2.7Description of Port Mirroring Options

Label	Description	Factory Default
Monitored direction	Select the monitoring direction. - **Disable**: To disable port monitoring. - **Input data stream**: To monitor input data stream of monitored ports only. - **Output data stream**: To monitor output data stream of monitored ports only - **Input/Output data stream**: To monitor both input and output data stream of monitored ports	Disabled
Monitored Port	Select the ports that will be monitored	Unchecked all
Mirror-to-port	Select the mirror port that will be used to monitor the activity of the monitored ports	Port1

2.3.7 System Time

Atop's industrial managed switch has internal calendar (date) and clock (or system time) which can be set manually or automatically. Figure 2.25shows the System Time and SNTP webpage. The users have options to configure **Current Date**and**Current Time** manually. There is a drop-down list of **Time Zone** which can be selected for the local time zone. If the switch is deployed in a region where daylight saving time is practiced (see note below for explanation), please check the **Enable** option for **Daylight Saving Time**. Then, the users will have to enter the **Start Date**, **End Date**, and **Offset** in hour(s).

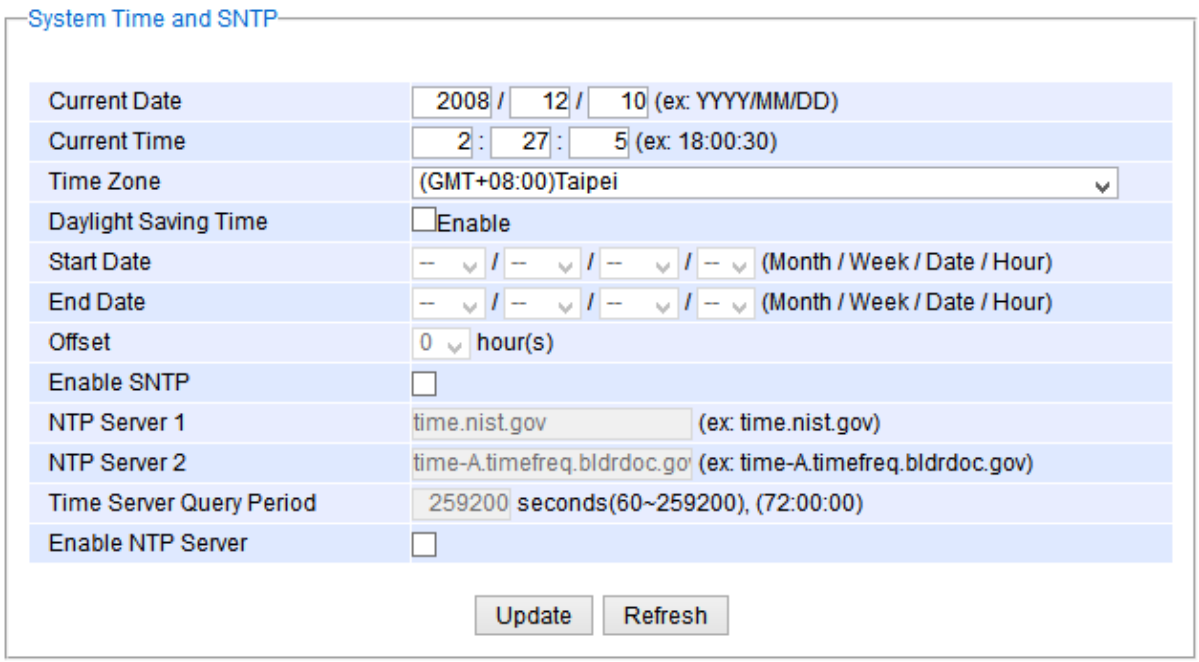


Figure 2.25Webpage for Setting System Time and SNTP

For automatically date and time setting, the users can enable Simple Network Time Protocol (SNTP) by checking the **Enable SNTP**option (see note below for explanation). Then, the users mustenter the NTP Server 1 and NTP Server 2 which will be used as the reference servers to synchronize date and time to. The users can specify the

Time Server Query Period for synchronization which is in the order of seconds. The value for this period will depend on how much clock accuracy the users want the switch to be. Finally, the managed switch can become a network time protocol server for the local devices by checking the box behind the **Enable NTP Server**option. Description of each option is provided in Table 2.8.

Table 2.8Descriptions of the System Time and the SNTP

Label	Description	Factory Default
Current Date	Allows local date configuration in yyyy/mm/dd format	None
Current Time	Allows local time configuration in local 24-hour format	None
Time Zone	The user'scurrent local time	(GMT+08:00) Taipei
Daylight Saving	Enable or disable Daylight Saving Time function	Unchecked
Start Date	Define the start date of daylight saving	NULL
End Date	Define the end date of daylight saving	NULL
Offset	Decide how many hours to be shifted forward/backward when daylight saving time begins and ends. See note below.	0
Enable SNTP	**Enables SNTP** function. See note below.	Unchecked
NTP Server 1	Sets the first IP or Domain address of **NTP Server.**	time.nist.gov
NTP 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.	Time-A.timefreq.bldrdoc.gov
Time Server Query Period	This parameter determines how frequently the time is updated from the NTP server. If the end devices require less accuracy, longer query time is more suitable since it will cause less load to the switch. The setting value can be in between 60 – 259200 (72 hours)seconds.	259,200 seconds
Enable NTP Server	This option will enable network time protocol (NTP) daemon inside the managed switch which allows other devices in the network to synchronize their clock with this managed switch using NTP.	Unchecked

***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.

- SNTP: **S**imple**N**etwork **T**ime **P**rotocol is used to synchronize the computer systems' clockswith a standard NTP server. Examples of two NTP serversare *time.nist.gov* and *time-A.timefreq.bldrdoc.gov.*

2.3.8 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 Modbusslave 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. A Modbus memory mapping table, which lists all the register's addresses inside the managed switch and their descriptions, is provide in 7 Modbus Memory Map. Figure 2.26 shows the Modbus Setting webpage.

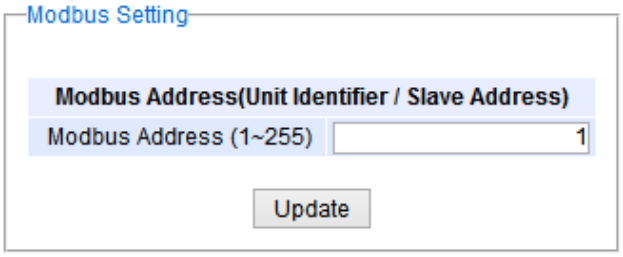


Figure 2.26Webpage for Setting the Modbus Address

Figure 2.26shows the webpage that users can set up the Modbus ID address. Users can use Modbus TCP/IP compatible applications such as **Modbus Poll** to configure the switch. Note that Modbus Poll can be downloadfromhttp://www.modbustools.com/download.html.The Modbus Poll 64-bit version 7.0.0, Build 1027 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 (Thisexample 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 2.27Mapping Table of Modbus Address for Switch's IP Address

1. Make sure that asupervising computer (Modbus Master) is connected to your target switch (Modbus Slave) over Ethernet network.
2. Launch**Modbus Poll** in thesupervising 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 2.28.

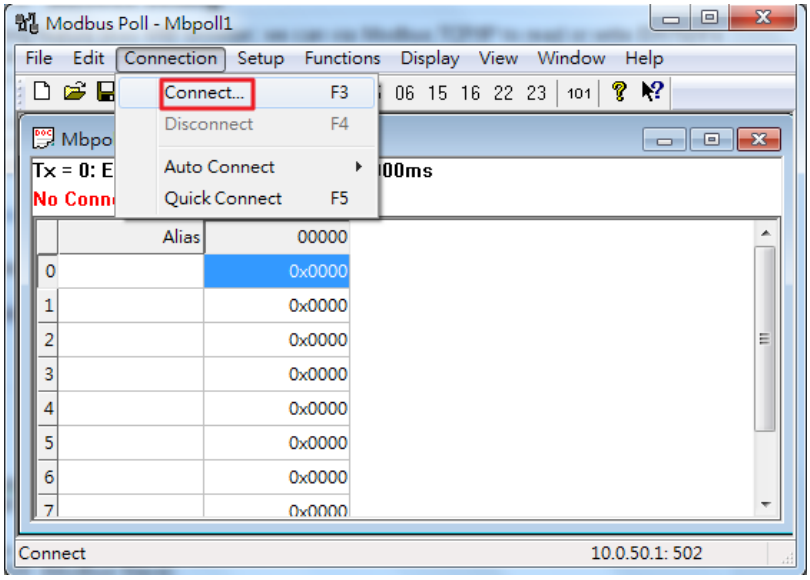


Figure 2.28Entering Connection Setup Menu of the Modbus Poll

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** fieldat the bottom as shown inFigure 2.29. The **Port** number should be set to 502. Then click **OK** button.

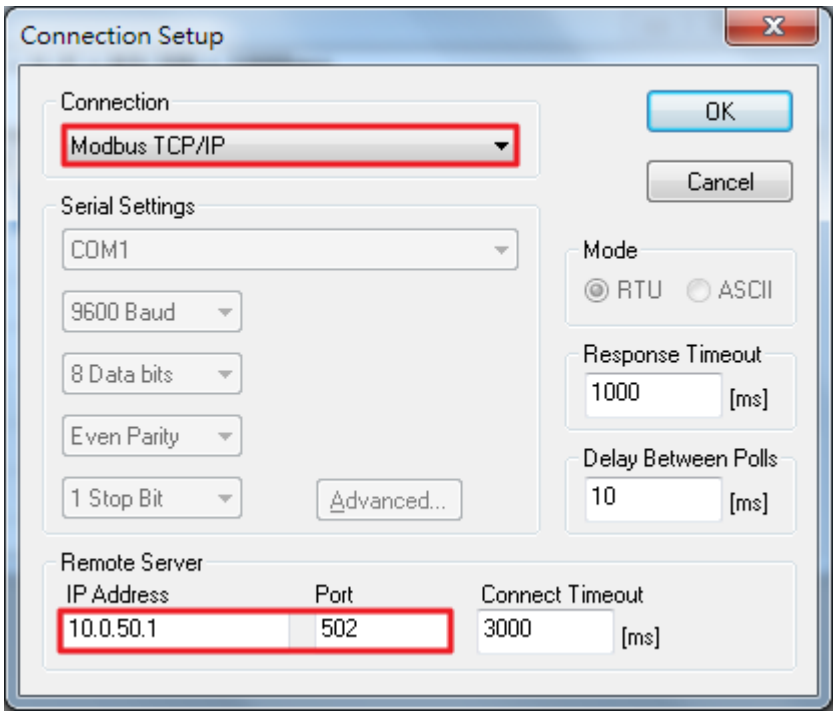


Figure 2.29Modbus Poll Connection Setup

5. On the window Mbpoll1, select multiple cells from row 0 to row 2by clicking on cells in second column of row 0 and row 2 while holding the shift key as shown inFigure 2.30.

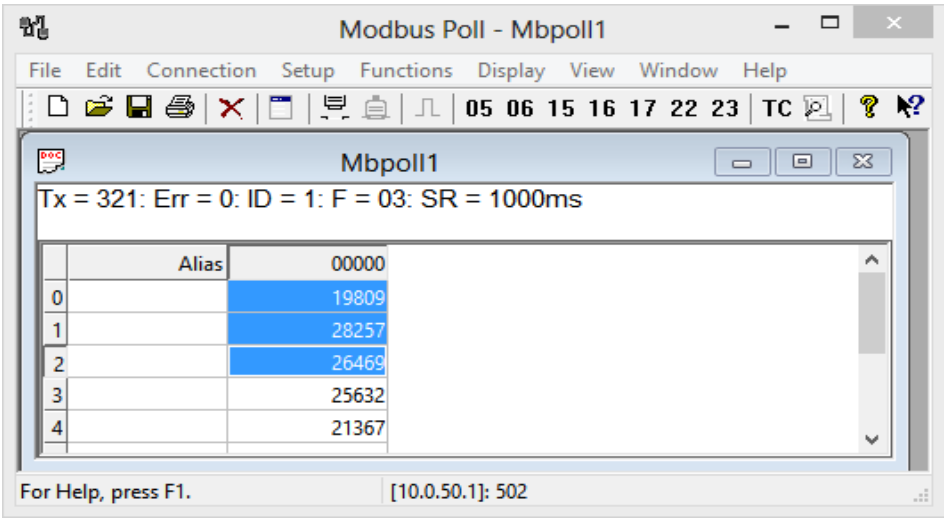


Figure 2.30 Multiple Cell Section in Modbus Poll

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 inFigure 2.31.

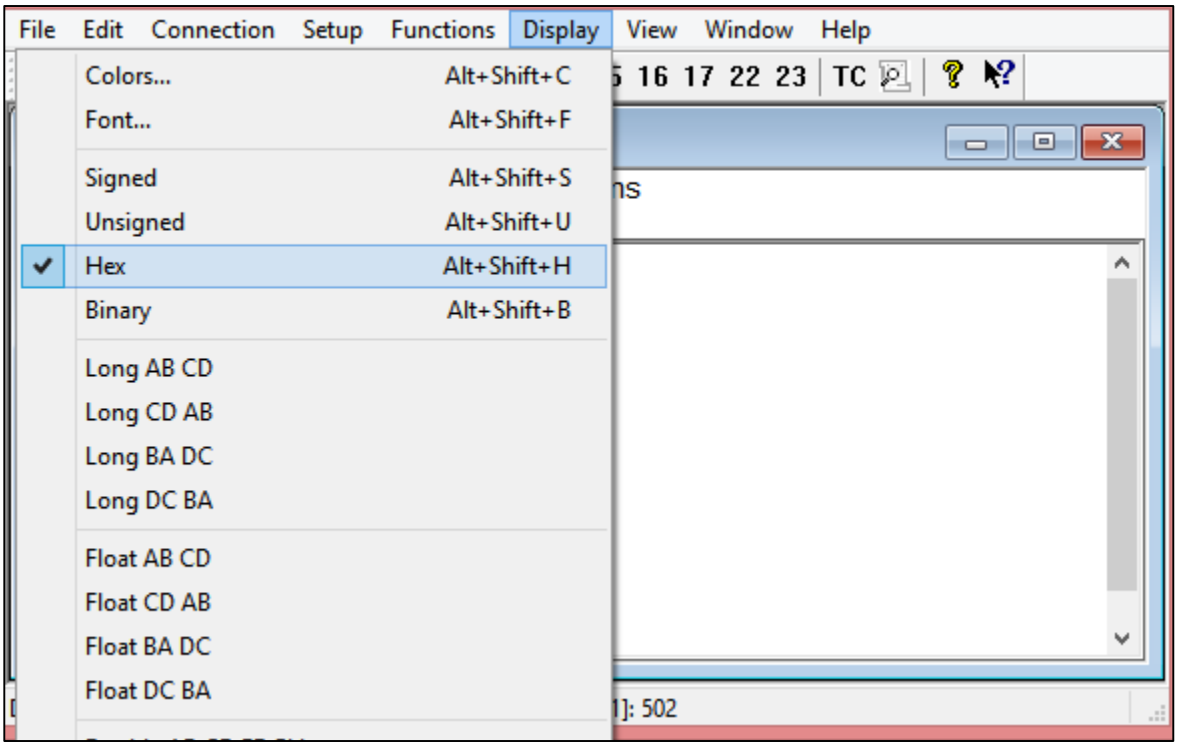


Figure 2.31 Set Display Mode to Hex in Modbus Poll

7. Click on the **Setup** pull-down menu and choose **Read/Write Definition…**as shown inFigure 2.32.

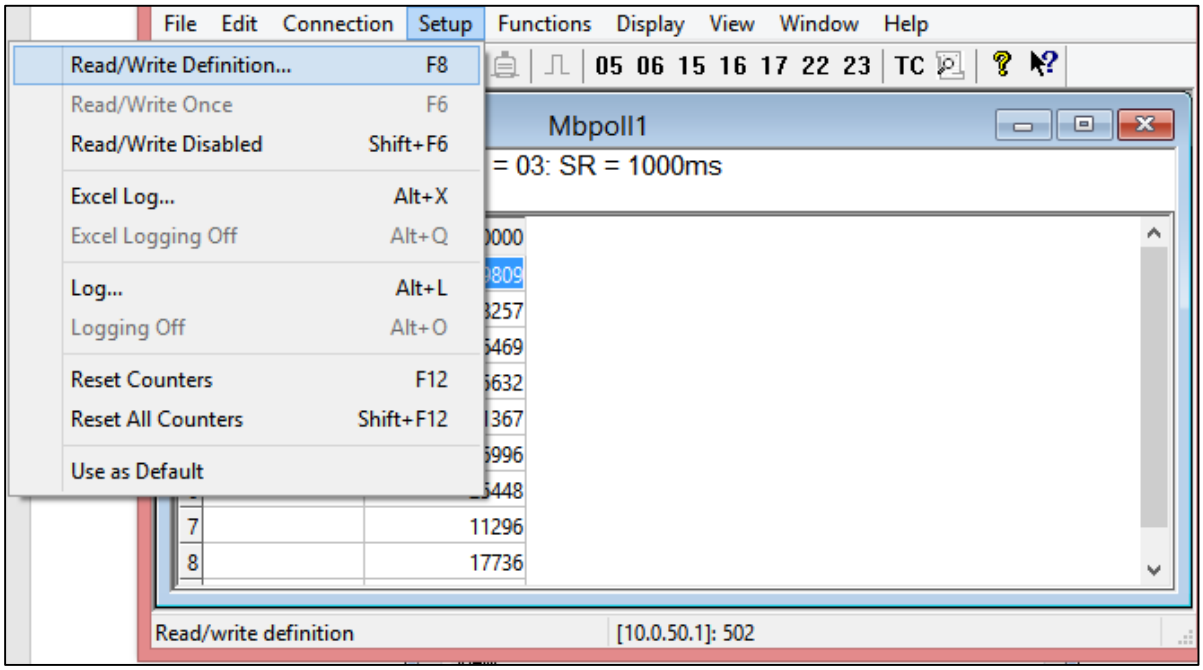


Figure 2.32 Modbus Poll Setup Read/Write Definition

8. Enter the **Slave ID** in the Modbus Poll function as shown in Figure 2.33, which should match the Modbus Address = 1 entered inFigure 2.26in Section 2.3.8 (Modbus Setting).

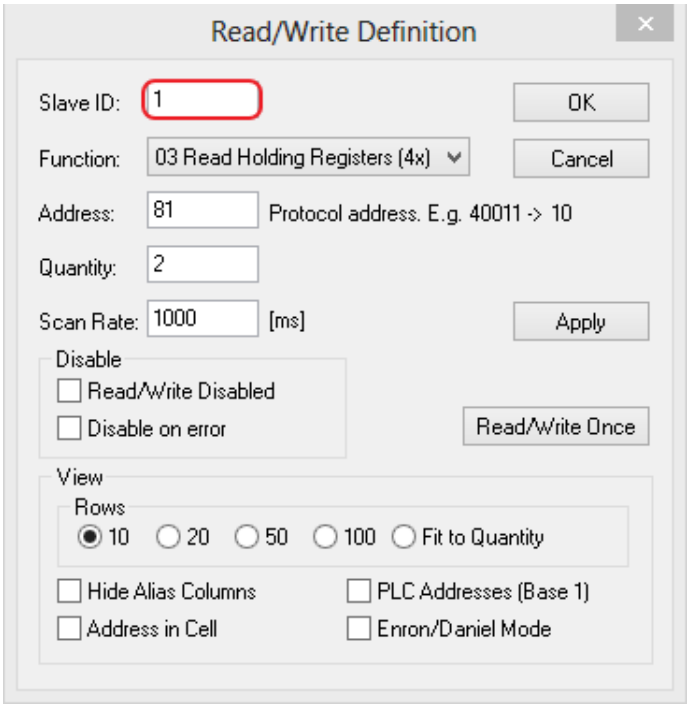


Figure 2.33Slave ID in the Modbus Poll Function is set to 1

9. Select **Function 03** or **04**because themanaged switch supports function code 03 and04 as shown in Figure 2.34.

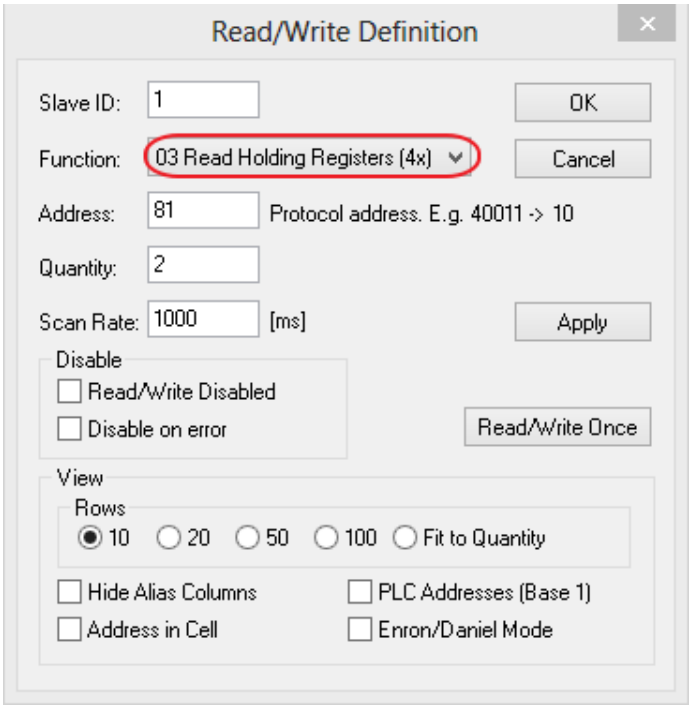


Figure 2.34 Set Code 03 in the Modbus Poll Function

10. Set starting**Address** to 81 and **Quantity** to 2 as shown in Figure 2.35.

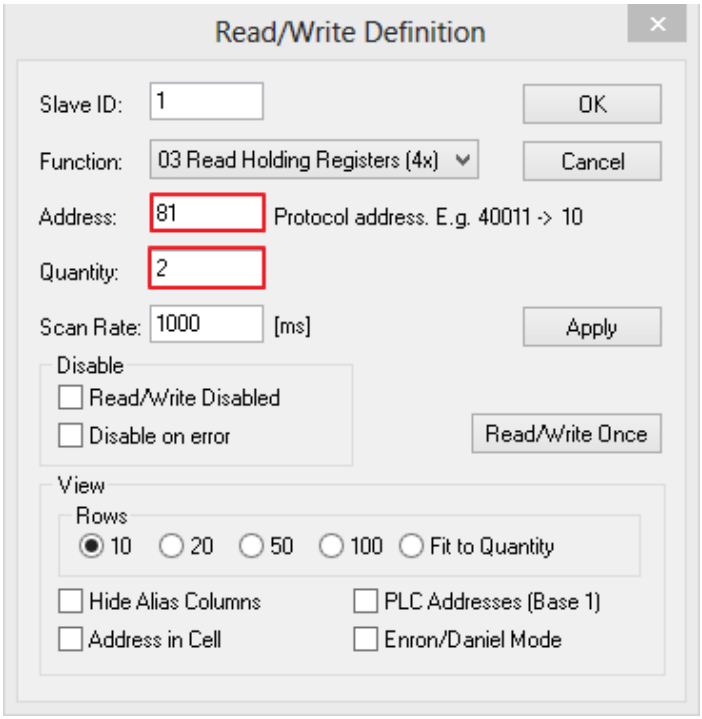


Figure 2.35 Setup Starting Address and Quantity in Modbus Poll

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

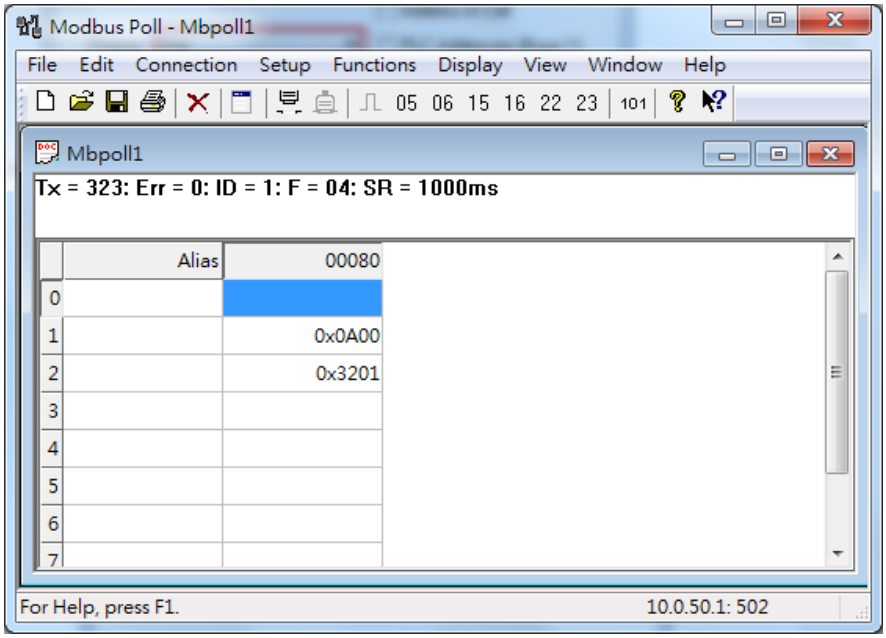


Figure 2.36 Modbus Memory Address 81 and 82 are the location of RHG96xx's IP Address

12. Modbus Poll will get the values 0x0A, 0x00, 0x32, 0x01, which means that the switch's IP is 10.0.50.1as shown in Figure 2.36.

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 2.37Mapping Table of Modbus Address for Clearing Port Statistics

1. Check the switch's Port TX/RX countsin **Port Statistics** page (described in Section 2.6.4) as shown in Figure 2.38.

Port Statistics

Port	Enable	Link	Tx	Tx Error	Tx Rate(Kbps)	Rx	Rx Error	Rx Rate(Kbps)
Port1	On	Up	11700	0	0	35115	0	0
Port2	On	Down	0	0	0	0	0	0
Port3	On	Down	0	0	0	0	0	0
Port4	On	Down	0	0	0	0	0	0
PortG1	On	Down	0	0	0	0	0	0
PortG2	On	Down	0	0	0	0	0	0

Clear Refresh

Figure 2.38 Port Count in Port Statistics Webpage

2. Click function **06** on the toolbar as shown in Figure 2.39.

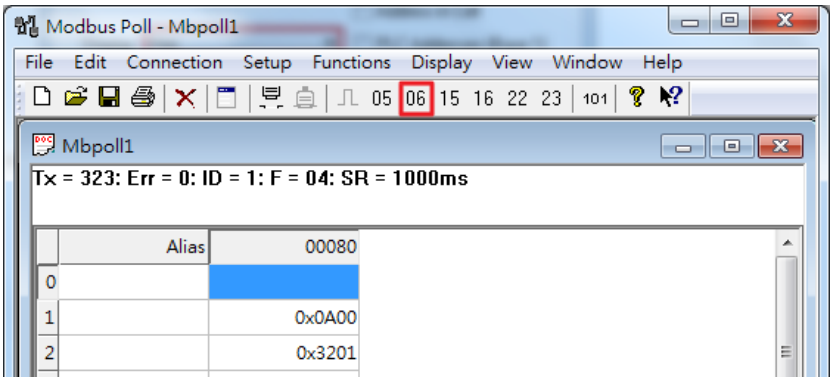


Figure 2.39 Click on Function 06 in the Modbus Poll

3. Set **Address** to 256 and **Value (HEX)**to 1 as shown in Figure 2.40, then click "**Send**" button.

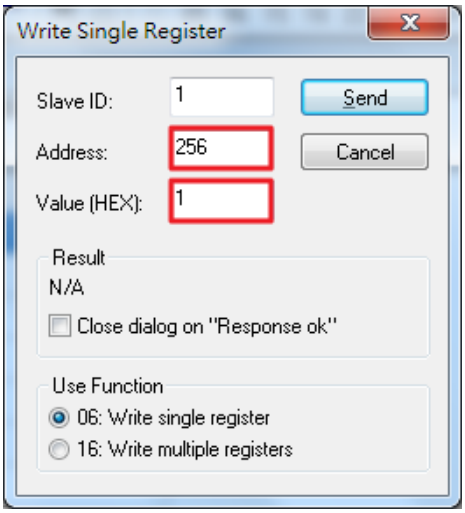


Figure 2.40 Use Modbus Poll to Clear Switch's Port Count

4. Check **Port Statistics** (described in Section2.6.4) in the managed switch's Web UI as shown in Figure 2.41. The packet count is now cleared.

Port Statistics

Port	Enable	Link	Tx	Tx Error	Tx Rate(Kbps)	Rx	Rx Error	Rx Rate(Kbps)
Port1	On	Up	8	0	0	27	0	0
Port2	On	Down	0	0	0	0	0	0
Port3	On	Down	0	0	0	0	0	0
Port4	On	Down	0	0	0	0	0	0
PortG1	On	Down	0	0	0	0	0	0
PortG2	On	Down	0	0	0	0	0	0

Clear Refresh

Figure 2.41 Cleared Port Statistics

2.3.9 Precision Time Protocol (PTP)

The Precision Time Protocol(PTP) is a high-precision time protocol. It can be usedwithmeasurement and control systems in local area network that require precise time synchronization. This menu is divided into two submenus:**PTP Setting** and **Output Module** as shown in Figure 2.42.

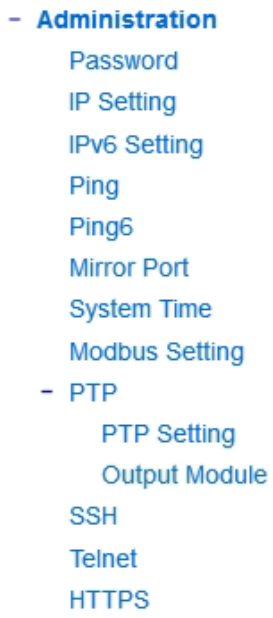


Figure 2.42 PTP's Submenu

2.3.9.1 PTP Setting

The PTP can be set in this PTP Setting webpage. Figure 2.43shows the PTP Configuration webpage in which the user can configure PTP and check its status. The lower part of Figure 2.43allows the users to enable or disable the PTP function per port and check their current status.

To enable PTP on the managed switch, please check the **Enabled** box behind the**State** option as shown in Figure 2.43.Note that the PTP will not be enabled per port if this State option is not checked. Please see description of PTP configuration inTable 2.9 and description of PTP port information inTable 2.10. Note that after setting the desired PTP options, please click **Update** button to allow the new configurationto take effect.

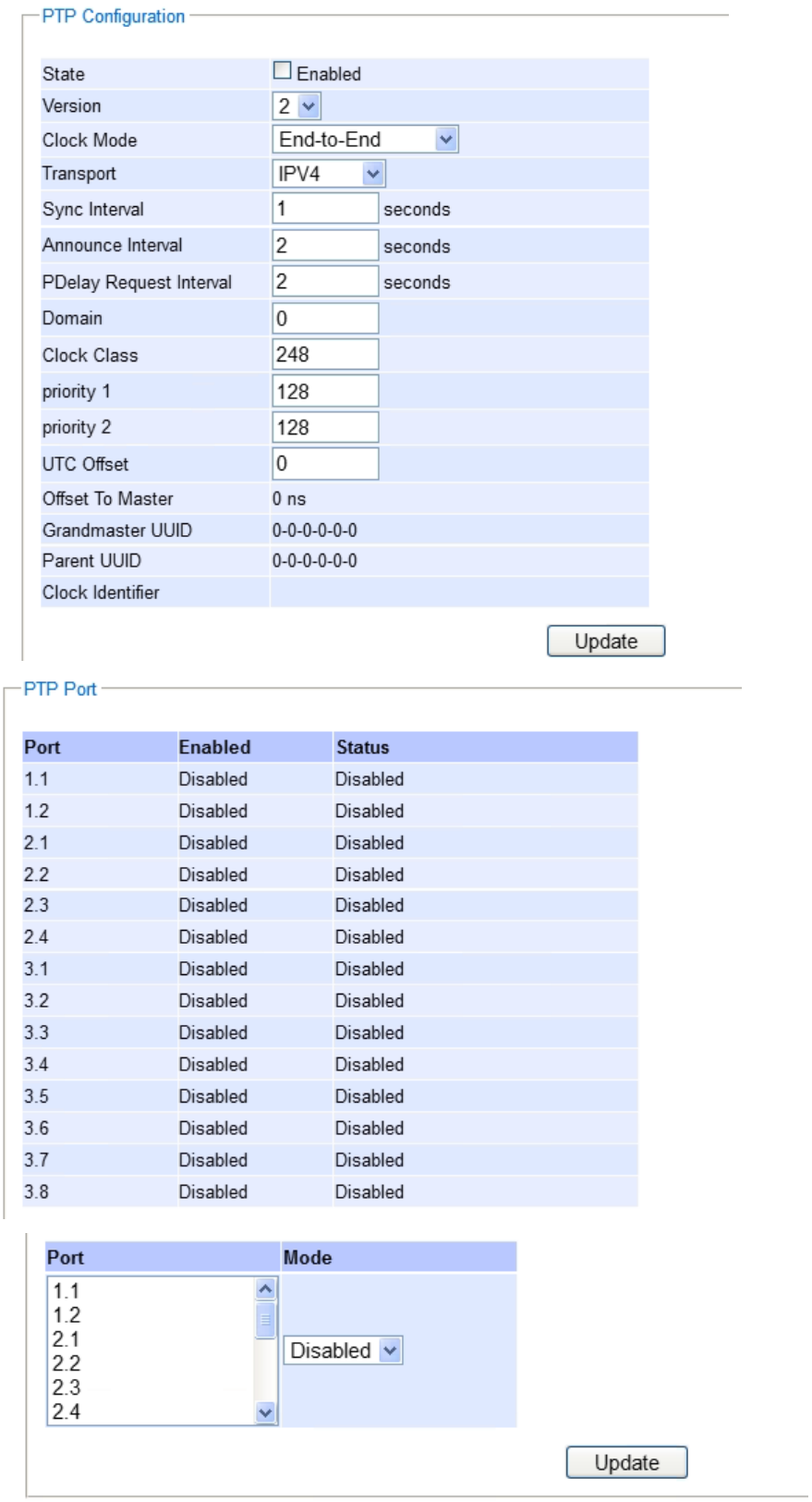


Figure 2.43 PTP Setting Webpage, example taken from RHG96XX series

Table 2.9Description of PTP Setting

Label	Description	Factory Default
State	Enabled/Disable the PTP function. This is the main optionthat needs to be enabled so that the port's PTP function will work according to other parameters defined in this table (Table 2.9).	Unchecked
Version	Set the PTP operation version. Note that only v2 (IEEE 1588-2008) are supported in RHG95xx and RHG9628 SB model.	2
Clock Mode	Select clock type of the PTP (Precision Time Protocol). The switch has four modes: End-End Boundary Clock, End-End Transparent Clock (TC), Peer-Peer Boundary Clock, and Peer-Peer Transparent Clock (TC).	End-to-End
Transport	Select Ethernet (layer 2) multicast transport or layer 3 (UDP/IPv4)multicast transports for PTP (Precision Time Protocol) messages.	IPV4
Sync Interval	Set the interval of the sync packet transmitted time. Small interval causes too frequent sync, which will cause more load to the device and network.	1
Announce Interval	Set the interval time of the packet announcement. The smaller the interval, the frequent the announce, which will cause more load to the device and network.	2
Pdelay Request Interval	Set the interval time of the PDelay request packet. The smaller the interval, the frequent the sync packet, which will cause more load to the device and network. Note this is only supported in RHG95xx and RHG9628.	2
Domain	Set the domain number field in 1588 packet	0
Clock Class	Clock Class represents clock's accuracy level. It is an attribute of an ordinary or boundary clock. It denotes time traceability or frequency distributed by the grandmaster clock. Please refer to IEEE 1588-2008, Table 5 for definitions, allowed values, and interpretation.	248
priority 1	Set the clock priority 1 (PTP version 2). The lower values take precedence to be selected as the master clock in the best master clock algorithm, 0 = highest priority, 255 = lowest priority.	128
priority 2	Set the clock priority 2 (PTP version 2). The lower values take precedence to be selected as the master clock in the best master clock algorithm (BMCA), 0 = highest priority, 255 = lowest priority.	128
UTC Offset	Coordinated Universal Time (UTC) offset value	0
Offset to Master	The offset time to the master clock	None
Grandmaster Identity	The Grandmaster UUID for PTP version 2	None
Parent Identity	The parent master UUID for PTP version 2	None
Clock Identifier	The clock identifier for PTP version 1	None

Table 2.10Description of PTP Port Setting

Label	Description	Factory Default
Port	Port number	-
Enabled	This is the port's mode information which indicates whether theport's PTP function is enabled or disabled.	Disabled
Status	This is PTP'sper port operation status. If the per port function is enabled, but the status is still disabled, please enable the PTP master option (State option in Table 2.9).	Disabled
Mode	Enabled/Disabled PTP per port function	Disabled

2.3.9.2 Output Module

RHG9628 can be equipped with optional output modules. These output modules support multiple legacy standards, such as IRIG-B, BCD, BJT, ST, and ST with checksumwhich can be enabled and selecting the desired format as shown inFigure 2.44.

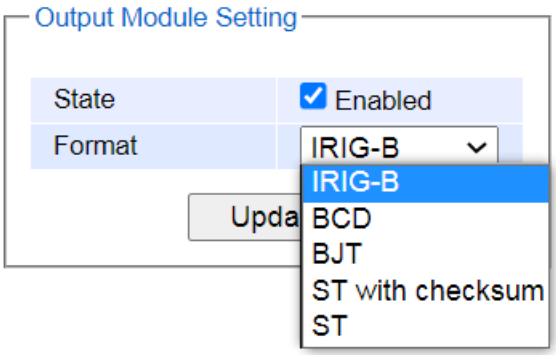


Figure 2.44Output Module Setting

Table 2.11Description of Output Module

Format	Details
IRIG time code B (IRIG-B)	The IRIG time codes were originally developed by the Inter-Range Instrumentation Group (IRIG), part of the Range Commanders Council (RCC) of the US Army. It has a pulse rate of 100 pulses-per-second with an index count of 10 milliseconds over its one-second time frame. The complete IRIG time code designation consists of a letter and three digits (Format (A, B, D, E, G or H), Modulation, Carrier Frequency / Resolution, Coded Expressions)
BCD	BCD Time of year and year code word consists of subwords in days, hours, minutes, seconds, and year with fractions of a second in a BCD representation
BJT	The official national standard time is called Beijing Time
ST with checksum	Newfoundland Standard Time (NST) is 3:30 hours behind Coordinated Universal Time (UTC). This time zone is in use during standard time in: North America. Newfoundland Standard Time is a half-hour time zone. Its local time differs by 30 minutes instead of the normal whole hour.
ST	Standard time

2.3.10 Secure Shell - SSH

The managed switch can be managed using command line interface (CLI) as described in Chapter4. The users have option to remotely connect to the managed switch using either secure shell (SSH) or Telnet through any of its port. In this subsection, SSH will be introduced and then Telnet will be discussed in the next subsection. SSH was designed to replace Telnet and other insecure remote shell protocols that sends data or command in plaintext. SSH uses encryption to secure its dataor command over an unsecure network.

To enable the SSH, please check the **Enabled** box behind the **SSH** option in Figure 2.45. At the beginning, the Server will send a public key to a Client, and the Client will check if the received public key is correct. If itis not correct, theServer will refuse the connection. Please click "**Generate**" button to change and regenerate the Server Key then obtain another public key from Server as shown in Figure 2.45.

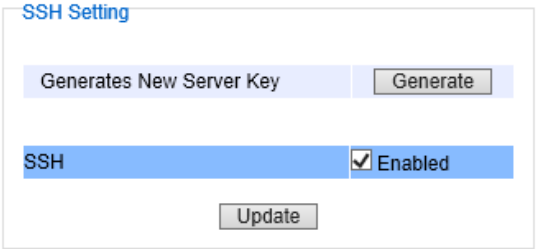


Figure 2.45 SSH Setting Webpage

Note:

1. The managed switch supports both SSH version 1 (SSH1) and SSH version 2 (SSH2).
2. The server key is re-generated when the managed switch is reset to its factory default setting or a received key is non-existent.

SSH version 1 and SSH version 2 share the following features:

1. Client programs that use SSH canperform remote logins, remote command execution, and secure file copying across a network.
2. Several selectable encryption algorithms and authentication mechanisms are supported by the SSH.
3. An SSH agent can cache keys for easy access in later session.

A number of new features are added to SSH version 2 for a stronger and more comprehensive product. These features include:

1. Encryption ciphers, i.e. Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES).
2. The use of sound cryptographic Message Authentication Code (MAC) algorithms for integrity checking.Examples of secure hash (functions) algorithms which are MAC algorithmsin SSH version 2 are the Message Digest algorithm5 (MD5) andSecure Hash Algorithm 1 (SHA-1).
3. Support for public key certificates.

2.3.11 Telnet

This subsection allows the users to set the Telnet optionfor the managed switch. The command line interface (CLI)configuration using Telnet (as described in Chapter 4) or SSH (previous section) are the same except that the SSH encrypts the communication data. For the Telnet administration, the managed switch only provides the enable or disable function selectable in this webpage. The default setting for Telnet is enabled. Clicking on the **Update** button when you change the option to update it on the managed switch. Figure 2.46shows the Telnet setting webpage. Note that the users are recommended to use SSH instead of Telnet for higher security protection of your managed switch.

Figure 2.46 Telnet Setting Webpage

2.3.12 HTTPS

This subsection enables the users to set the HTTPS (HyperText Transfer Protocol Secure) for the web-based management user interface of the switch as shown inFigure 2.47. This option will encryptthe normal HTTP message between the switch and the client PC to secure their communication over the network. To access the web GUI when this option is enabled, the users mustaccess the switch via https://10.0.50.1 for enchanced security during device configuration. Note that once this option is enabled, every HTTP request for web console of the managed switch will be forced to redirect to https connection.Clicking on the **Update** button when you change the option to update it on the managed switch.

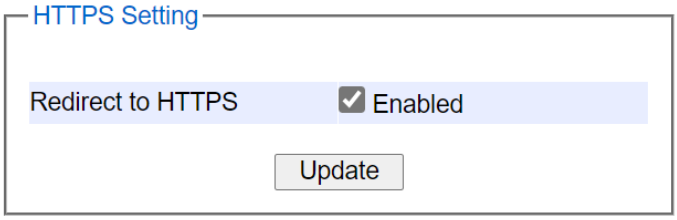


Figure 2.47 HTTPS Setting Webpage

2.3.13 sFlow

sFlow, short for "sampled flow", is an industry standard for packet export at Layer 2 of the OSI model for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.
The UDP payload contains the sFlow datagram. Each datagram provides information about the sFlow version, the originating device's IP address, a sequence number, the number of samples it contains and one or more flow and/or counter samples.

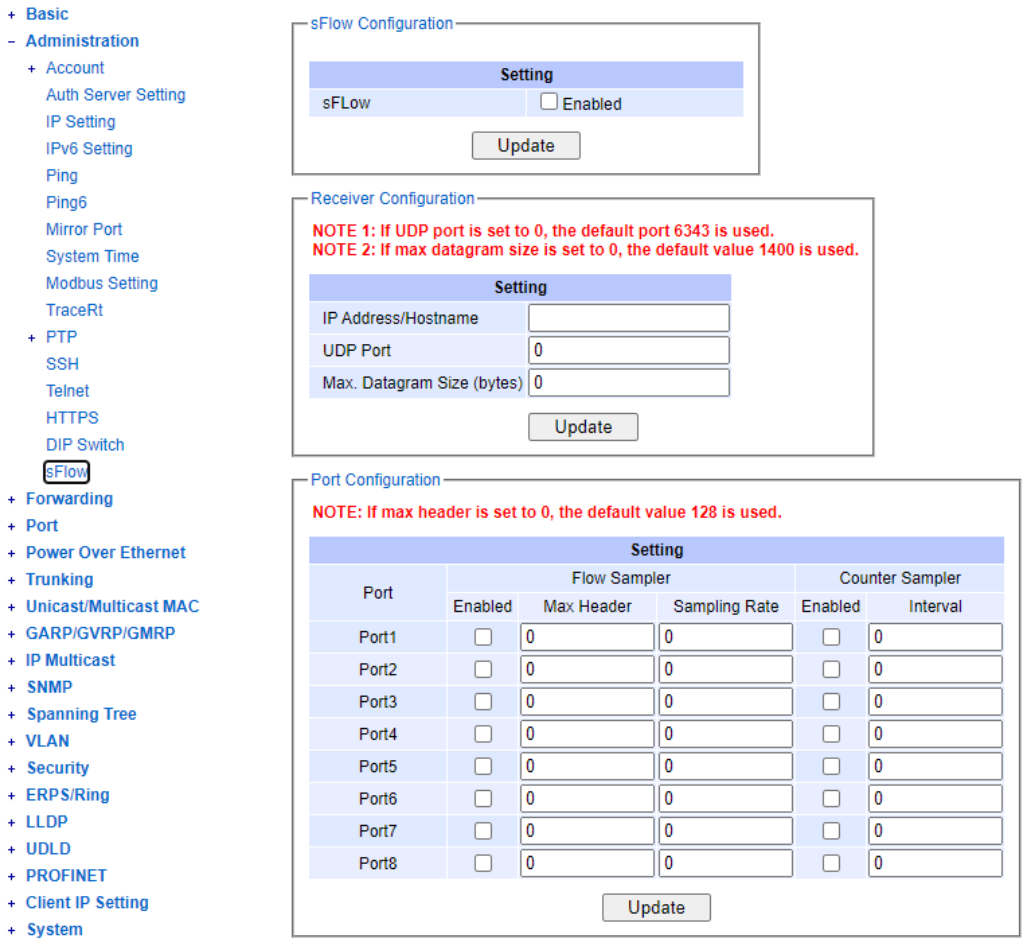


Figure 2.48 sFlow setting Webpage

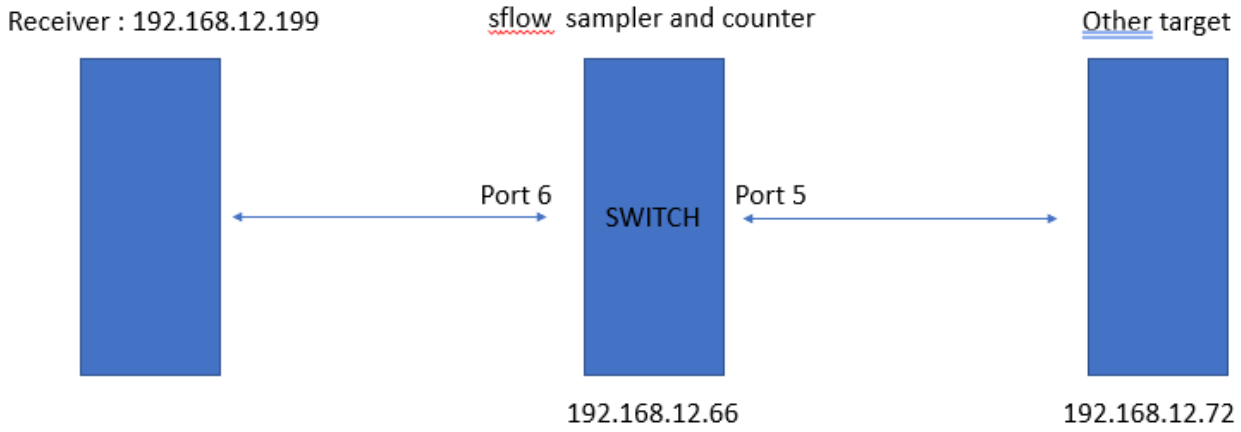


Figure 2.49 sFlow working sample

Table 2.12 Descriptions of sFlow Setting

Label		Description	Factory Default
sFlow Configuration			
Enabled		Check the box to enable/disable sFlow feature	Uncheck
Receiver Configuration			
IP Address/Hostname		The IP address of sFlow receiver	Null
UDP Port		The UDP port number of sFlow receiver	0
Max. Datagram Size (bytes)		The maximum number of data bytes that can be sent in a single sample datagram	0
Port Configuration			
Flow Sampler	**Enabled**	Check the box to enable/disable the status of flow sampling on specific port(s).	Uncheck
	Max Header	The maximum number of bytes that should be copied from a sampled packet to the sFlow datagram	0
	Sampling Rate	Set to N to sample on average 1/Nth of the packets transmitted/received on the port	0
Counter Sampler	**Enabled**	Check the box to enable/disable the status of counter polling on specific port(s).	Uncheck
	Interval	With counter polling enabled, this specifies the interval - in seconds	0

2.4 Forwarding

There are many network technologies for forwarding packets over network. In this industrial managed switch, three main technologies are implemented: QoS, rate control, and storm control. Figure 2.50 depicts the submenus under the Forwarding section.

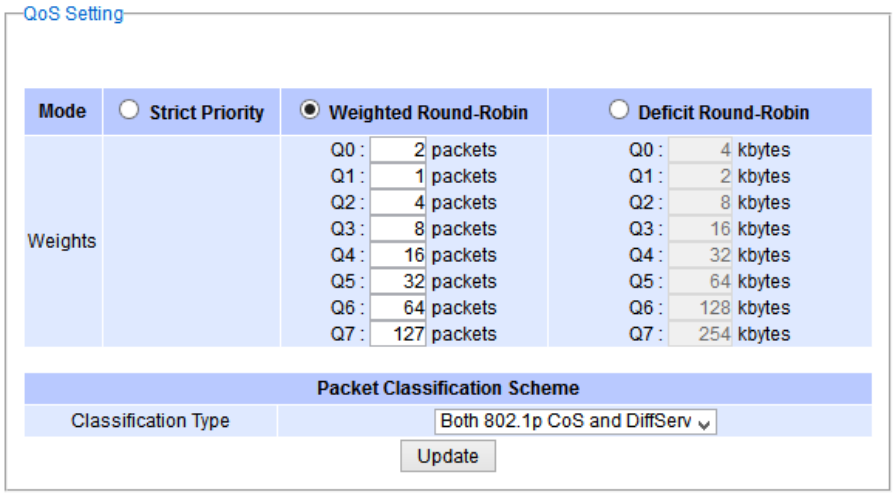


Figure 2.50 Forwarding Dropdown Menu

2.4.1 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 bitrate, bit error rate, delay, jitter, and probability of packet dropping. QoS guarantees are important if the network capacityis 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.

In the QoS section, three QoS mechanisms are included: queuing methodsor packet scheduling disciplines in **Setting** section, **CoS Queuing Mapping**section, and **DSCP Mapping** section, as shown inFigure 2.51. Table 2.13 summarizes the descriptions of QoS Setting.

Figure 2.51 QoS Dropdown Menu

Table 2.13 Descriptions of QoS Setting

Label	Description	Factory Default
Setting	Queuing Methods (packet scheduling disciplines) includes**Strict Priority, Weighted Round-Robin,** and **Deficit Round Robin** See notes in the following subsection for detailed descriptions and comparison.	Weighted Round-Robin
Header Mapping	**CoS Queuing Mapping** and **DSCP Mapping**	802.1p CoS only

	For 802.1p CoS only, switch only checks Layer 2 (L2) 802.1p CoS priority bits. **For DiffServ**, switch checks DiffServ Code Point (DSCP). See notes below for a detailed description.	

2.4.1.1 QoS Setting

Three types of queuing methods are configurable in this managed switch:Strict Priority, Weighted Round-Robin, and Deficit Round-Robin.

In **Strict Priority**,the QoS scheduler allows the highest priority queue to preempt other queues as long as there are still packets waiting to be transmitted in the highest priority queue.This mode guarantees that traffic in the highest queue is always transmitted first.Only if the high priority queues are empty, the lower priority queues can be transmitted.Queue 0 (Q0)to Queue 7 (Q7)are ranked from the lowest priority queue to the highest priority queue. Therefore, packets in Q7 will be all transmitted first before packets in Q6, and packets in Q6 will all be sent first before packets in Q5, and so on in this order.

Weighted Round Robin (WRR) is the simplest approximation of generalized processor sharing (GPS). In WRR, each packet flow or connection has its own packet queue in a network interface controller. It ensures that all service classes have access to at least some configured amount of network bandwidth to avoid bandwidth starvation.But WRR has a limitation, as it is unfair with variable length packets. It only provides the correct percentage of bandwidth to each service class only if all of the packets in all the queues are the same size or when the mean packet size is known in advance. Usually, a weight of each queue is set proportion to requested bit rate. Each queue is served proportionally to its weight for a service cycle.

Deficit WRR (DWRR)addressed the limitation of WRR on unfairness over variable size. Each queue is configured with a weight, a deficit counter (total number of bytes that the queue is permitted to transmit each time visited by the scheduler), and a quantum of service (bytes). DWRR scans all non-empty queues in sequence. When a non-empty queue is selected, its deficit counter is incremented by its quantum value. Then, the value of the deficit counter is the maximal number of bytes that can be sent at this turn. If the deficit counter is greater than the packet's size at the head of the queue, this packet can be sent and the value of the counter is decremented by the packet size. Then the size of the next packets is compared to the counter value. Once the queue is empty or the value of the counter is insufficient, the scheduler will skip to the next queue. If the queue is empty, the value of the deficit counter is reset to 0. If the packet size is too small, the scheduler has to visit queues too many times before serving a queue. But if the packet size is too large, some short-term unfairness may arise**.** It is fair only over a time scale longer than a round time. At the shorter time scale, some flows may get more service. Small packet size or high transmission speed reduce the round time. Figure 2.52depicts the QoS Setting webpage. By default, the QoS in the managed switch works under the Strict Priority mode. For Weighted Round Robin, packet weights of Q0 to Q7 are set in term of packet as followings.

- COS Q0 = 2 packets
- COS Q1 = 1 packet
- COS Q2 = 4 packets
- COS Q3 = 8 packets
- COS Q4 = 16 packets
- COS Q5 = 32 packets
- COS Q6 = 64 packets
- COS Q7 = 127 packets

Weight of Deficit Round Robin is double the number of packets of WRR, but it is in term of Kbytes instead as shown in the last column of Figure 2.52.

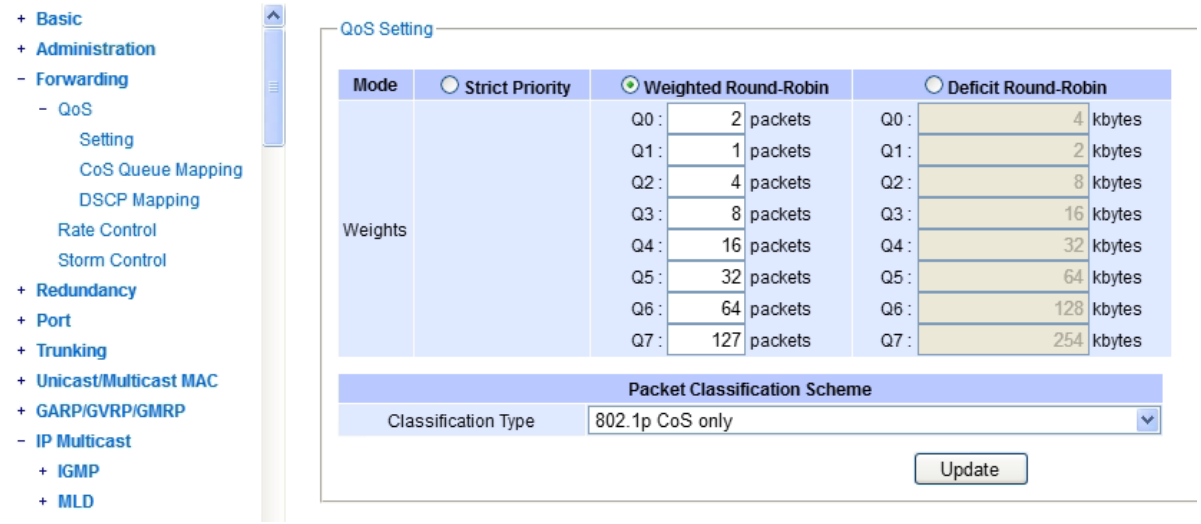


Figure 2.52 QoS Setting Webpage

At the bottom of the QoS Setting webpage in Figure 2.52, the users can select the packet classification scheme that will be used by the managed switch. There are two classification types to choose from the drop-down list: **802.1p CoS only** or **Both 802.1p CoS and DiffServ**. The default classification type is **802.1p CoS only**. Note that after changing the schedule discipline, setting the desired weights if any for the WRR or DWRR, or selecting the classification type, please click on the **Update** button to enable them on the switch.

2.4.1.2 CoS Queue Mapping

802.1p CoS is the QoS technique developed by the IEEE P802.1pworking group, known as Class of Service (CoS) mechanism at Media Access Control (MAC) level. It is a 3-bit field called the priority code point (PCP) within an Ethernet frame header (Layer 2) when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value between 0 and 7 that can be used by QoS to differentiate traffic. When this option is enabled, the switch inspects the 802.1p CoS tag in the MAC frame to determine the priority of each frame.

The switch can classify traffic based on a valid 802.1p (CoS- Class of Service) priority tag. These options allow users to map Priority Code Point (PCP) within an Ethernet frame header to different CoS priority queues as shown inFigure 2.53. The user can choose the desired CoS Priority Queue from the drop-down list from Q1 to Q7 for each PCP value.Descriptions of priority queue in CoS Queue Mapping page are summarized in Table 2.14.

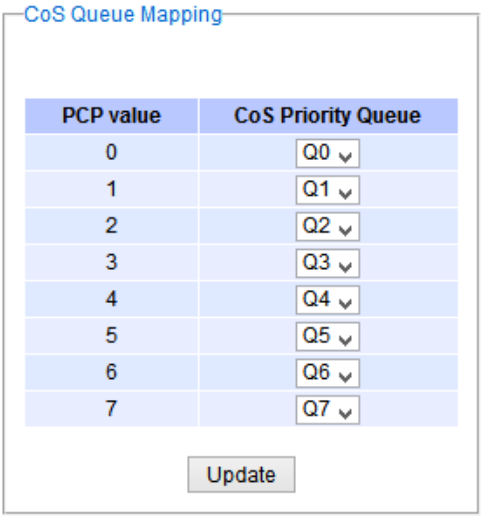


Figure 2.53Mapping Table of CoS Webpage

Table 2.14Priority queue descriptions

Label	Description	Factory Default
PCP	Priority Code Point within the Ethernet frame header. PCP 0 is the lowest priority and 7 is the highest priority.	PCP 0 ->Q0 PCP 1 ->Q0 PCP 2 ->Q1 PCP 3 ->Q1 PCP 4 ->Q2 PCP 5 ->Q2 PCP 6 ->Q3 PCP 7 ->Q3
CoS Priority Queue	The priority queue that a specific Ethernet frame needs to be assigned into.	

2.4.1.3 DSCP Mapping

DiffServ/ToS stands for Differentiated Services/Type of Services. Itis a networking architecture that specifies a simple but scalable mechanism for classifying network traffic and providing QoS guarantees on networks. DiffServ uses a 6-bit Differentiated Service Code Point (DSCP) in the 8-bit differentiated services field (DS field) in the IP header for packet classification purposes. The DS field and ECN field replace the outdated IPv4 TOS field in IPv4 to make per-hop behavior decisions about packet classification and traffic conditioning functions, such as metering, marking, shaping, and policing.

The RFCs (Request for Comments) do not dictate the way to implement Per-Hop Behaviors (PHBs). Atop implements queuing techniques that can base their PHB on the IP precedence or DSCP value in the IP header of a packet. Based on DSCP or IP precedence, traffic can be put into a particular service class. Packets within a service class are treated the same way.

DiffServ allows compatibility with legacy routers, which only supports IP Precedence, since it uses the DiffServ Code Point (DSCP), which is the combination of IP precedence and Type of Service fields. Note that you need to select the "**Classification Type**" pull-down list under the **Packet Classification Scheme** to be "**Both 802.1p CoS and Diffserv**" in Section 2.4.1.1 first to enable DSCP Mapping.

TOS (Type of Service) of the switch can be configured with the default queue weights as shown in Figure 2.54. Note that the TOS consists of DSCP (Differentiated Service Code Point (6 bits)) and ECN (Explicit Congestion Notification (2 bits)).The users can assign TOS values (**DSCP**) to predefined queue types (**Priority**)manually using DSCP Mappingweb page in Figure 2.54. The priority number can be between 0 to 7 where the number 7 is the highest priority and 0 is the lowest priority. After assigning any new priority to a DSCP, please click the **Update** button at the bottom of the page to allow the new mapping to take effect.

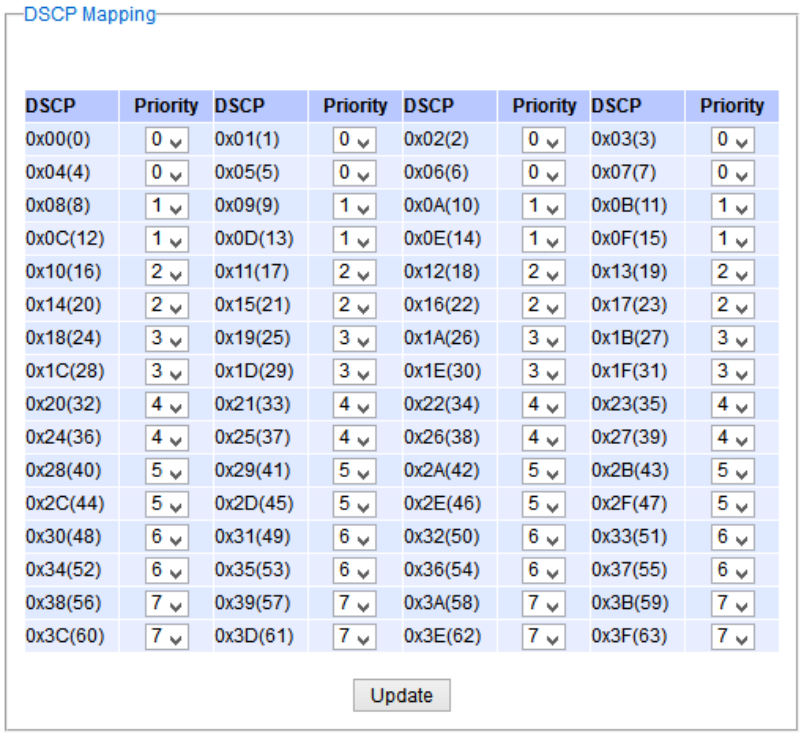


Figure 2.54 Mapping Table of DSCP and ECN Webpage

2.4.2 Rate Control

The users have options to set the Rate Control for each porton the managed switchas shown in Figure 2.55. The rate control mechanism will set a limit or maximum data rate which the port can transmit. Moreover, the rate control can be imposed on both directions: the incoming traffic (**Ingress**) and the outgoing traffic (**Egress**). However, there are some restrictions on the values that can be set on these two rate control parameters. Here is the summary of the rules for Rate Control settings:

- The outgoing (Egress) and incoming (Ingress) values have to be set between 0 and 102,400 (for 100 Mbps) or 1,024,000 (for 1000 Mbps).
- The value 0 is set to turn off the rate control mechanism.
- The values have to be integer andmultiple of 64 when the transmission rate is less than 1,792 Kbps. For example: 64 Kbps, 128 Kbps, 512 Kbps, and 1,792 Kbps.
- The values have to be integerand multiple of 1,024 when the transmissionrate is between 1,792 Kbps and 102,400 Kbps (for 100Mbps) or 106,496 Kbps (for 1000M). Ex: 2,048Kbps, 3,072 Kbps… 102,400Kbps.
- The values have to be integer and multiple of 8,192 when the transmission rate is greater than 106,496 Kbps.

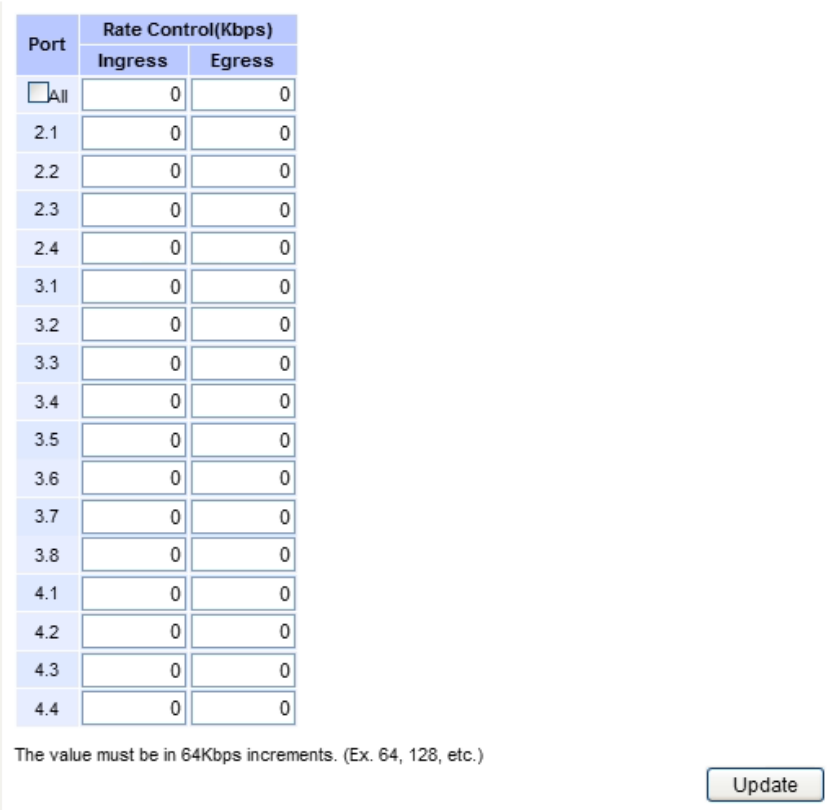


Figure 2.55 Rate Control Webpage

Table 2.15 provides descriptions of rate control setting. Note that after configuring the rate control in each port, please click on the **Update** button to enable it on the switch.

Table 2.15 Descriptions of Rate Control Setting

Label		Description	Factory Default
Port		Port number on the managed switch.	-
Rate Control (Kbps)	**Ingress**	Sets limits on its transmission rates for the incoming (Ingress) traffic. Note that the unit is inkilo-bits per second (Kbps).	0 (Disabled)
	Egress	Sets limits on its transmission rates for the outgoing (Egress) traffic. Note that the unit is inkilo-bits per second (Kbps).	0(Disabled)

2.4.3 Storm Control

This subsectionprovides the storm control or storm filter features of the managed switch. Storm control prevents traffic on a LAN from being disrupted byingress traffic of broadcast, multicast, and destination lookup failure (DLF) on a port. Figure 2.56 depicts the Strom Control webpage. The users can impose thesame limiting parameters on all ports at the same time by clicking on the box in front of the **all**line and set the storm control data rate under each limiting column (DLF, Multicast, Broadcast). The storm control limiting can also be independently control on each port.Note that the limiting value of 0 means that the storm control is disable and the value must be in multiples of 64kbps. Additional ingress storm traffic will be dropped after the limit has reached.

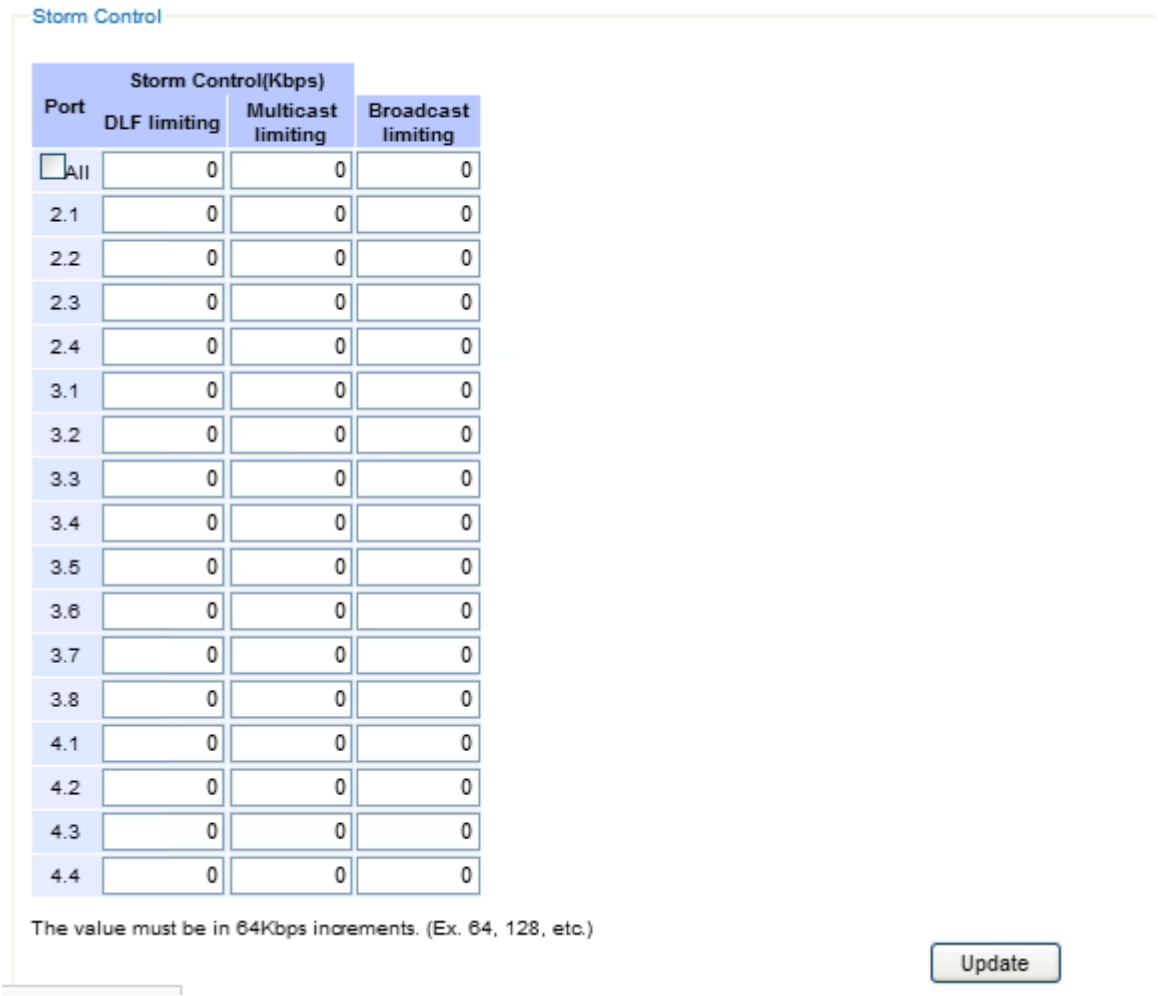


Figure 2.56 Storm Control Webpage

Table 2.16 summarizes the descriptions of storm control.

Table 2.17 summarizes the descriptions of limitingparameters for storm control.

Table 2.16 Descriptions of Storm Control

Label	Description	Factory Default
All	Enable or Disable the storm control or filter on all ports at the same time. The limiting data rate for each type of storm packets (**DLF**, **Multicast**, and **Broadcast**) can be controlled by changing the number under each column.Note that the value must be in multiples of 64kbps.	Uncheck and Disable
Port	Set the limiting data rate of storm packets that can be controlled for each Port, which are **DLF**, **Multicast**, and **Broadcast**. Note that the value must be in multiples of 64kbps. See notes below for the detailed description and comparison.	Disable

Table 2.17 Descriptions of Limiting Parameters

Label	Description	Factory Default
DLF limiting (Destination Lookup Failure)	DLF limiting (0~9876480) Kb	0 (Disable)
Multicast limiting	Multicast limiting (0~9876480) Kb	0 (Disable)
Broadcast limiting	Broadcast limiting (0~9876480) Kb	0 (Disable)

Type of Storm Packets:

- **DLF**: **D**estination **L**ookup **F**ailure. The switch will always look for a destination MAC addressin its MAC Table first. In case that a MAC address cannot be found in the MAC Table, which means DLF occurs, the switch will forward the packets to all ports that are in the same LAN.
- **Multicast**: This type of transmission sends messages from one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive it. Network devices that support multicast send only one copy of the information across the network until the delivery path that reaches group members diverges. At these diverging points, multicast packets will be copied and forwarded. This method helps reducinghigh traffic volumesdue tolarge number of destinations, using network bandwidth efficiently.
- **Broadcast**: Messages are sent to all devices in the network.

2.5 Redundancy

Atop's industrial managed switch provides fullcontrol on redundancy. In this section, the users can select redundancy protocol for each port: either PRP (Parallel Redundancy Protocol) or HSR (High availability Seamless Redundancy).All Redundancy's settingfor each port can be viewed in this section.Figure 2.57illustrates the Redundancy Setting webpage. The Redundancy section is subdivided into one subsection which is: **Setting.**

2.5.1 Setting

Both High-availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) arethe methods of network recovery which provide "zero recovery time" without any packet loss. PRP and HSR are standardized by the IEC 62439-3:2016.Both methods are suitable for applications that require high availability and low switch-over time, such as the protection ofan electrical substation, or the protection of high-power inverters.

HSR-PRP module is developed to be a part of **RHG9628** switch. The FPGA device licensed fromFlexibilis is used to organize the module. The basic operation of these protocols is that the Ethernet packets are transferred from switch to the FPGA.Then, the FPGA converts these packets into HSR or PRP format before forwarding the packets to two of its redundant ports.

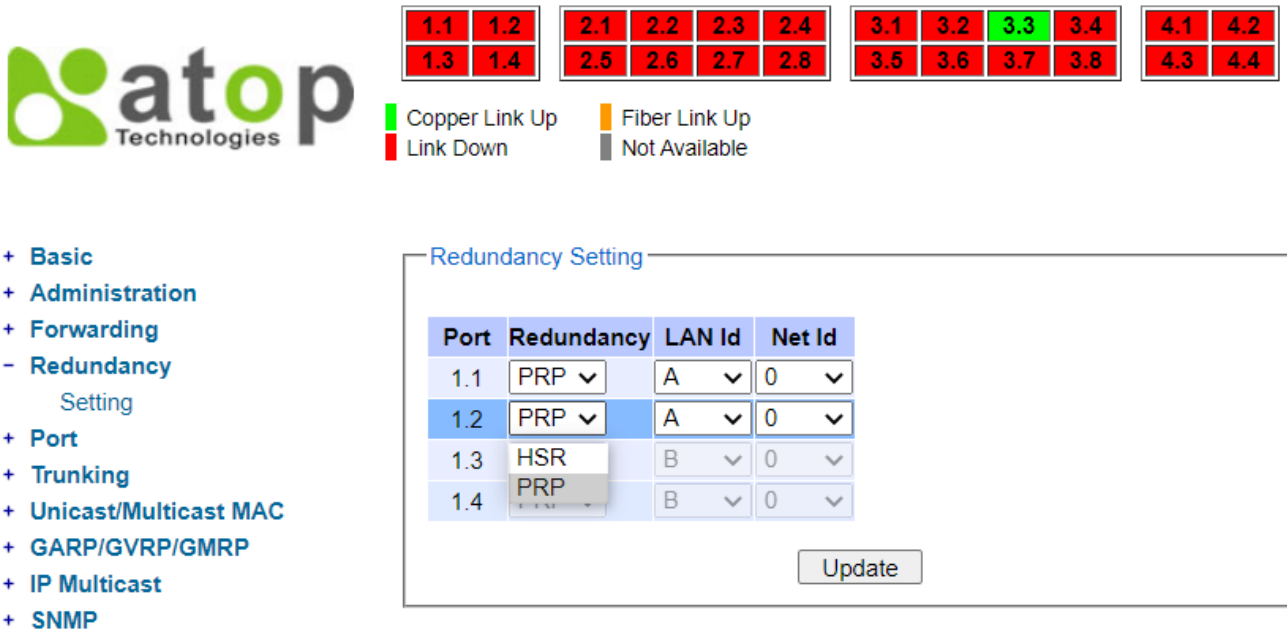


Figure 2.57Setting Webpage under Redundancy Section

Figure 2.57shows the dropdown menu for HSR/PRP section on the RHG9628 managed switch. User could modify the redundancy type of each port by selecting either HSR or PRP type and chosing the configured LAN IDand Net ID before clicking the update button.

2.6 Port-related settings

Atop's industrial managed switch provides fullcontrol on all of its network interfaces. In this section, the users can enable or disable each port and set preferredphysical layer mode such as copper or fiber. Moreover, the users will be able to configurenegotiation mechanism, data rate (speed), duplexing, and flow controlforeach port. All port's status and statistics can be viewed in this section. Figure 2.58illustrates the Port webpage. The Port section is subdivided into four subsections which are:

- PortSetting
- Port Status
- Mini-GBIC Port Status
- Port Statistics

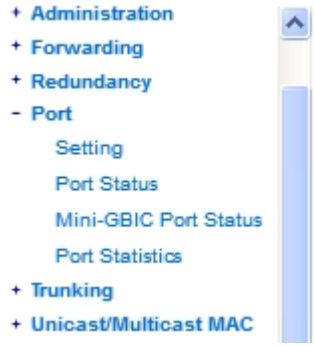


Figure 2.58 Port Dropdown Menu

2.6.1 Port Setting

Port Settingwebpage is shown inFigure 2.59. The userscan control the state of each port by checking on the corresponding**Enable** box. The possible physical layer connections of each port are listed on the **Mode** column. In some of Atop's managed switches (EH76xx Series), the users can then select one of the physical media to be a preferred mode of operation. For instance, a gigabit Ethernet port (PortG1) can support either copper or fiber physical layer connections. The users can click on the radio button behind the Fiber option to set the fiber optical mode as its preferred physical medium connection. Note that when both modes are selected, this means that the port is a combo port. However, the example inFigure 2.59 is based on RHG9628-410GSFP-BC-DCwhich does not have a combo port and cannot select preferred mode of operation.

Figure 2.59 Port Setting Webpage

Next on the fourth column ofFigure 2.59, for *Copper* option port 1.1-1.4, user can select only **Auto** from the dropdown list in the **Negotiation** mechanism. Port's speed is unchangeable and it is set at **1000** Mbps, **full** duplex, and Flow control is set to **off**. The setting is more flexible for the user when it is the *other Copper port* and *Fiber* option.Here, the users can select from the dropdown list the port's**Negotiation** mechanism which can be either **Auto** or **Force**. When selecting the **Force** negotiation, the port's speed and duplexing will be locked to the settings configured by the users. On the other hand, the **Auto** negotiation will allow the switch to determine the actual speed and duplexing for that port. Note that the Gigabit Small Form-factor Pluggable (SFP) Port of the EH Series switch is downward compatible with 125/155Mbps Transceivers; however, the speed needs to be set to 100 manually.The Gigabit SFP Port of the RHG Series is not downward compatible.

On the fifth column, the transmission **Speed** of each port can be chosen from the dropdown list which could be **10**, **100**, or **1000** Mbps. The default speed is set to the highest possible rate in Mbps. Next the port's duplexing (**Duplex**)can be either **Full** duplex or **Half**duplex. The **Half duplex** option allows one-way communication at a time, while the **Full duplex** option allows simultaneous two-way communication.

Each port can set the **Flow Control** mechanism to either **On** or **Off** on the eighth column. This flow control will be useful to avoid packet loss when there is a network congestion. However, the **Flow Control** setting is **Off** by default.After configuring the port setting, please click on the **Update** button to enable any of your new configuration on the switch. Descriptions of port setting options are summarized inTable 2.18.

Table 2.18Descriptions of Port Settings

Label	Description	Factory Default
Port	Port number on the managed switch.	-
Enable	Check the box to allow data to be transmitted and received through this port	All ports are enabled
Mode	Copperand/or Fiber modes. When both Copper and Fiber are listed, it means that this is a Combo port	Depend
Negotiation	Choose from either**Force** or **Auto**. See description in the paragraphabove.	Auto-negotiation is enabled to all ports.
Speed	Select either **10**, **100**,or**1000Mbps**	Highest Speed
Duplex	Select either **Half** or **Full** Duplex. See description in the paragraph above.	Full-Duplex
Flow Control	Either **on** or **off**. TheFlow Controlmechanism can be enabled (On) to avoid packet loss when congestion occurs.	Off

2.6.2 Port Status

The overview of port status on the managed switch can be viewed in this webpage. The users can compare the actual status and the configured options described in previous subsection for each port. The rate control (ingress and egress) can be configured based on the instructions on Section 2.4.2. Figure 2.60 shows the Port Status webpage. Note that the last column also reports the security status whether it is turned on or off on each port, which can be either static security or 802.1x (See how to set security option for each port in Section2.17). To check the latest status of all port, click the **Refresh** button either on the top or the bottom of the webpage.

Port Status

Refresh

Port	Mode	Enabled	Link	Negotiation		Speed		Duplex		Flow Control		Rate Control		Security
				Config	Actual	Config	Actual	Config	Actual	Config	Actual	Ingress	Egress	
1.1*	C	Yes	Down	Auto	-	1000	-	Full	-	Off	Off	Off	Off	Off
1.2*	C	Yes	Down	Auto	-	1000	-	Full	-	Off	Off	Off	Off	Off
1.3*	C	Yes	Down	Auto	-	1000	-	Full	-	Off	Off	Off	Off	Off
1.4*	C	Yes	Down	Auto	-	1000	-	Full	-	Off	Off	Off	Off	Off
2.1	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
2.2	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
2.3	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
2.4	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
3.1	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
3.2	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
3.3	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
3.4	C	Yes	Up	Auto	Auto	1000	100	Full	Full	Off	Off	Off	Off	Off
3.5	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
3.6	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
3.7	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
3.8	C	Yes	Down	Auto	-	1000	-	Full	-	Off	-	Off	Off	Off
4.1	F	Yes	Down	Force	-	10000	-	Full	-	Off	-	Off	Off	Off
4.2	F	Yes	Down	Force	-	10000	-	Full	-	Off	-	Off	Off	Off
4.3	F	Yes	Down	Force	-	10000	-	Full	-	Off	-	Off	Off	Off
4.4	F	Yes	Down	Force	-	10000	-	Full	-	Off	-	Off	Off	Off

Refresh

Figure 2.60 Port Status Webpage

The header in each column and its possiblevalues of the ports's status are listed here:

- **Mode**(Copper (C) or Fiber (F))
- **Enable** (Yes or No)
- **Link** (Up or Down)
- **Negotiation** (Auto or Force)
- **Speed**(unit:Mbps)
- **Duplex** (Full or Half)
- **Flow Control** (On or Off)
- **Rate Control** (On or Off)
- **Security** (On or Off): Either static security or 802.1x port security is turned on or off.

2.6.3 Mini-GBIC Port Status

The Small Form-factor Pluggable (SFP) port is sometimes referred to as a Mini-GBIC (**G**iga **B**itrate **I**nterface **C**onverter). In this subsection, all Mini-GBIC ports status can be shown if supported by the managed switch. Figure 2.61depicts the Module (or Mini-GBIC Port) Status webpage. Here, the status provides the Ethernet compliance codes, vendor name, vendor part number (PN), laser wavelength (L.W.), vendor serial number (SN), Connection Type, temperature T(C), voltage V, transmitted (Tx) power and received (Rx) power. The link status (up or down) can be viewed in the previous subsection.

Module Status

SFP Port	Com. Codes	Vendor Name	Vendor PN	L.W.	Vendor SN	Con. Type	T(C)	V	Tx Power (mW/dBm)	Rx Power (mW/dBm)
4.1	-	-	-	-	-	-	-	-	-	-
4.2	-	-	-	-	-	-	-	-	-	-
4.3	-	-	-	-	-	-	-	-	-	-
4.4	-	-	-	-	-	-	-	-	-	-

Note: Com. Codes:Gigabit Ethernet Compliance Codes. Vendor PN:Vendor Part Number. L.W.:Laser wavelength. Vendor SN:Vendor Serial Number. Con. Type:Connector Type. T(C): Temperature (C). V:Voltage (V).

Figure 2.61 Mini-GBIC Port Status Webpage

2.6.4 Port Statistics

The Port Statistics are summarized in this webpage as shown inFigure 2.62. The users can use this subsection to help them diagnose the problem such as link quality of each port. The key statistics are the total number of normal (**OK**) frames, the number of discarded (**Error**) frames, and the speed of the transmission (**Rate** in Bps) for both transmitted (**Tx**) and received (**Rx**) traffic in each port. To clear or reset all the statistics to zero on this page, click on the **Clear** button. To obtain the latest statistics on this page, click on the **Refresh** button.

Port Statistics

Clear Refresh

Port	Enabled	Link	Tx			Rx		
			OK (frames)	Error (frames)	Rate (Bps)	OK (frames)	Error (frames)	Rate (Bps)
1.1*	Yes	Down	0	0	0	0	0	0
1.2*	Yes	Down	0	0	0	0	0	0
1.3*	Yes	Down	0	0	0	0	0	0
1.4*	Yes	Down	0	0	0	0	0	0
2.1	Yes	Down	0	0	0	0	0	0
2.2	Yes	Down	0	0	0	0	0	0
2.3	Yes	Down	0	0	0	0	0	0
2.4	Yes	Down	0	0	0	0	0	0
3.1	Yes	Down	0	0	0	0	0	0
3.2	Yes	Down	0	0	0	0	0	0
3.3	Yes	Down	0	0	0	0	0	0
3.4	Yes	Down	0	0	0	0	0	0
3.5	Yes	Down	0	0	0	0	0	0
3.6	Yes	Up	67154	0	81	756620	0	8466
3.7	Yes	Down	0	0	0	0	0	0
3.8	Yes	Down	0	0	0	0	0	0
4.1	Yes	Down	0	0	0	0	0	0
4.2	Yes	Down	0	0	0	0	0	0
4.3	Yes	Down	0	0	0	0	0	0
4.4	Yes	Down	0	0	0	0	0	0

Clear Refresh

Figure 2.62 Port Statistics Webpage

The header in each column and its possible values of the ports'sstatistics are listed here:

- **Enable** (Yes or No): The port is enabled (Yes) or disabled (No).
- **Link** (Up or Down): Actual link status of the port.
- **TxOK** (**frames**): Total number of packets transmitted.

- **Tx Error(frames)**: The number of outbound packets which were chosen to be discarded even though no errors have been detected to prevent them from being transmitted.
- **Tx Rate(Bps)**: Speed of transmission in Bytes per second.
- **RxOK(frames)**: Total number of packets (not including faulty packets) received.
- **Rx Error(frames)**: Total number of faulty packets (includingOversize, Undersize, Frame Check Sequence (FCS), Alignment, Jabber and Fragment Errors in packets) received.
- **Rx Rate(Bps)**: Receiving speed in Bytes per second.

2.7 Trunking

The managed switch supports Link Trunking, which allows one or more links to be combined together as a group of links to forma singlelogical link with larger capacity.The advantage of this function is that it gives the users more flexibility while setting up network connections. The bandwidth of a logical link can be doubled or tripled. In addition, if one of links in the group is disconnected, the remaining trunked ports can share the traffic within the trunk group. This function creates redundancy for the links, which also impliesa higher reliability for network communication. Figure 2.63 shows the Trunking dropdown menu.

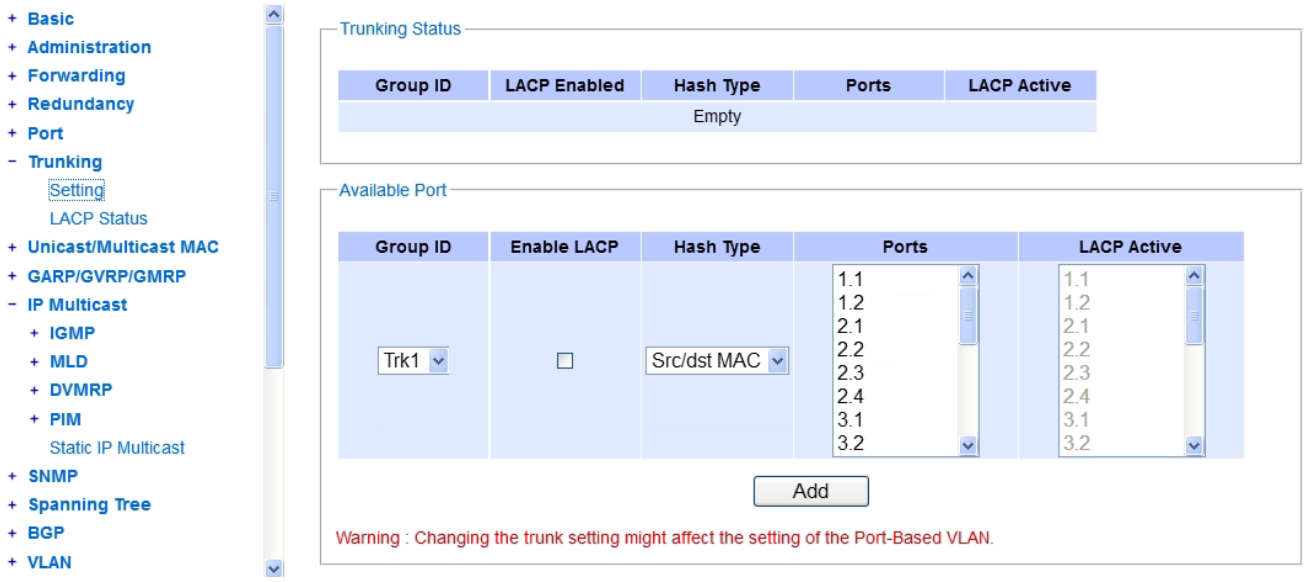


Figure 2.63Trunking Dropdown Menu

2.7.1 Trunking Setting

In this subsection, the user can create new trunking assignment(s) and remove existing trunking assignment(s).Figure 2.64illustrates the **Trunking Setting** webpage. The top part of the page called **Trunking**lists existing trunk(s) which can be removed by pressing the**Remove** button in the last column. Each line of the trunking provides information about the group of links (Trunk) based on **Group ID** labelled with **Trk*x*** where ***x*** is the integer

number between 1 to 4 (for RHG9628-410GSFP-BC-DC). The managed switch can support up to 4 trunk groups (for RHG9628-410GSFP-BC-DC).

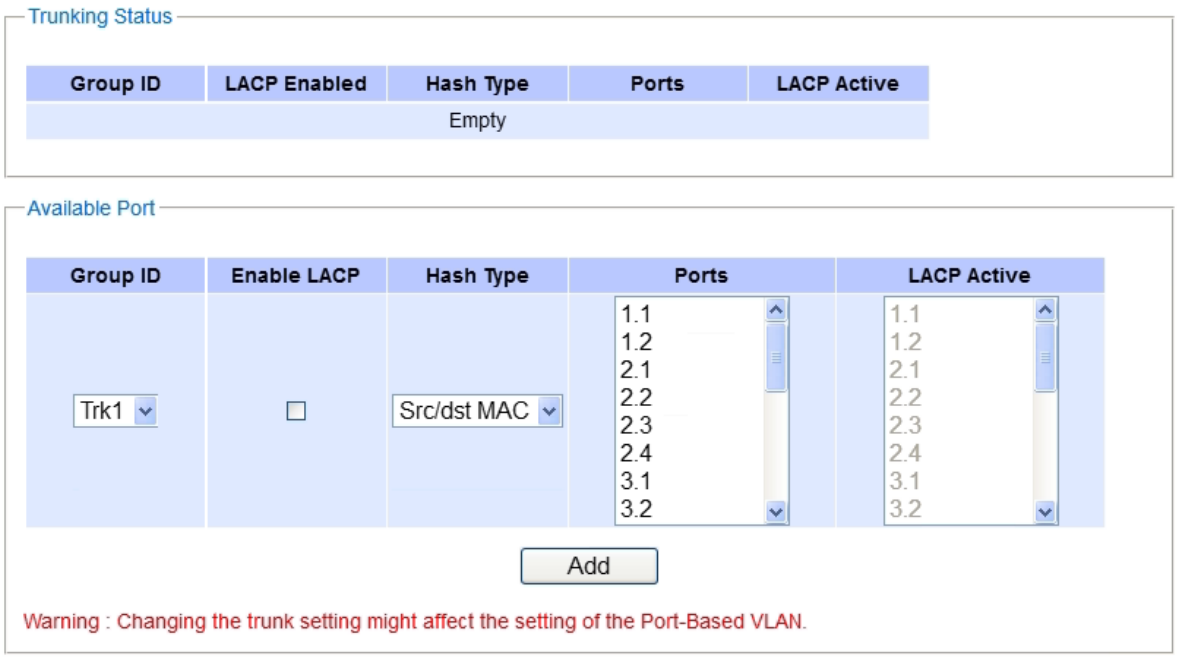


Figure 2.64Trunking Setting Webpage, example with RHG9628-410GSFP-BC-DC

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 checking on the box under the LACP column for each group. LACP allows the managed switch to negotiate an automatic bundling of links by sending LACP packets to the LACP partner or another device thatis 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 LACPport 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). To enable trunking over multiple ports, the users can follow the steps below:

Step 1:Select Trkx (x = 1 to 4) from Group IDdropdown list.
Step 2: Choose whether to enable LACP (IEEE standard, Link Aggregation Control Protocol).
Step 3: Select the Hash Typefrom the dropdown list.
Step 4: Select specific ports to be in this trunk group from the text box.
Step 5: Select specific ports in this trunk group to be LACP active.
Step 6: Click **Apply** button to set the configuration on the managed switch.

Descriptions of trunking settings are summarized in Table 2.19.

Table 2.19Descriptions of Trunking Settings

Label	Description
Group ID	Up to 4 trunk groupscan be created:Trk1~Trk4 (for RHG9628-410GSFP-BC-DC).
LACP	Enable/Disable LACP (**L**ink **A**ggregation **C**ontrol **P**rotocol). Brief explanation of LACP is discussed in previous paragraph.
Hash Type	The hash result determines which port to use for a specific frame. The available hash options are: Src MAC, Dst MAC, Src/dst MAC, Src IP, Dst IP, and Src/dst IP.
Ports	Specify the member portsfor this trunking group. Please hold **Control**key to select more than one port at a time.
LACP Active	Specify which ports within the group should bein LACP Active mode. The ports that are not selected willbe in LACP Passive mode.
Apply	Click **Apply** button to confirm the changes.
Remove	Click this button to remove any existing trunking group.

2.7.2 LACP Status

Figure 2.65 lists the current switch's trunking information. At the top of the page, the status of LACP on the managed switchis reported whether it is enabled or disabled. Next,the users can also specify the system priority here. LACP uses the system priority with the switch's MAC address to form the system ID and also during negotiation with its LACP partner. The LACP system ID is the combination of the LACP system priority value (defined in this webpage) and the MAC address of the managed switch. The system priority determines which managed switch makes the decisions on ports that will be bundled into a logical link. The lowest value determines who has higher priority and is in charge. The table of LACP status provides information per port which are port number, status of LACP, group ID, and LACP partner. Table 2.20explains the descriptions of LACP status. To change system priority, enter the desired number in the number box behind the system priority field and then click **Update** button. To obtain the latest status of the LACP, click on the **Refresh** button.

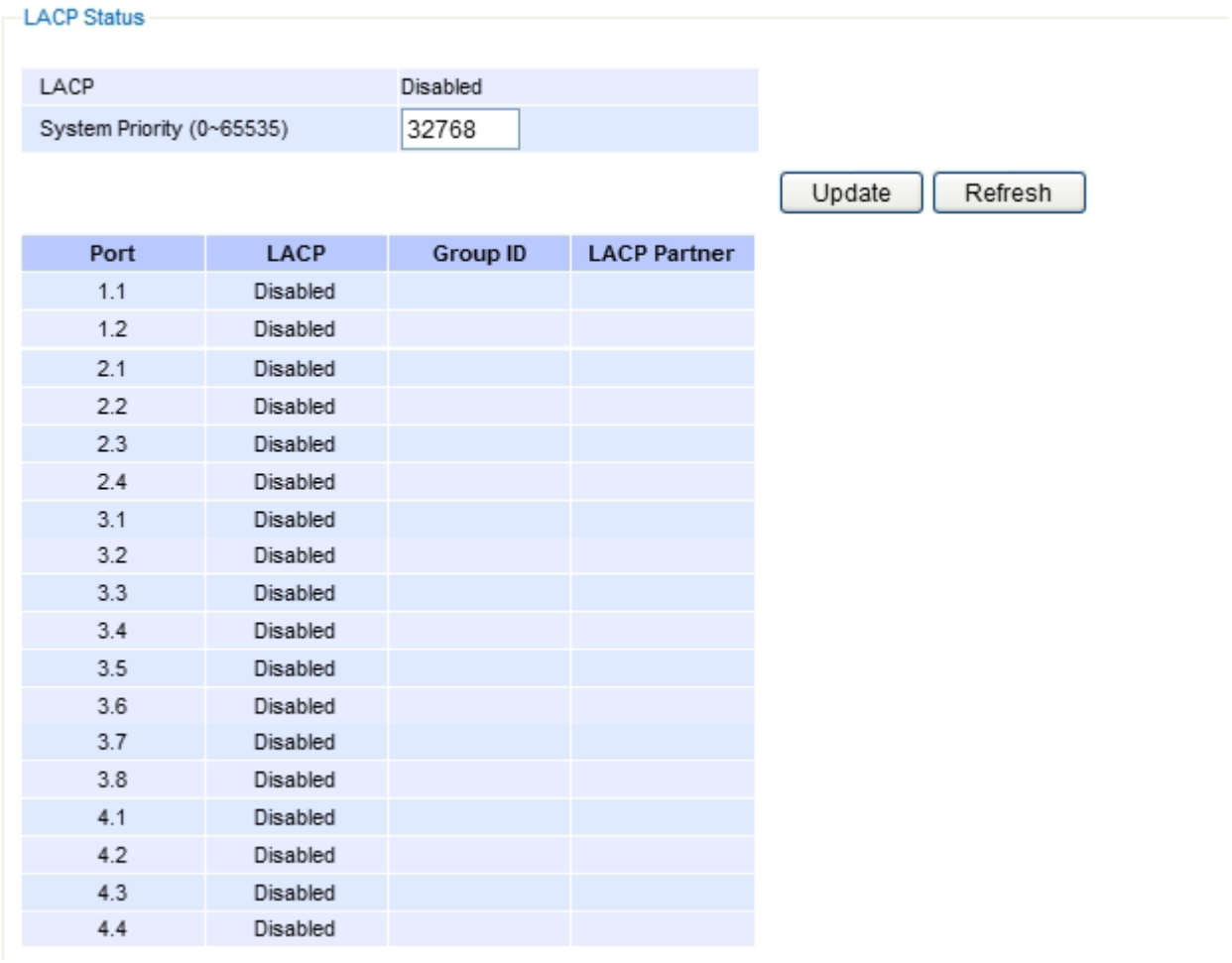


Figure 2.65LACP Webpage

Table 2.20Descriptions of LACP Status

Label	Description	Factory Default
System Priority	Indicate the system priority value of the managed switch in the range of 1 ~ 65535. System priority is used during the negotiation with other systems. System priority and switch's MAC address is used to form a system ID. Note that a higher number means a lower priority.	32768
Group ID	Show which trunk group that this port belongs to.	-
LACP	**Disabled:**LACP is disabled. **Passive:**LACP will only passively respond to LACP requests. **Active:**LACP will be actively searching for LACP Partner.	-
LACP Partner	Indicates whether a **LACP Partner**can be locatedon the other side.	-

2.8 Unicast/Multicast MAC

The managed switch is a network device which operate at the OSI layer 2 or medium access control (MAC) layer. It forwards frames of OSI layer 2 based on the MAC addresses. Generally, the layer 2 switch will learn about the destination MAC addresses of the end devices which are connected to the switch over time based on the exchanged traffic. For instance, in the beginning if the switch does not know which port a destination MAC address is, it will forward or broadcast a frame to all of its ports and wait for a response from end device connected to one of the port. This way the switch will learn of the MAC address and corresponding port number. Later on, the switch will forward the frame to the destination port only thus saving the traffic on other ports.

The managed switch typically maintains the learned MAC addresses in its memory which is usually called a MAC Address table. In this section, the managed switch allows the users to control the MAC Address table by adding static MAC addresses into the tableor filtering certainMAC addresses so that they will not be forwarded by the managed switch. Atop's manage switch also provides the users with the ability to set the MAC address age-out manually. Note that the age-out period is a duration of time that a learned MAC address will be maintained in the MAC address table before it was removed to save the memory.

The MAC addressesthat can be managed by the switch can be both Unicast and Multicast MAC addresses. This section will briefly explain the concept of Unicast and Multicastforwardingas well as their benefits. Please see Figure 2.66for illustrations of the Unicast versus the Multicast concept.

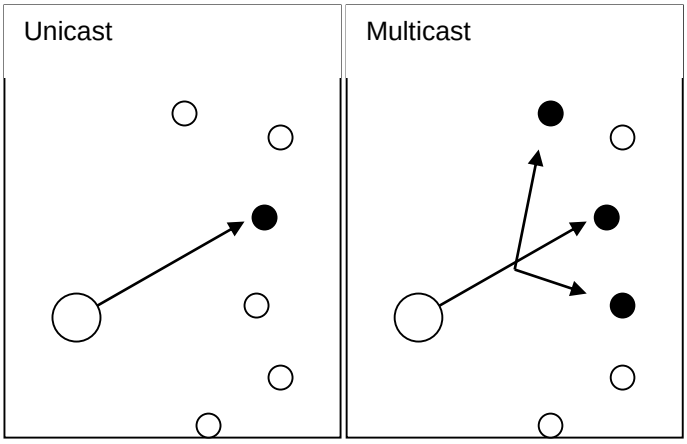


Figure 2.66Unicast vs. Multicast

- **Unicast:**This type of transmission sends messages to a single network destination identified by a unique MAC address. This method is simple with one source and one destination.
- **Multicast:** This type of transmission is more complicated. It sends messages from one sourceto multiple destinations. Only those destinations or hosts that belong to a specific multicast group will receive the multicast packets. In addition, networks that support multicast send only one copy of the information across the network until the delivery path that reaches group members diverges. At these diverging points, multicast packets will be copied and forwarded. This method can manage high volume traffic with different destinations while using network bandwidth efficiently. Multicast filtering improves the performance of networks that carry multicast traffic.

Figure 2.67shows the Unicast/Multicast dropdown menu which allows the users tomanage and view the status of MAC address table.

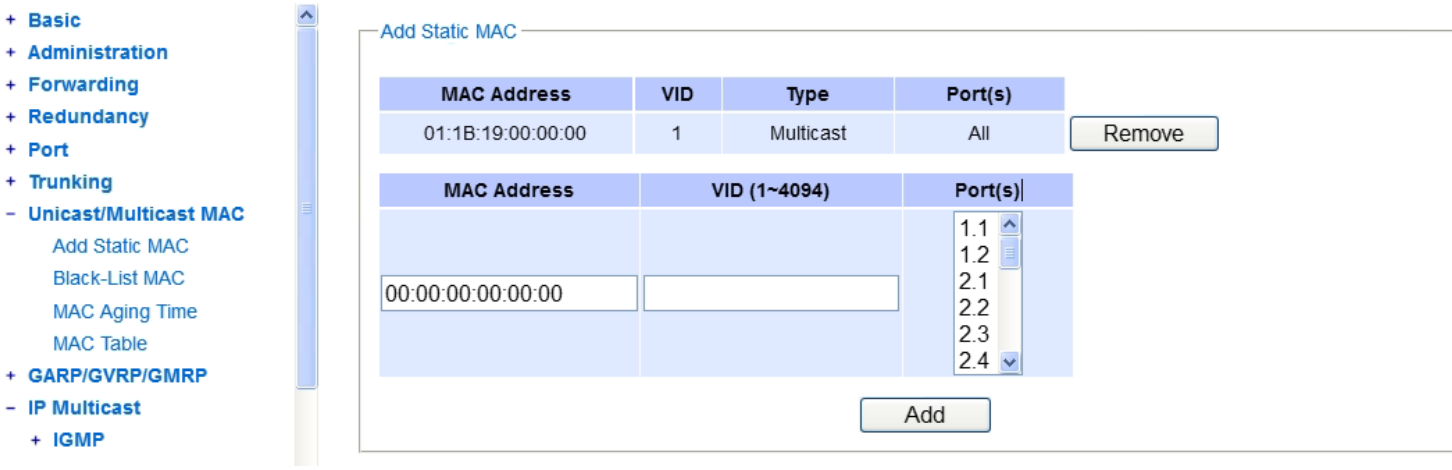


Figure 2.67Unicast/Multicast Dropdown Menu

2.8.1 Add Static MAC

The managed switch allows the users to manually add static MAC addresses into its memory. The static MAC addresses will enable the managed switch to forward the traffic based on the MAC addresses in its memory to the destination port with specific virtual local area network (VLAN) identification (**VID**). Following the simple steps here to add a static MAC address.

Step 1:Enter a **MAC Address** which can be either Unicast or Multicast MAC Address.
Step 2:Specify VLAN ID (**VID**).
Step 3:Select the ports to apply this static MAC address. Use **Ctrl-key** to add more than one port.
Step 4: Click on **Add** button.

Figure 2.68depicts the **Add Unicast/Multicast MAC** webpage. There is an example of a table of static MAC address in the upper part of the webpage where the last column of the table has **Remove** buttons for each entry. The users can remove any existing static MAC address by clicking on the **Remove** button. The lower part of the webpage is where the user can enter a new static **MAC address** along with its VLAN ID**(VID)**as outlined by the procedure above. Table 2.21summarizes the fields in this Add Static MAC webpage.

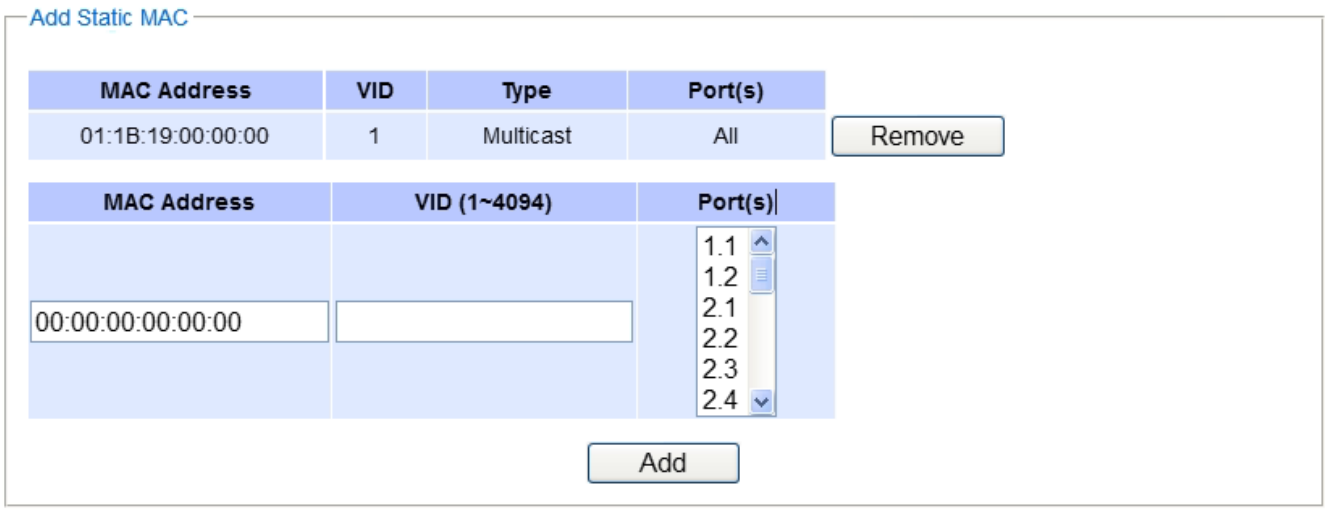


Figure 2.68Add Static MAC Webpage

Table 2.21Description of fields inAdd Static MAC Webpage

Label	Description
MAC address	Enter a MAC address manually
VID	Specify VLAN ID that this static MAC belongs to (1 –4096)
Type	Multicast or Unicast MAC address
Port(s)	Define which ports toapply this static MAC address
Add	Confirm and add the MAC addressby clicking on this button
Remove	Click on this button to remove existing static MAC addressinthe table

2.8.2 Black-List MAC

As discussed earlier, the managed switch also allows users to set MAC filtering manually. Figure 2.69shows the Black-ListMAC webpage. The upper part of the page is the table of existing filtered MAC address where the users can remove the filter by clicking on the **Remove** button on each entry. The lower part of the page is where a new **source MAC address** that the users would like to filter can be entered into the MAC filtering table (black-list). Table 2.22summarizes the fields in the **MAC Filter** webpage.

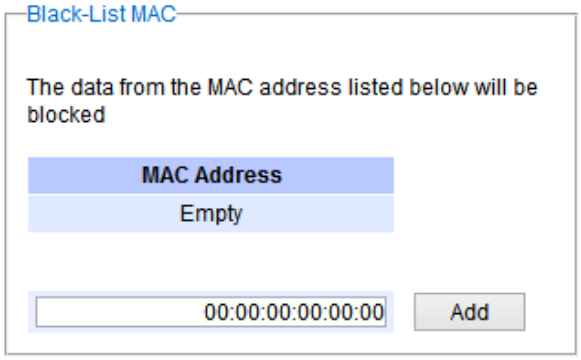


Figure 2.69Black-List MACSetting Webpage

Table 2.22Descriptions ofMAC Filtering Webpage

Label	Description
MAC Address	Enter MAC address to be black-listed or filtered manually
Remove	**Remove** the corresponding entry in MAC filteringtable
Add	**Add** a MAC addresses to the MACfilteringtable

2.8.3 MAC Aging Time

This function allows users to set MAC address age-out or aging time manually as shown inFigure 2.70. The users can specify the **Age-out Time** between 0 and 600 seconds in the following field. Note that the default value of age-out timeis 300seconds. In the managed switch, a MAC address table is stored in the memory to map a MAC address and a port number to forward frames. The aging time is the duration of time to keep MAC addresses in the MAC addresstable. For a longer aging time, the learned MAC address will stay in the memory longer. As a result, the switch will be able to forward the frames to a specific port quickly instead of forwarding to all ports to prevent frame flooding. A shorteraging time will allow the switch to free up the old MAC addressesin the table to learn new MAC addresses. This will be useful when there are large number of MAC addresses (or end devices) in the network and when the traffic between any two end devices are short-lived.

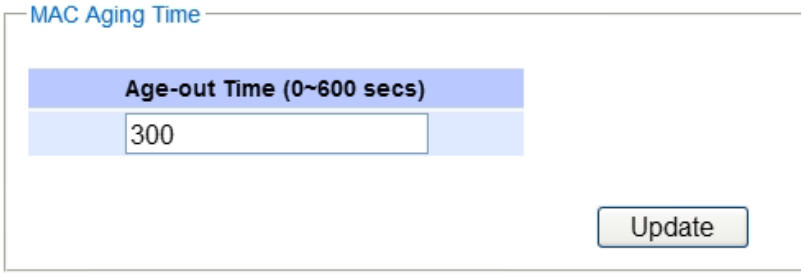


Figure 2.70MAC Aging TimeWebpage

2.8.4 MAC Table

Information of current Unicast and Multicast MAC addresses in the memory (MAC Table) of the managed switch is displayedin this webpage as shown inFigure 2.71. The list of Unicast MAC addressesis shown first and follows by the list of Multicast MAC addresses. If there are more entries to be displayed, the users can click on the **Next Page** button to see other entries. The users also have an option to clear dynamic entries in the MAC address table by clicking on the **Clear Dynamic Entries** button at the bottom of the webpage. The descriptions of the MAC Address table aresummarized in Table 2.23.

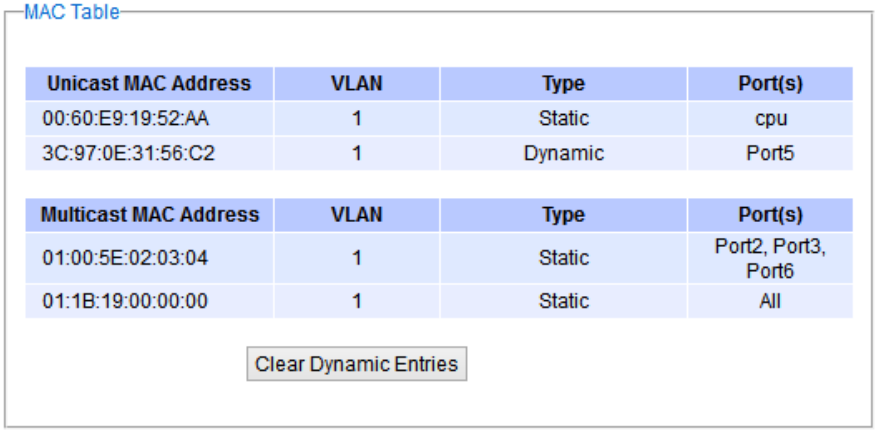


Figure 2.71MAC Table Webpage

Note: The static multicast address can be set from “Add Static MAC” (Section 2.8.1)in “Unicast/Multicast MAC” (Section 2.8)or from “Static IP Multicast” (Section2.10.5) in “IP multicast” (Section0).

Table 2.23Descriptions ofMAC Address Table

Label	Description
Unicast/Multicast MAC	Displays MAC address
VLAN	Displays VLAN ID
Type	Displays whether the MAC address is dynamic or static. Note that dynamic is the address that is learned automatically, while static is the address that is entered by the users.
Ports	Displays which port that this MAC address belongs to
Clear Dynamic Entries	Clears all Dynamic MAC addressesby clicking this button
Next Page	Clicking on this button to continue to the next page when there are more MACs available

2.9 GARP/GVRP/GMRP

This page includes three options, **GARP, GVRP, and GMRP**settings. Main concept of all three protocols are to eliminate unnecessarynetwork traffic by preventing transmission/retransmission to unregistered users. These functions are enabled by default. They can only be disabled if no MAC addresses are added in the multicast group table.

GARP:Generic **A**ttribute **R**egistration**P**rotocol, previously called **A**ddress **R**egistration **P**rotocol, is a LAN protocol that defines procedures by which end stations and switches can register and de-register attributes, such as network identifiers or addresses with each other. Every end station and switch thus has a record, or list, of all the other end stations and switches that can be reached at a given time.Specific rules are used to modify set of participants in the network topology, or socalled reachability tree.

GVRP:GARP **V**LAN **R**egistration **P**rotocol. GVRP is similar to GARP, but work with VLAN instead of other network identifiers. Itprovides a method to exchangeVLAN configuration information with other devices and conforms to IEEE 802.1Q.

GMRP:GARP **M**ulticast **R**egistration **P**rotocol provides a mechanism that allows bridges (or switches in this case) and end stations to dynamically register group membership information with the MACs of bridges (switches) attached to the same LAN segment and for that information to be disseminated acrossall bridges (switches) in the Bridged (switched) LAN that supports extend filtering services. GMRP provides a constrained multicast flooding facility similar to IGMP snooping. The difference is that IGMP is IP-based while GMRP is MAC-based.

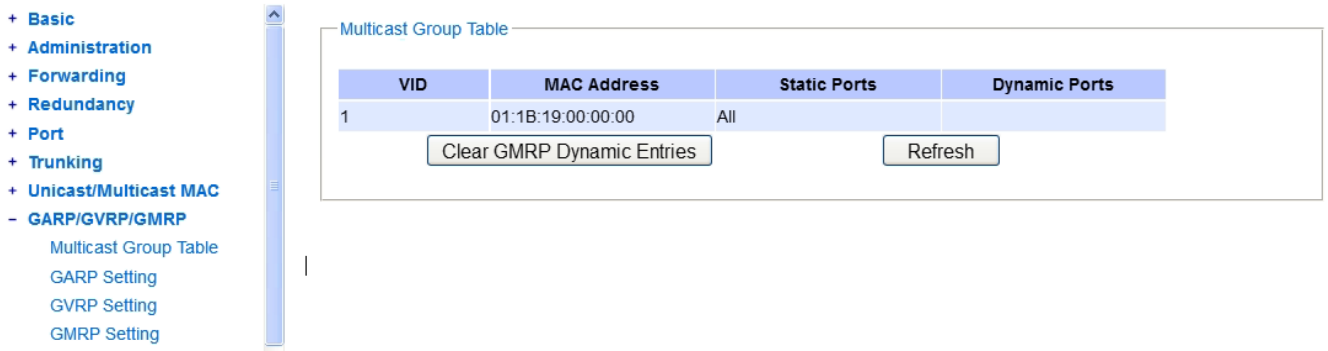


Figure 2.72 GARP/GVRP/GMRP Dropdown Menu

2.9.1 Multicast Group Table

In this subsection, the list of MAC addresses which were dynamically registered by GMRPinto the Multicast Group Table can be viewed. The multicast group table in Figure 2.73displays the following information for each MAC Address: VLAN ID (VID), Static Port(s), and GMRP's Dynamic Port(s). The user can clear the table by clicking on the Clear GMRP Dynamic Entries button or obtain the latest update on the table by clicking on the Refresh button.

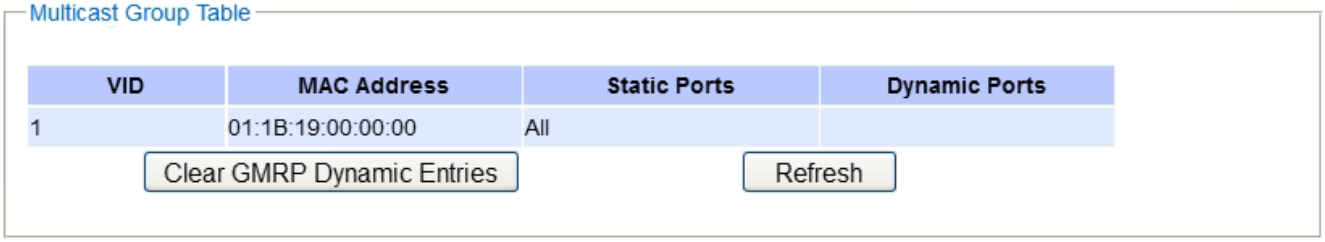


Figure 2.73Multicast Group Table

2.9.2 GARP Setting

Figure 2.74 shows GARP Setting webpage where different Timers (Join, Leave, and LeaveAll) can be set. All devices that areexchanging attributes must set these timers to the same values. Note that the GARP Timer values are in multiple of 10 milliseconds. Table 2.24 summarized the descriptions and values of all Timers for GARP setting. Please click the **Update**button after setting your new values.

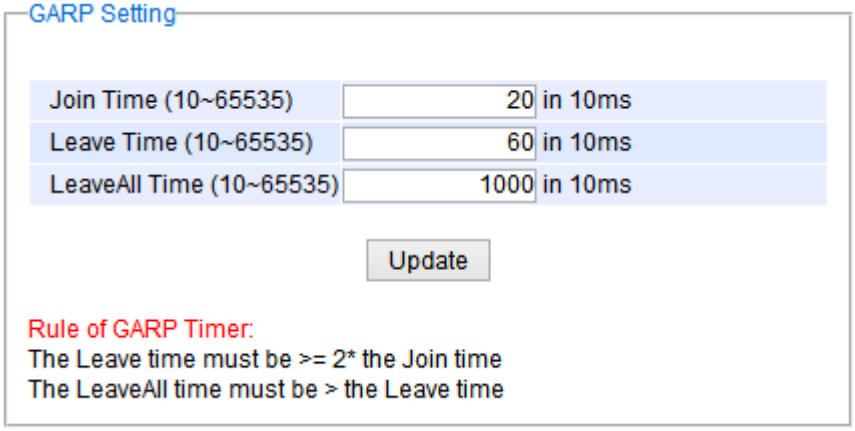


Figure 2.74GARP Setting Webpage

Table 2.24Descriptions of GARP Timer Settings

Label	Description	Factory Default
Join Timer	Indicates the GARP **Join timer,** in 0 ~ 65535 seconds	20 in 10ms
Leave Timer	Indicates the GARP **Leave timer,** in 0 ~ 65535 seconds	60 in 10ms
LeaveAll Timer	Indicates the GARP **Leave All timer**, in 0 ~ 65535 seconds	1000 in 10ms

2.9.3 GVRP Setting

In this section, GVRP can be enabled on the switchand then it can be enabled for all ports or specific port(s) and trunking group(s). The multicast IP address with designated VLAN ID can be accessed from each port. Figure 2.75and Figure 2.76below illustrate GVRP Setting and Statistics. When GVRP is enabled, the switch which is an end node of a network needs to add static VLANs locally. Others switches can dynamically learn the rest of the VLANs configured elsewhere in the network via GVRP.

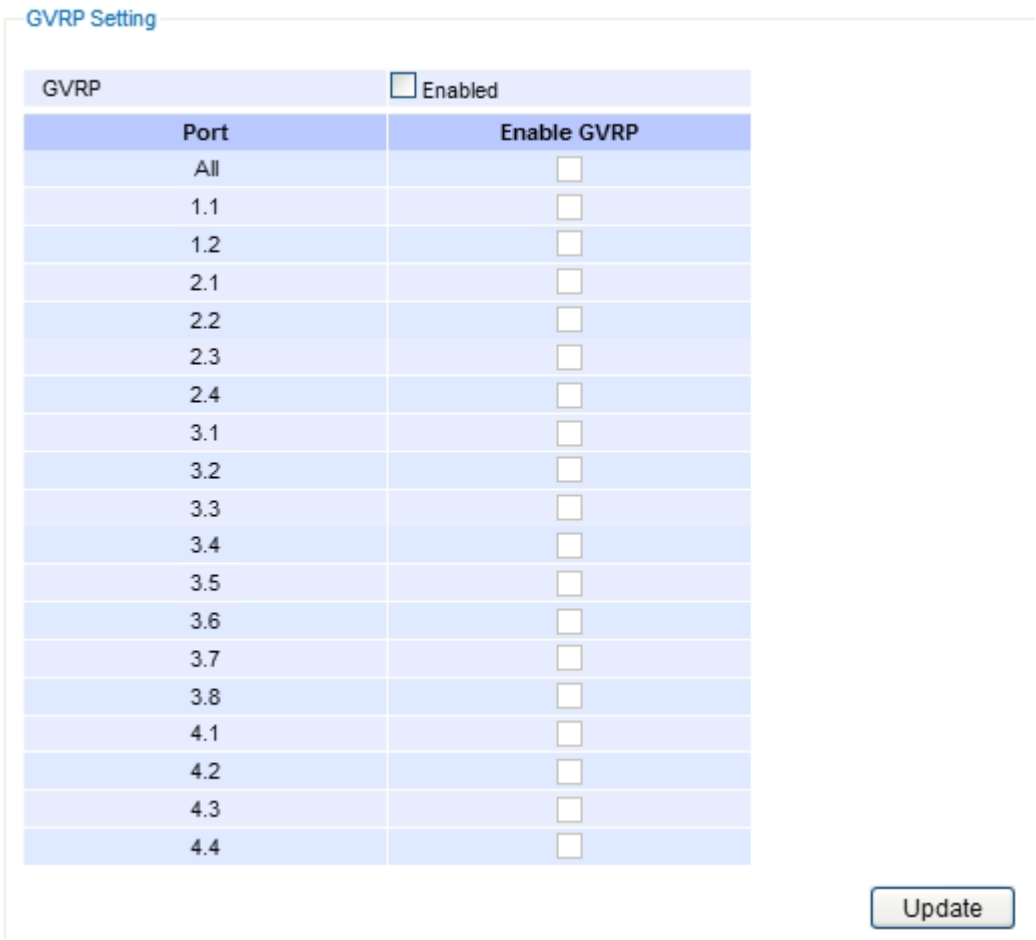


Figure 2.75GVRP Setting Box with Port Enabling

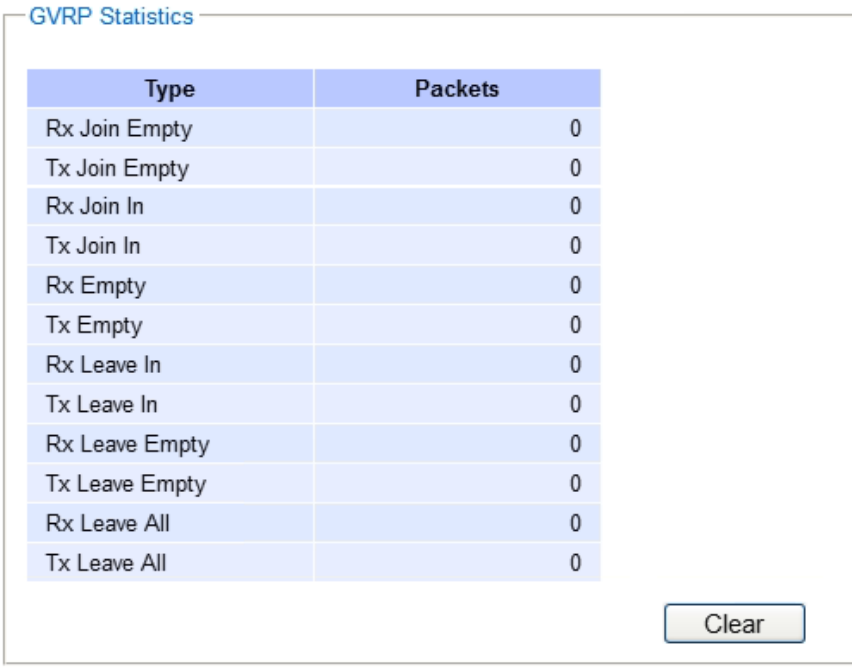


Figure 2.76GVRP Statistics

To enable GVRP in Figure 2.75, check the **Enabled**'s box and then select the desired port(s) by flagging the corresponding checkbox(es).Please click **Update** button to save the change to the switch. Figure 2.76 provides summarized statistics on the packet count of GVRP based on the following packet types: Rx Join Empty, Tx Join Empty, Rx Join In, Tx Join In, Rx Empty, Tx Empty, Rx Leave In, Tx Leave In, Rx Leave Empty, Tx Leave Empty, Rx Leave All, and Tx Leave All. To clear the statistics on this table, please click on the **Clear** button at the bottom of the table. Table 2.25 describes the GVRP setting's options.

Table 2.25GVRP Setting Descriptions

Label	Description	Factory Default
GVRP	Enables or disables GVRP protocol Enables GVRP, the switch must be in 802.1q VLAN mode	Disabled
Port	Enables or disables GVRP on each port. If users have already defined trunking group (e.g. Trk1), it can also be selected to be enabled. If you check the **All** Port's box, all ports will be enabled.	All ports are disabled
Clear Statistics	Clears all GVRP statistics counts	Clears the record

2.9.4 GMRP Setting

The users can use this subsection to enable GMRP and enable GMRP for all ports or specified port(s) andtrunking group(s) as shown in Figure 2.78. To enable GMRP in Figure 2.77, check the **Enabled**'s box and then select the desired port(s) by flagging the corresponding checkbox(es). Please click **Update** button to save the change to the switch.

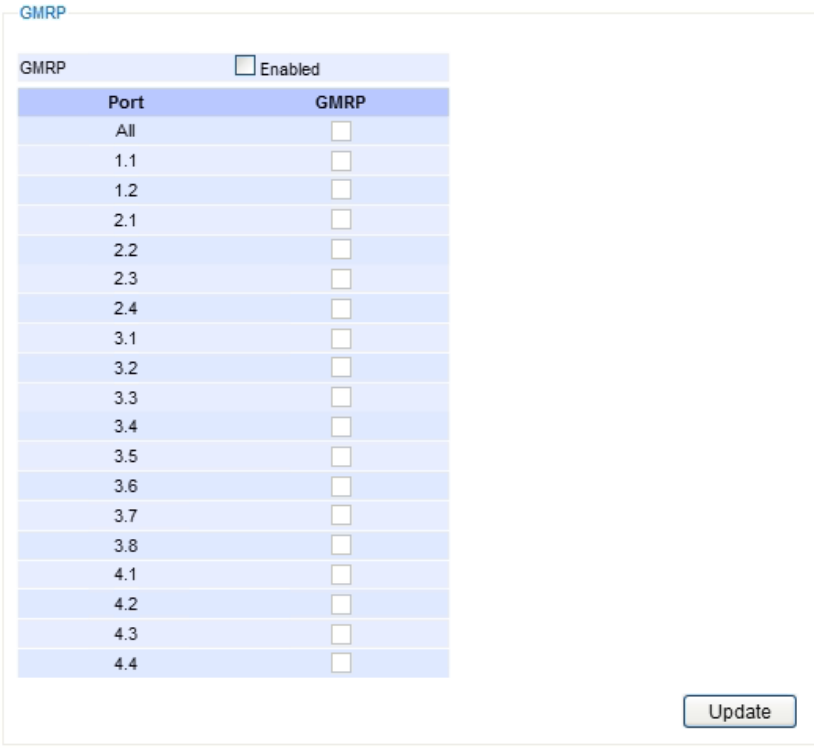


Figure 2.77 GMRP Setting Box

The GMRP Statistics can also be viewed on the bottom of this page as shown in Figure 2.78. The GMRP Statistics provides summarized statistics on the packet count of GMRP based on the following packet types: Rx Join Empty, Tx Join Empty, Rx Join In, Tx Join In, Rx Empty, Tx Empty, Rx Leave In, Tx Leave In, Rx Leave Empty, Tx Leave Empty, Rx Leave All, and Tx Leave All. To clear the statistics on this table, please click on the **Clear** button at the bottom of the table. Table 2.26 briefly describes GMRP setting and statistics.

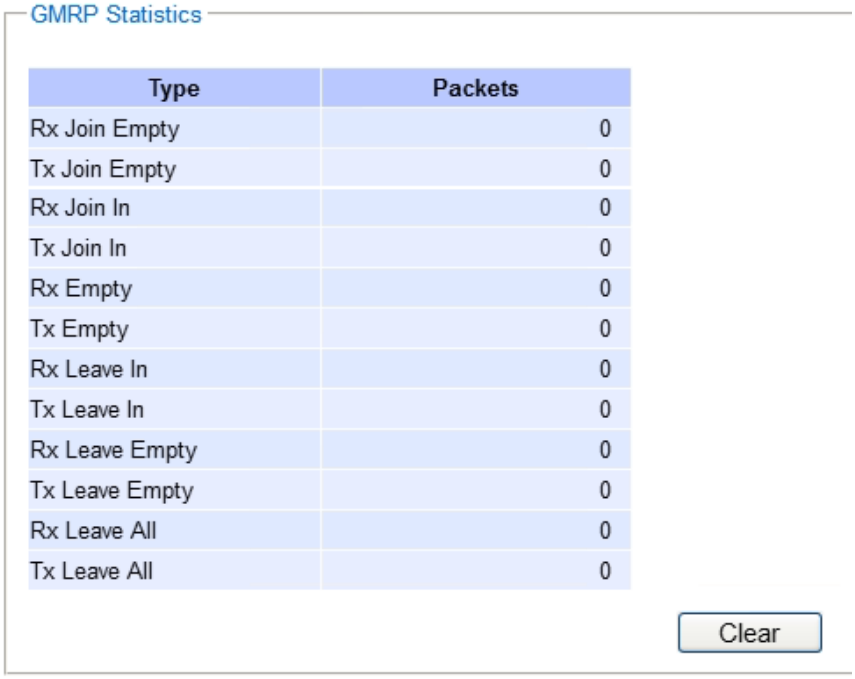


Figure 2.78GMRP Statistics

Table 2.26 Descriptions of GMRP Settings and Statistics

Field	Field Description	Factory Default
GMRP	You can enable or disable GMRP byenabling the checkbox. To enables GMRP, the switch must be in 802.1q VLAN mode.	Disabled
Port	You can enable or disable GMRP onspecified ports by clicking thecorresponding checkbox. If you have already defined trunking group (e.g. Trk1), you can also enable it. If you check the **All** Port's box, all ports will be enabled.	All Ports are disabled.
ClearStatistics	You can clear all GMRP Statistics	Clears the records

2.10 IP Multicast

The managed switch supports Internet Group Management Protocol (IGMP) which is a communication protocol used on IP version 4 networks to establish multicast group memberships among switches in the network. IGMP is an integral part of IPv4 multicast. It operates above the network layer of OSI model. One of the most important features related to this protocol is IGMP snooping, which is supported by the managed switch and greatly strengthens network functionality.The IGMP snooping is a process of“listening” to IGMP network traffic. By listening to conversations between different devices, it maintains a map of links and IP multicast streams. This means that multicast traffic may be filtered from the links of the managed switch which do not need them. Therefore, IGMP snooping enables the managed switch to only forward multicast traffic to the links that have requested it. Four additional multicast mechanisms are support by L3 managed switch, which areMLD (Multicast Listener Discovery), DVMRP, PIM (Protocol-Independent Multicast), and Static IP Multicast. This section contains five submenus as shown inFigure 2.79which are:

- IGMP
- MLD
- DVMRP
- PIM
- Static IP Multicast

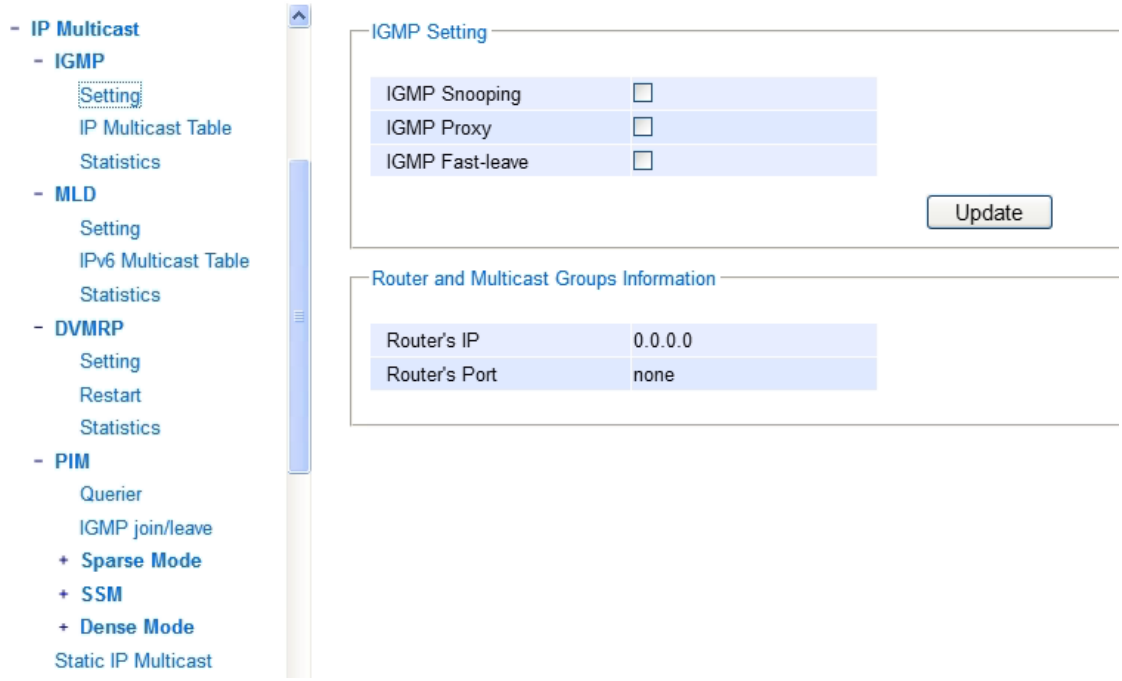


Figure 2.79IP Multicast Dropdown Menu

2.10.1 IGMP

The **IGMP**(Internet Group Management Protocol)submenu is further divided into three options which are:**Setting**, **IP Multicast Table**, and **Statistics**. Figure 2.80 shows the three options under the IGMP submenu.

Figure 2.80 IGMP's Options

2.10.1.1 IGMP's Settings

This webpage allows the users to set IGMP features on the managed switch as shown inFigure 2.81.There are three features that can be enabled:**IGMP Snooping**, **IGMP Proxy**, and **IGMP Fast-leave**. After checking the desired feature's boxes, please click on the **Update** button to allow the options to take effect.The lower part of the page lists**Router and Multicast Groups Information** which are router's IP and port information.Table 2.27summarizes the descriptions of IGMP's Settings.

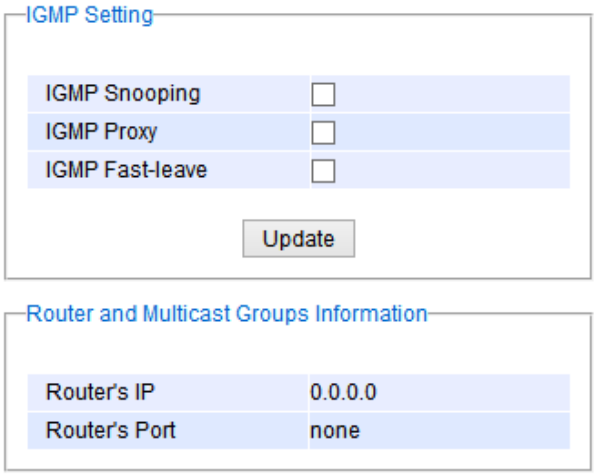


Figure 2.81IGMP Setting Webpage

Table 2.27Descriptions of IGMP'sSettings

Label	Description	Factory Default
IGMP Snooping	Checkthe box to enable IGMP snooping	Disabled
IGMP Proxy	Checkthe box to enable IGMP proxy.See note below.	Disabled
IGMPFast-leave	Checkthe box to enable IGMP Fast-leave. See note below.	Disabled
Router's IP	Display the multicast router's IP address	-
Router's Port	Display the port that is connected to multicast router	-

***NOTE:**

IGMP Snooping is a feature that enables the managed switch to listen in on IGMP conversation between hosts and a multicast enabled router. IGMP snooping allows the managed switch, which is placed in between these hosts and the multicast enabled router, to only forward multicast traffic to the links that have solicited them. Therefore, it is designed to prevent hosts connected to the managed switch's ports from receiving traffic for a multicast

group that they have not explicitly joined. It provides managed switch with a mechanism to prune multicast traffic from links that do not contain a multicast listener. This is useful for bandwidth-intensive IP multicast application.

IGMP Proxy works as an intermediate server, as shown inFigure 2.82. When it receives a membership query message from the router, it sends a membership report message to the router port. When it receives a membership report message from a computerin a new multicast group, it sends a membership report message back to the router port. When it receives a leave group message from a computerwhich is the only one in the group, it sends a leave group message to the router port and removes the computer from multicast group. Proxy is like a middle man that handles information about multicast group in between routers and computers.

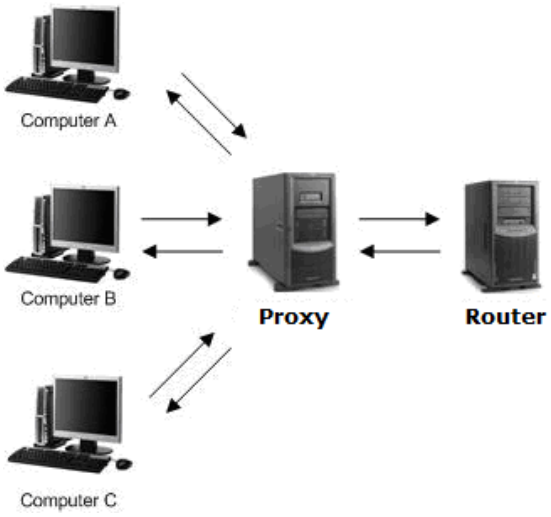


Figure 2.82Example of IGMP Proxy

IGMP Fast-leave: When a leave group message is received, the ports in the group will be immediately removed from the IP multicast entry.

2.10.1.2 IGMP's IP Multicast Table

This webpage provides information about IGMP membership table and IP multicast table. Figure 2.83depicts the IGMP'sIP Multicast Table webpage. The upper table is an IGMP membership table and the lower table is IP multicast table which contain both static configured IP multicast addresses and dynamically joined IP multicast addresses. The static configured port is manually added by the users, while the dynamically joined port is added by the managed switch's IGMP snooping feature. To get the latest update information on each table please click on the **Refresh** button.

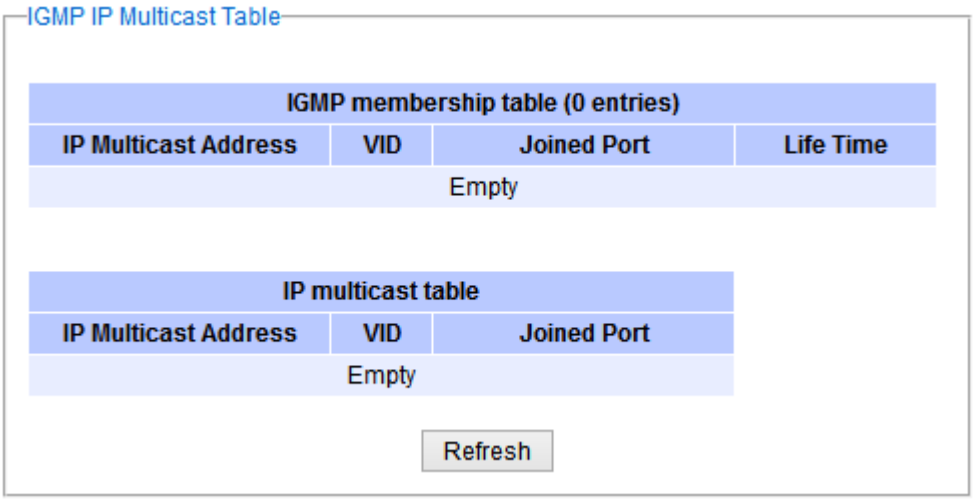


Figure 2.83 IGMP's IP Multicast Table Webpage

Figure 2.84shows examples of IGMP membership table and IP multicast table. Note that the display format in Figure 2.84is from an early version of managed switch firmware which may have a slightly different display format from Figure 2.83. These tables are based on the information in the memory of the managed switch. The IGMP membership table contains IP Multicast Address, VLAN ID(**VID**), Joined Port(port number)and Life Time. Note that the Life Time is in the unit of second. The IP multicast table has only IP Multicast Address, VLAN ID(**VID**),and Joined Port. Note that the joined port can be labelled with(S)or (D)which refer to as Static Configured or Dynamically Joined, respectively.

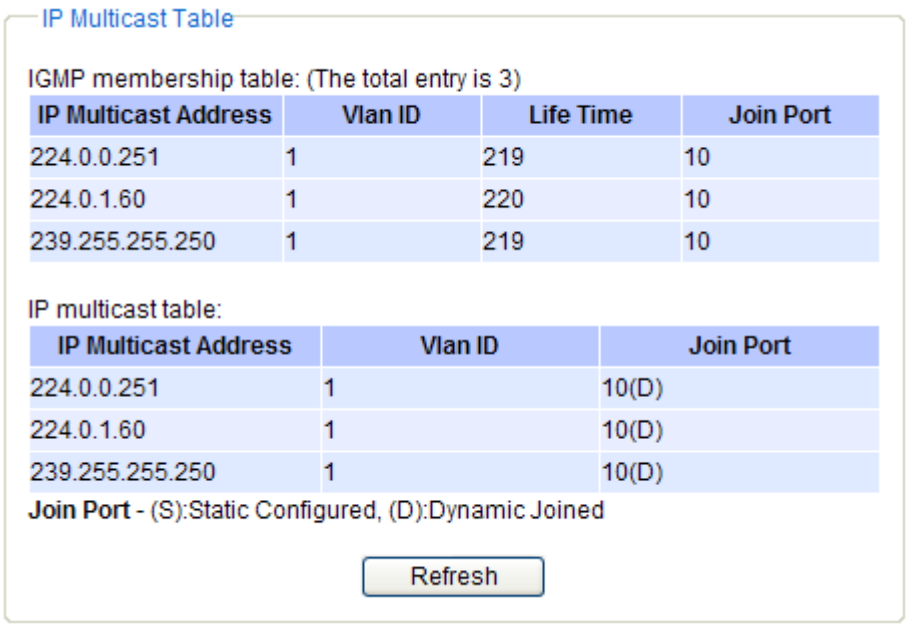


Figure 2.84 Example of IGMP's IP Multicast Table

2.10.1.3 IGMP's Statistics

This webpage provides information about IGMP statistics as shown inFigure 2.85. The users can view the number of IGMP packets in different categories: Rx Total, Rx Valid, Rx Invalid, Rx General Queries, Tx General Queries, Rx Group-Specific Queries, Tx Group-Specific Queries,Rx Leaves, Tx Leaves, Rx Reports, Tx Reports, and Rx Others. The users can reset the numbers in all categories by clicking on the**Clear** button.

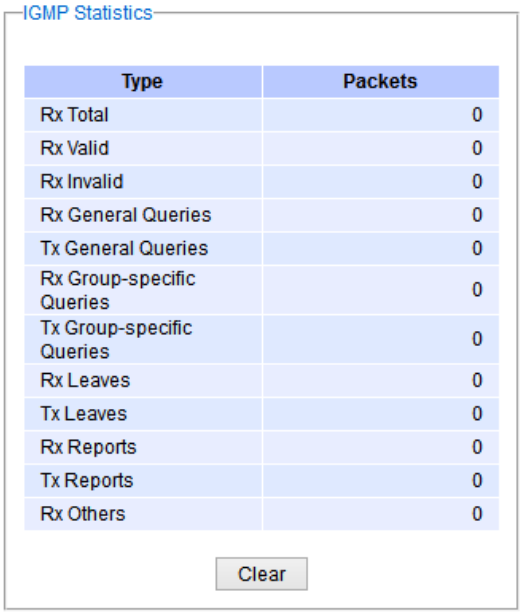


Figure 2.85 IGMP's Statistics Webpage

Example of IGMP statistics are shown in Figure 2.86. Note that the display format inFigure 2.86 is from an early version of managed switch firmware which may have a slightly different display format from Figure 2.85. It shows the statistical values of IGMPpackets which the managed switch received and transmitted over time. Table 2.28summarizes the descriptions of the IGMP statistics.

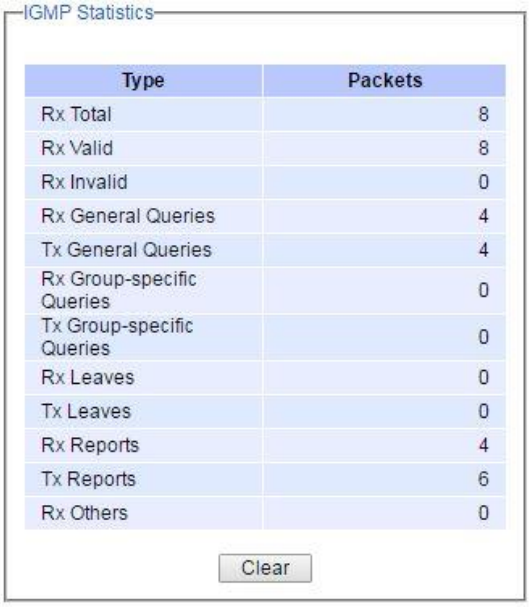


Figure 2.86 Example of IGMP's Statistics

Table 2.28 Descriptions of IGMP Statistics

Statistics Label	Description	Factory Default
Rx Total	Total number of IGMP packets received by the managed switch	-
Rx Valid	Number of valid IGMP packets received by the managed switch	-

Statistics Label	Description	Factory Default
Rx Invalid	Number of invalid IGMP packets received by the managed switch	-
Rx General Queries	Number of IGMP's Membership General Query packets received by the managed switch	-
Tx General Queries	Number of IGMP's Membership General Query packets transmitted by the managed switch	-
Rx Group Specific Queries	Number of IGMP's Membership Group Specific Query packets received by the managed switch	-
Tx Group Specific Queries	Number of IGMP's Membership Group Specific Query packets transmitted by the managed switch	-
Rx Leaves	Number of IGMP's Leave Group packets received by the managed switch	-
Tx Leaves	Number of IGMP's Leave Group packets transmitted by the managed switch	-
Rx Reports	Number of IGMP's Membership Report packets received by the managed switch	-
Tx Reports	Number of IGMP's Membership Report packets transmitted by the managed switch	-
Rx Others	Number of IGMP's other packets received by the managed switch	-

2.10.2 MLD

Multicast Listener Discovery (MLD) is a protocol used by RHG96XX in Internet Protocol Version 6 (IPv6) network to discover nodes on its directly attached interfaces that would like to receive multicast packets. These neighboring nodes are called multicast listeners. MLD is embedded in ICMPv6 (Internet Control Message Protocol Version 6) as a part of IPv6 protocol suit. It is similar to Internet Group Management Protocol (IGMP). The protocol specifically discovers which multicast addresses are of interest to its neighboring nodes. For IPv6, the address range of FF00::/8 are reserved for multicast addresses. Then, MLD provides this information to the active multicast routing protocol on the RHG96XX so that multicast packets can be delivered to all relevant interfaces and eventually to the subscribed multicast listeners. Note that MLD is an asymmetric protocol in which it specifies different behaviors for multicast listeners and for routers (or managed switches in our case). The MLD section, which is under the IP Multicast menu, contains three submenus which are Setting, IPv6 Multicast Table, and Statistics as shown inFigure 2.87.

Figure 2.87 MLD's Submenus

Typically, MLD device can be classified as one of the follows: a querier, a snooper, or a proxy. An MLD querier is a device that coordinate multicast streams and MLD membership information. The MLD querier can generate membership query message to check which nodes are group members. It can process membership reports and leave messages. An MLD snooper is a device that spies on MLD messages to create flow efficiencies by allowing only subscribed interfaces to receive multicast packets. The MLD snooper can decide on the best path to send multicast packets at Layer 2; however, it cannot alter those packets or generate its own MLD messages. An MLD proxy is a device that passes membership reports upstream towards a source in another subnet. On the downstream, the MLD proxy will forward multicast packets and queries towards one or more IP subnets.

2.10.2.1 MLD's Setting

The MLD's Setting webpage as shown inFigure 2.88. To configure the MLD on RHG96XX, the users need to configure a VLAN in the second box of the webpage called MLD VLAN Setting first. To configure the options under the MLD VLAN Setting. First, select a VLAN ID from the drop-down list of VLAN. This VLAN will be configured with the MLD snooping function. Second, the user can enable or disable MLD snooping's Fast Done function by checking the box behind this option. This function will immediately remove the membership of a multicast listener when the switch received an MLD done message. Third, the MLD Snooping function can be enabled or disabled for the selected VLAN by checking the box behind the Snooping option.

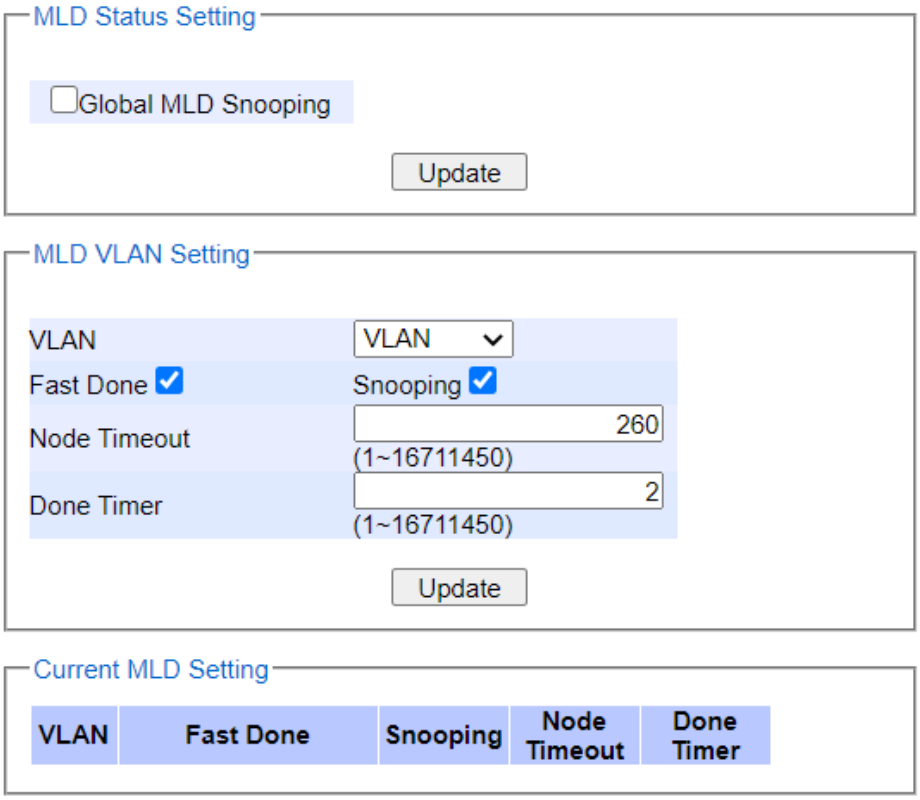


Figure 2.88 MLD's Setting

Fourth, the user can specify the amount of time that a node on a port will no longer be considered as a multicast listener. This is called Node Timeout. The default value for Node Timeout is 260 seconds. Fifth, the user can specify the amount of time that a multicast group will remain in the switch after the switch receives a done message of the multicast group without receiving a node listener report. This is called Done Timer. The default value for Done Timer is 2 seconds. Finally, clicking on the Update button to update the configuration of MLD on the selected VLAN ID. The entry of the configured VLAN should be listed in the next part of the webpage.

After setting the VLAN in the step above, the user can enable the Global MLD Snooping option inside the MLD Status Setting box. Then, click **Update** button to enable the MLD protocol on RHG96XX. Note that the MLD snooping is the key to efficient multicast traffic flow in a Layer 2 network of RHG96XX managed switch. If no MLD VLAN Setting was done on any VLAN, the user will encounter an error message as show in Figure 2.89.

Figure 2.89Error: No vlans configured for MLD

The current VLANs with MLD setting are listed in the last part of the webpage under the Current MLD Setting box. The setting is summarized as a table with all the options associated with particular VLAN ID. To remove any entry of the MLD setting, the user can click on the Delete button for that particular entry.

2.10.2.2 MLD's IPv6 Multicast Table

This webpage provides information about IPv6 Multicast Table and MLD membership table. Figure 2.90shows the MLD's IPv6 Multicast Table webpage. The table inside the box is an MLD membership table which contains entries of MLD memberships. Each entry consists of Port Listener, VID (VLAN ID), Multicast group, MAC address, Reports, and Live Time columns. The Multicast group column shows the IPv6 address of the multicast group in each entry. The MAC address column shows the corresponding MAC address of the multicast group in that particular entry. The Reports column displays the number of group reports for that multicast group. The Port Listener column lists the Port number for each entry. To get the latest update information on each table please click on the Refresh button. lists the Port number for each entry. To get the latest update information on each table please click on the Refresh button.

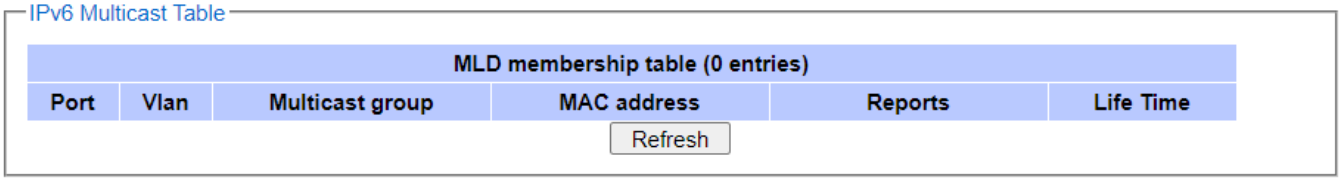


Figure 2.90 MLD's IPv6 Multicast Table

2.10.2.3 MLD's Statistics

This webpage provides information about MLD's statistics as shown in Figure 2.91, which is similar to the IGMP statistics. The users can view the number of MLD packets in different categories: Rx Total, Rx Valid, Rx Invalid, Rx General Queries, Tx General Queries, Rx Group-Specific Queries, Tx Group-Specific Queries ,Rx Leaves, Tx Leaves, Rx Reports, Tx Reports, and Rx Others. The users can reset the numbers in all categories by clicking on the Clear button. Table 2.29 summarizes the descriptions of the IGMP statistics.

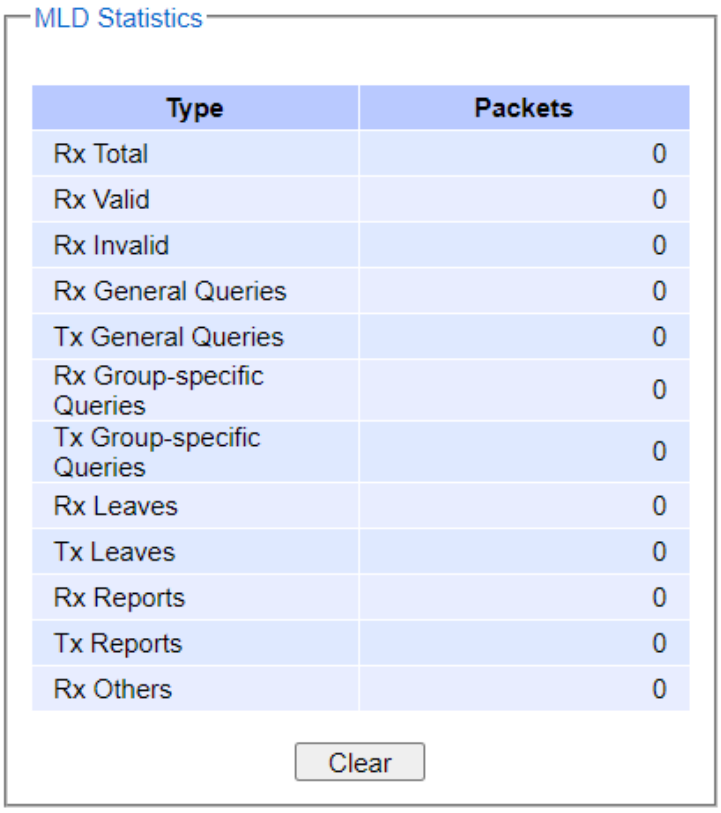


Figure 2.91 MLD's Statistics

Table 2.29 Description of MLD's Statistics

Statistics Label	Description
Rx Total	Total number of MLD packets received by the managed switch
Rx Valid	Number of valid MLD packets received by the managed switch
Rx Invalid	Number of invalid MLD packets received by the managed switch
Rx General Queries	Number of MLD's Membership General Query packets received by the managed switch
Tx General Queries	Number of MLD's Membership General Query packets transmitted by the managed switch
Rx Group Specific Queries	Number of MLD's Membership Group Specific Query packets received by the managed switch
Tx Group Specific Queries	Number of MLD's Membership Group Specific Query packets transmitted by the managed switch
Rx Leaves	Number of MLD's Leave Group packets received by the managed switch
Tx Leaves	Number of MLD's Leave Group packets transmitted by the managed switch
Rx Reports	Number of MLD's Membership Report packet received by the managed switch
Tx Reports	Number of MLD's Membership Report packet transmitted by the managed switch
Rx Others	Number of MLD's other packets received by the managed switch

2.10.3 DVMRP

Distance Vector Multicast Routing Protocol (DVMRP) is a routing protocol for IP multicast packets. It is described in RFC 1075 as an interior gateway protocol (IGP) within a multicast domain and is derived from Routing Information Protocol (RIP), which is suitable for use within an autonomous system. DVMRP uses the Internet Group Management Protocol (IGMP) to exchange routing information with other routers. It operates via a reverse path flooding technique in which it sends a copy of received IGMP message (containing routing information) out through each interface except the one at which the message arrived. By using flooding technique, the DVMPR may not scale

very well in some network topologies. DVMRP creates a routing table with route entries that map between multicast group (IP address) and source address. The purpose of DVMRP is to keep track of the return paths to the source of multicast datagrams. DVMRP router dynamically discovers their Neighbors by sending Neighbor probe messages periodically to an IP multicast group address that is reserved for all DVMRP routers.

To enable DVMRP on RHG96XX, you first need to configure at least two VLAN interfaces, set all relevant parameters for the interfaces such as IP addresses,DVMRP VLAN and enable IP Routing. We present these steps in detail as follows:

1. Add at least two VLANs in **802.1Q VLAN** menu as described in Section 2.14.2.1. Figure 2.92 shows examples of three VLAN settings which are named vlan10, vlan20, and 4090. Note that this is only for illustration. For each VLAN, you need to set the **Name** and VLAN identifier (**VID**). Then, select one or multiple **Member Ports** from the list for that VLAN. For **Tagged Ports**, you can select one or multiple ports from the list or leave it empty when you do not want to add VLAN tag to the outgoing packet (the packet will assume the native VLAN number). Note that you can select multiple ports from the list by selecting desired ports while holding the Ctrl-key. Importantly, all the configured VLAN ports should to be removed from the DEFAULT member port list. Finally, click **Add/Modify** button to add a new entry to the upper table in Figure 2.92

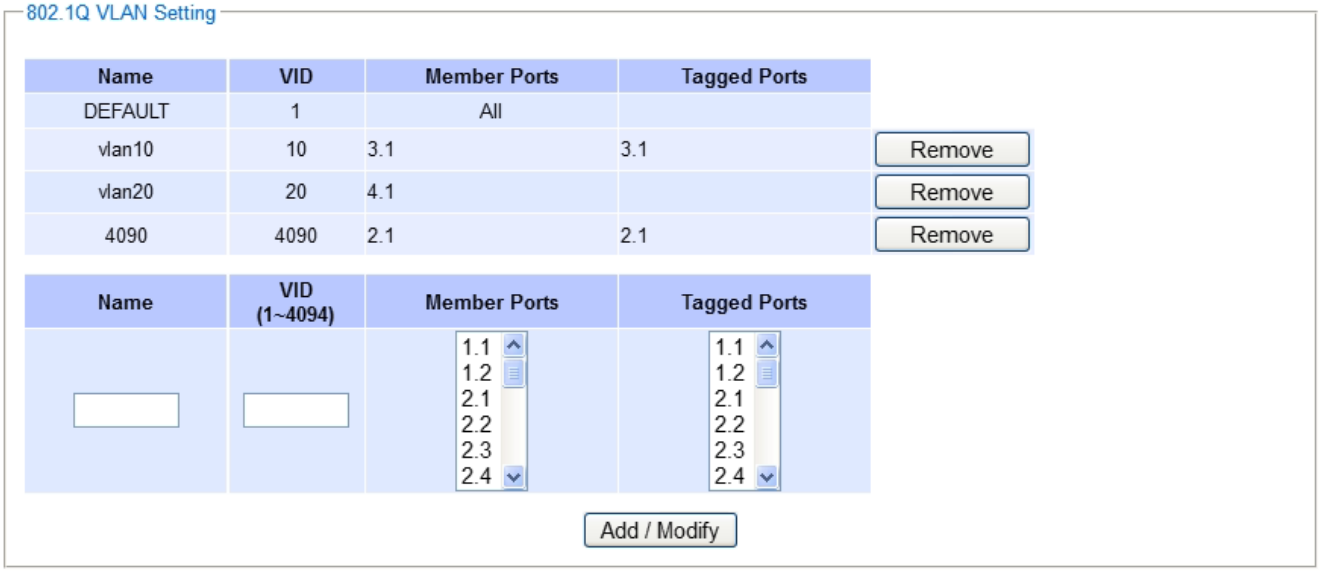


Figure 2.92 Example of Setting 802.1Q VLAN Interface for Multicast Routing

2. Setting the Port VLAN ID (**PVID**) or native VLAN number for port in **PVID Setting** menu as described in Section 2.14.2.2. The **PVID** must be the same as the VLAN identifiers (**VID**) set in previous step for multicast routing. Figure 2.93 depicts example of setting Port 3 and Port 4 with PVID = 10 and 20, respectively. You can assign one or multiple ports to the same Port VLAN ID (PVID). The Port VLAN ID can be the number from 1 to 4094. Note that the default value of Port VLAN ID is 1.

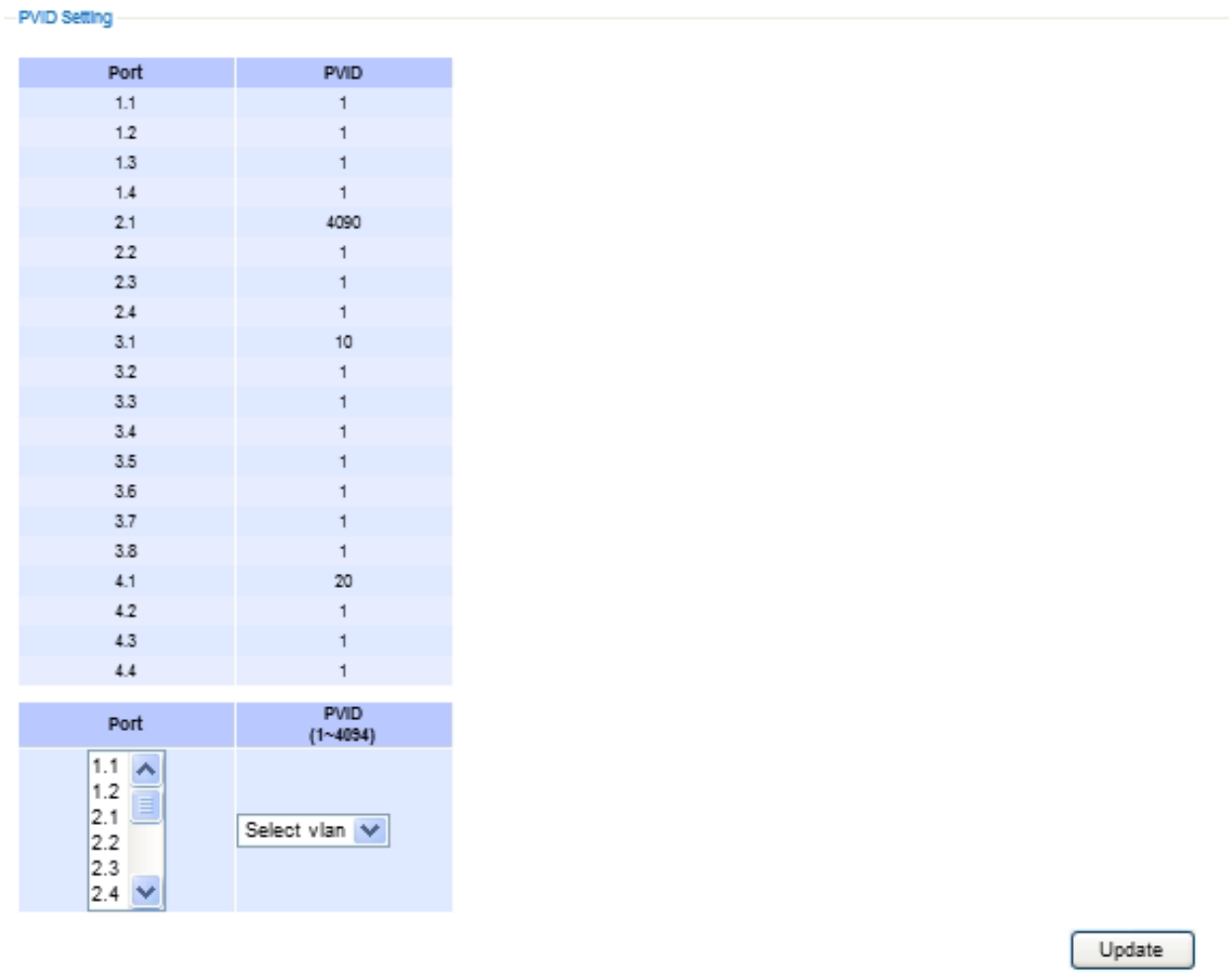
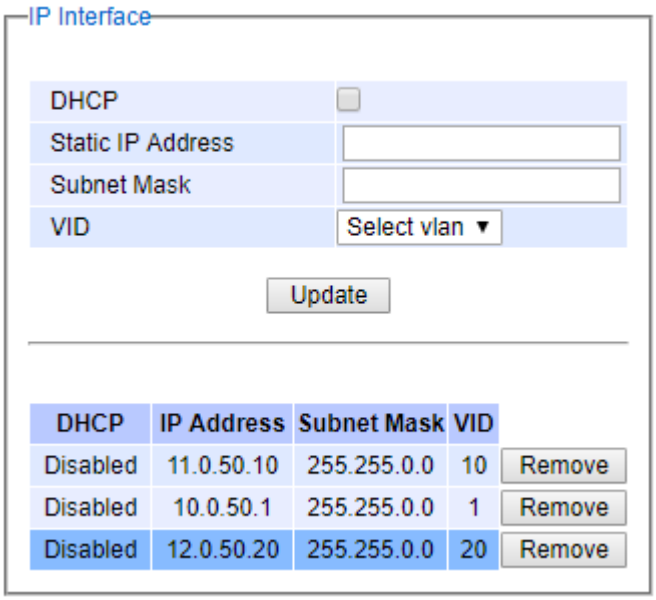


Figure 2.93 Example of Setting Port VLAN ID (PVID) for Multicast Routing

3. Assign IP addresses for VLANs which were set in the first step in **IP Setting** submenu under **Administration** menu as described in Section 2.3.2. Figure 2.94 shows example of assigned IP Addresses and Subnet Masks for VLAN identifier (VID) = 10 and 20 which were set for multicast routing.



11.0.50.1161

Figure 2.94 Example of IP Address Setting for VLAN Interfaces used in Multicast Routing

4. Configure DMVRP Interfaces as explained in the next subsection (**DVMRP Setting**).

5. To enable DVMRP process on RHG96XX, you can click on the **Enable** button on the DVMRP menu inside the **Running Status** box as shown in Figure 2.95.

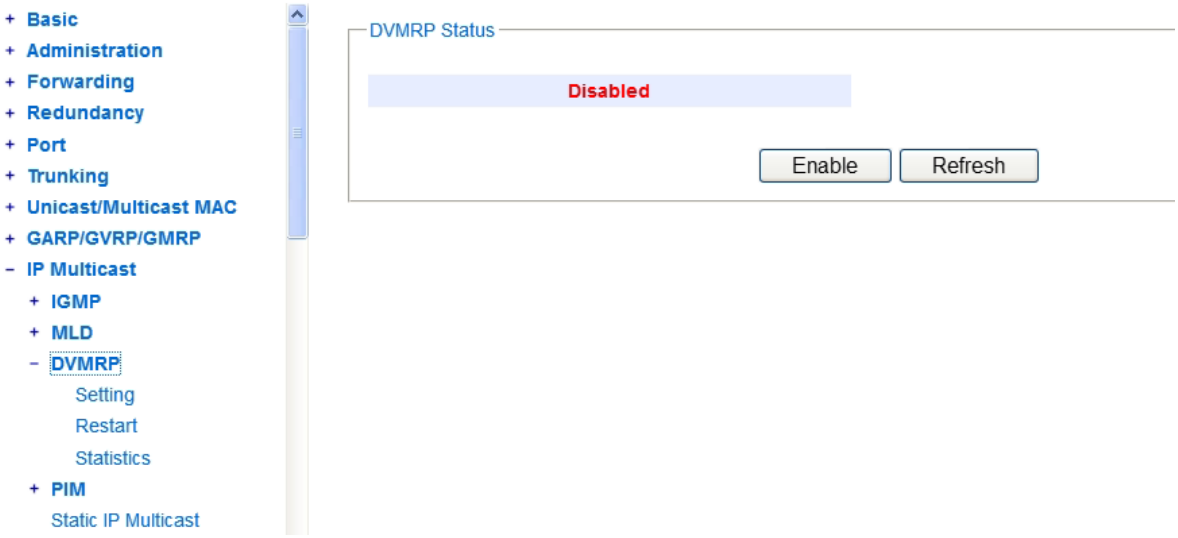


Figure 2.95 DVMRP Running Status Web Page

Note that you will be notified with an error message as shown in Figure 2.96 if the minimum of two DVMRP VLAN interfaces were not configured as described in Step 1 to 5, and you are trying to enable the DVMRP on this **DVMRP Running Status** box.

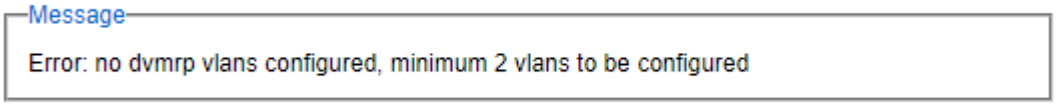


Figure 2.96 Error Message When Enabling DVMRP with no DVMRP VLANs

2.10.3.1 DVMRP Setting

On this submenu, it allows you to add or remove VLAN interface(s) from DVMRP interface(s). Figure 2.97 illustrates the **DVMPR Setting** web page that consists of two parts: the **DVMRP Settings** and the table of DVMRP interface(s). To add a VLAN interface to the **DVMRP Setting**, you first select a **VLAN** ID from the drop-down list and fill in a desired **Route Matric** between 1 and 31. The **Route Metric** is the cost of the path (or VLAN interface) through which the packet will be sent. Note that the default metric is 1.Then click on the **Add VLAN** button inside the **DVMRP Settings** box. Note that you must already configure DVMRP VLAN interfaces first as described in previous subsections.

To remove an VLAN interface from the DVMRP Setting, you can check the corresponding box in front of a VLAN entry inside the lower part of the web page. Then, click on the **Delete** button. To check the latest configuration of the DVMRP Settings, you can click on the **Update** button to refresh the web page.
12.0.50.20 24

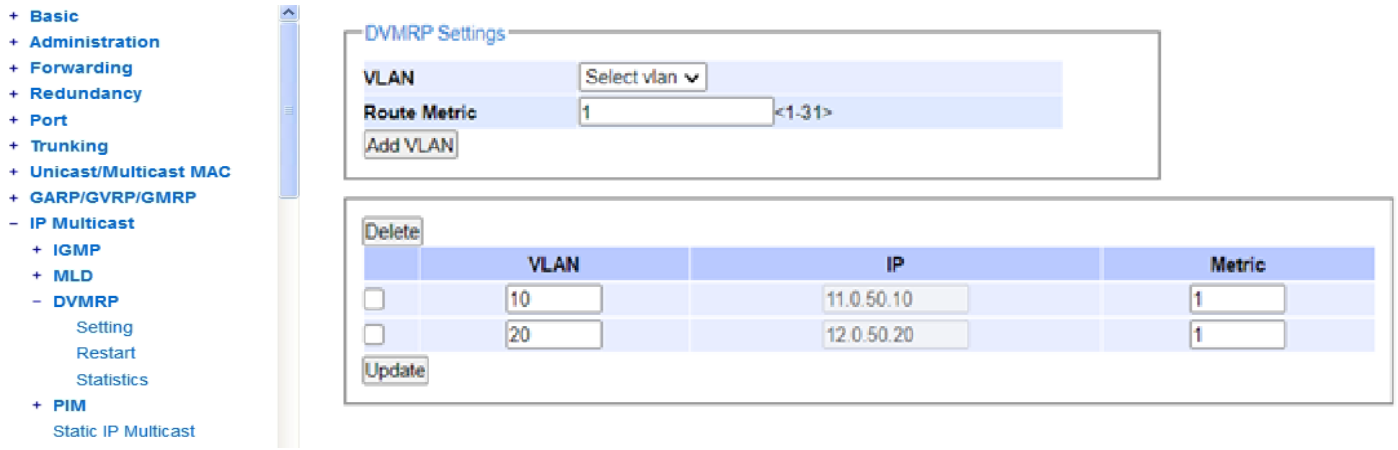


Figure 2.97 DVMRP Setting Web Page

2.10.3.2 DVMRP Restart

Figure 2.98 shows the **DVMRP Restart** submenu that allows you to restart the DVMRP process inside the RHG96XX Layer-3 Managed Switch by simply clicking on the **Restart** button.

Figure 2.98 DVMRP Restart Web Page

2.10.3.3 DVMRP Statistics

Under **DVMRPStatistics** web page as shown in Figure 2.99, you can view the DVMRP Routing Table or **Multicast Routing Table**. Inside the table, there are entries of mapping between **Source**'s IP address and IP address of Multicast **Group**. Note that if the DVMRP was not enabled, the multicast routing table will not be available and the web page will display an error message as shown in Figure 2.100.

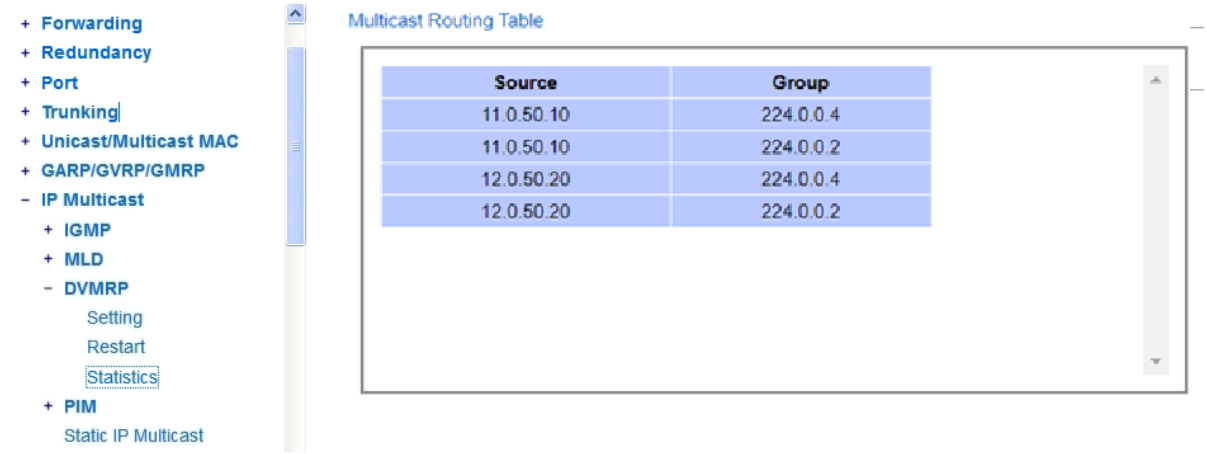


Figure 2.99 DVMRP Statistics Web Page

Figure 2.100 Error Message on DVMRP Statistics Web Page

2.10.4 PIM

ProtocolIndependent Multicast (PIM) is a set of multicast routing protocols developed for large heterogeneous inter-networks. Routers or Layer-3 switches that utilize PIM will interact to create and maintain multicast distribution trees that help forwarding IP multicasting packets to members of multicast group. It is efficient for multicasting topology that multicasting senders and group members are distributed sparsely across wide area and inter-domain internets. PIM is not dependent on any particular unicast routing protocoland uses soft-state reliability mechanisms to adapt to chaging in network conditions and group memberships. It does not perform topology discovery by itself and does not build its own routing table. Instead, PIM uses existing unicast routing tables which can be computed by any unicast routing protocol in use on the network for reverse path forwarding. It utilizes the traditional IP multicast model of receiver-initiated membership and supports both group-shared and shortest-path trees.

RHG96XX Layer-3 Managed Switch supports three modes of operation for Protocol Independent Multicast (PIM) routing protocols which are Sparse Mode (SM), Source-Specific Multicast (SSM) mode, and Dense Mode (DM). Figure 2.101shows the submenus under the PIM menu.

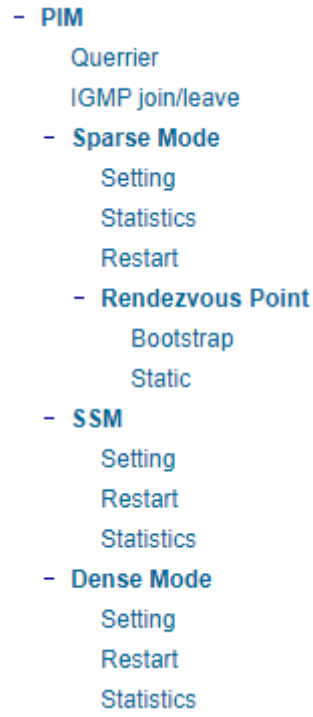


Figure 2.101 PIM Menu and Its Submenus

To enable PIM on RHG96XX Layer-3 Managed Switch, you first need to configure at least two VLAN interfaces for PIM Sparse Mode and PIM Dense Mode or at least one VLAN interface for PIM Source Specific Multicast (SSM) mode. Additionally, all relevant parameters for multicast routing must be configured such as VLAN's IP addresses, IGMP mechanism, and IP routing function. Note that before enabling any of the three PIM modes, you will also need to go through the **Setting** web page under each PIM mode too. We summarize these steps in detail as follows:

1. Setting up VLANs in 802.1Q VLAN menu as described in Section 2.14.2.1. Figure 2.102shows examples of three VLAN settings which are named vlan10, vlan20, and vlan30. Note that this is only for illustration. For each VLAN, you need to set the **Name** and VLAN identifier (**VID**). Then, select one or multiple **Member Ports** from the list for that VLAN. For **Tagged Ports**, you can select one or multiple ports from the list or leave it empty when you do not want to add VLAN tag to the outgoing packet (the packet will assume the native VLAN number). Note that you can select multiple ports from the list by selecting desired ports while holding the Ctrl-key. Finally, click **Add/Modify** button to add a new entry to the upper table inFigure 2.102.

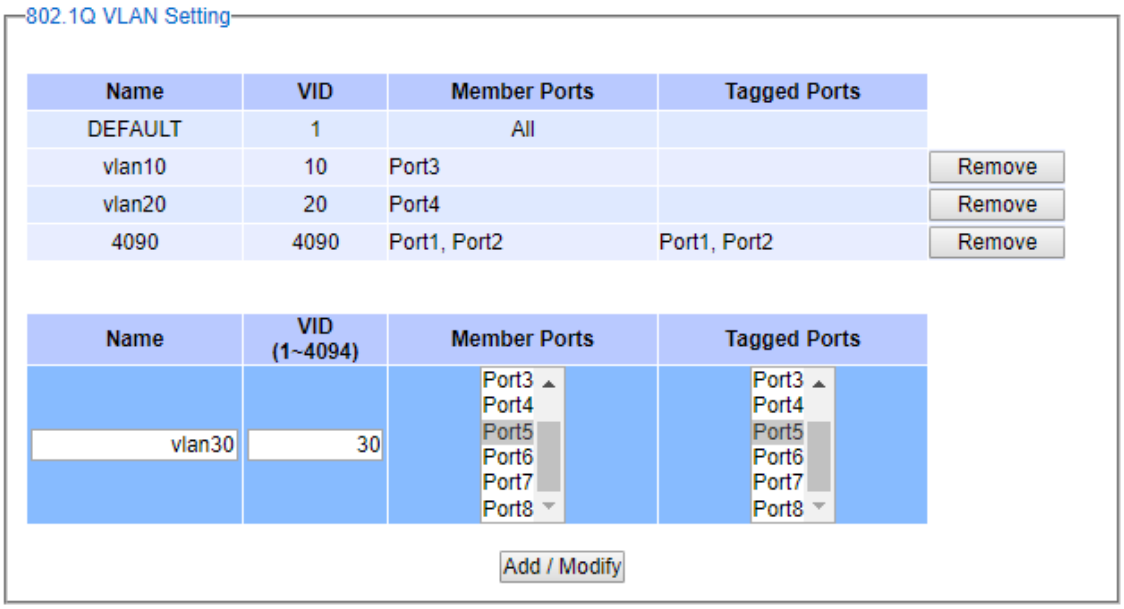


Figure 2.102 Example of Setting 802.1Q VLAN Interface for PIM Protocol

2. Setting the Port VLAN ID (**PVID**) or native VLAN number for port in **PVID Setting** menu as described in Section 2.14.2.2. The **PVID** must be the same as the VLAN identifiers (**VID**) set in previous step for multicast routing. Figure 2.103depicts example of setting Port 3 and Port 4 with PVID = 10 and 20, respectively. You can assign on or multiple ports to the same Port VLAN ID (PVID). The Port VLAN ID can be the number from 1 to 4094. Note that the default value of Port VLAN ID is 1.

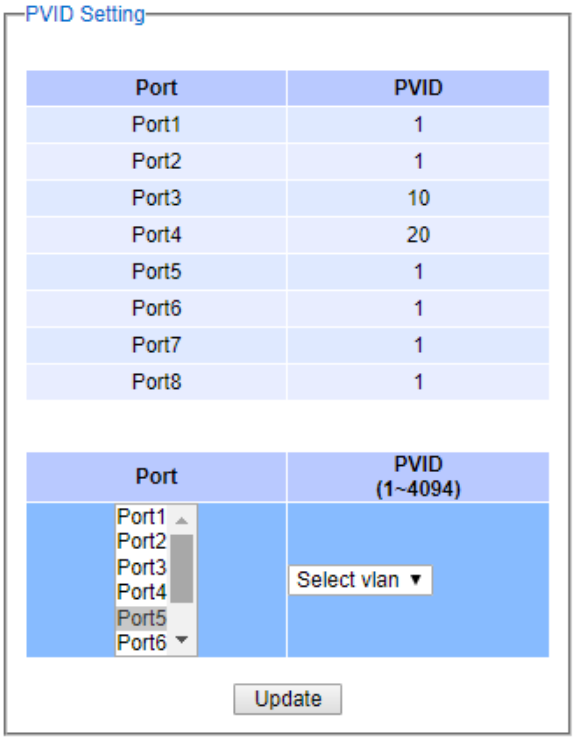


Figure 2.103 Example of Setting Port VLAN ID (PVID) for PIM

3. Assign IP addresses for VLANs which were set in the first step in **IP Setting** submenu under **Administration** menu as described in Section 2.3.2. Figure 2.104shows example of assigned IP Addresses and Subnet Masks for VLAN identifier (VID) = 10 and 20 which were set for multicast routing.

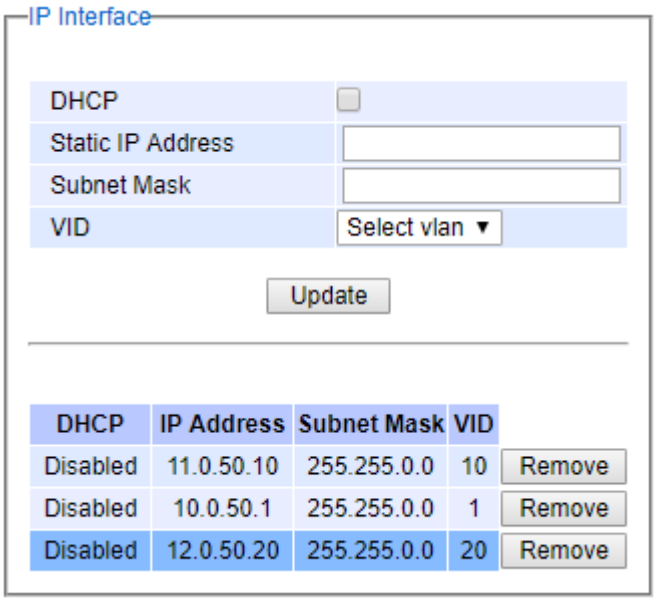


Figure 2.104 Example of IP Address Setting for VLAN Interfaces used in PIM

4. The IP routing or L3 routing function must be enabled on the RHG96XX Layer-3 managed switch as shown inFigure 2.105. This is required for Protocol Independent Multicast (PIM) because it does not have topology discovery mechanism. This can be done in **Setting** submenu under **IP Routing** menu as described in Section 2.21.1

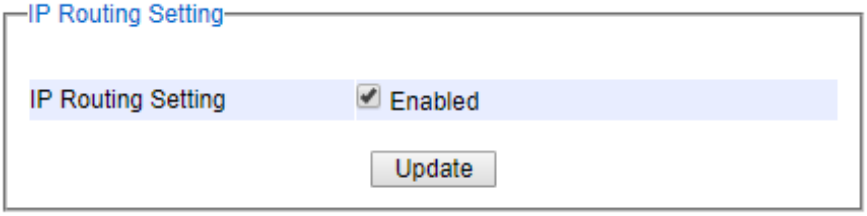


Figure 2.105 Enabling of IP Routing Function in Layer-3 Managed Switch for PIM

5. Configure the **IPv4 Static Routing** as described in Section 2.21.2 for desired IPv4 multicast address range such as 239.0.0.0 and subnet mask 255.0.0.0 for the VLAN interface used in PIM.

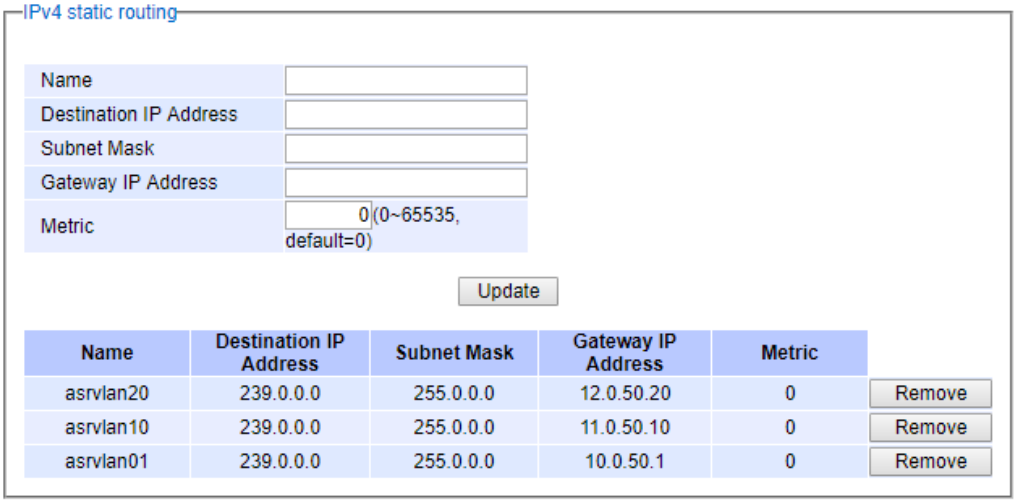


Figure 2.106 Example of Adding Static Routes for PIM

1. Alternatively, configure OSPF as described in Section 2.21.4 如下
2. Configure the desired mode of PIM as described in Section 2.10.4.3 and/or Section2.10.4.4, and/or Section2.10.4.5.

2.10.4.1 Querier

To enable any of the PIM mode, you will need to configure **IGMP Querier Settings** as shown in Figure 2.107. This interval is the time between IGMP queries when the RHG96XX Layer-3 Managed Switch is elected as querier. The value can be set from 12 to 60 seconds.

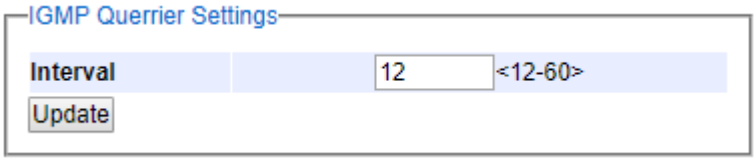


Figure 2.107 PIM's IGMP Query Interval Setting Web Page

2.10.4.2 IGMP join/leave

This web page as shown in Figure 2.108called **IGMP join/leave** allows you to manually send IGMP Join or IGMP Leave messages. You will need to configure the fields in the message which are **VLAN** identifier, multicast **Group Address**, **Source Address**, and type of message which can be either **Join** or **Leave**. Note that the "*" in the Source Address field means any source.The PIM Join message can be use in PIM Sparse Mode (next subsection) to notify the Rendezvous Point (RP) that there is a host or a downstream router or Layer-3 switch that want to join a multicast group. When you finished configured the message, please clicking on **Send** button to send the message. This page can be used for sending Join/leave message for any mode of the PIM.

Figure 2.108 IGMP Join/Leave Web Page

2.10.4.3 Sparse Mode

PIM Sparse Mode (SM) uses the concept of **Rendezvous Point** (**RP**) as a meeting point for any routers or Layer-3 switches that will involve in multicasting as multicast source and receivers. The RP can be manually configured as **Static Rendezvous** or can be automatically discover in the network using some protocols such as **Bootstrap Rendezvous**. Each router or Layer-3 switch that receives multicast traffic from a source will forward it to the RP. Routers or Layer-3 switches in PIM SM will not forward any multicast traffic unless some node requests it. Each router or Layer-3 switch called**Designated Router** (**DR**)that would like to receive multicast traffic will have to send or forward a PIMJoin message to the RP.

PIM **Sparse Mode** (PIMSM) explicitly builds unidirectional root path tree (RPT) or shared distributed tree rooted at a Rendezvous Point (**RP**) per multicast group. PIMSM can optionally create shortest-path tree per source so that the router or Layer-3 switch can switch to Source Path Tree (SPT) or **Shortest-Path Tree** (SPT) which is the most optimal path. This switch operation can remove the RP from the shared distributed tree and get multicast traffic directly from the multicast source. Note that receivers that never switch to shortest-path tree are effectively running Core Based Trees (CBT).

PIMSM generally scales fairly well for wide-area usage. The RP helps reducethe amount of states in other non-RP routers or switches in the network. However, all routers or Layer-3 switches in PIMSM domain must provide mapping to a Rendezvous Point router/switch.

shows the menu and submenus for **PIM Sparse Mode** which consists of **Setting**, **Statistics**, **Restart** and **Rendezvous Point**.

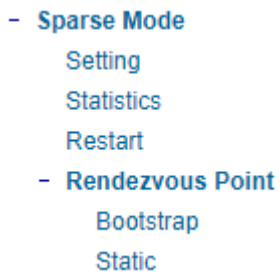


Figure 2.109 Menu and Submenus of PIM Sparse Mode

To enable PIM Sparse Mode on RHG96XX Layer-3 Managed Switch, you can click on the **Enable** button inside the **Running Status** box on the**Sparse Mode** submenu under **PIM**as shown inFigure 2.110.However, you will also need to set up PIM Spare Mode **Setting** such as PIM SM VLAN interfaces, hello interval, RP election, and STP switch-over mechanisms first as described in the next section (Section 2.10.4.3.1).

Figure 2.110 PIM Sparse Mode Running Status Web Page

Note that if you did not follow the steps described in Section2.10.2and Section 2.10.4.3.1before enabling PIM Sparse Mode here. You will be notified by error messages such as the IP routing is not enabled as shown in Figure 2.111or no PIM SM VLAN interface is configured as shown in Figure 2.112.

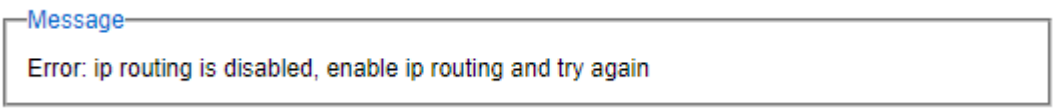


Figure 2.111 Error Message when IP Routing function is not enabled

Figure 2.112 Error Message when no Sparse-Mode VLAN was configured

2.10.4.3.1 Setting

PIM Sparse Mode (SM) configuration and its VLAN interface settings must be configured in this **Setting** web page before enabling it in previous section. **PIM SM Setting** web page is divided into three parts: **PIM SM Settings**, **PIM SM VLAN Settings**, and **Sparse Mode Settings** as shown in Figure 2.113.

The first part called **PIM SM Settings** contains three PIM SM options which are Rendezvous Point (**RP**) **Election**, Shortest-Path Tree (**SPT**) **switch-over**, and **Hello Interval**. In **RP Election** option, you can choose how the PIM SM choose an RP from either **Static Rendezvous** or **Bootstrap Rendesvous**. The **SPT switch-over**option can be configured as either **Never** or **Immediate**. If SPT switch-over is immediate, the Layer-3 managed switch will change to receive multicast traffic from the shortest path tree. The **Hello Interval** is the time between transmission of Hello message that allows Layer-3 managed switch to advertise their existence as PIM routing device on all PIM-enabled interface. This will allow neighboring PIM routers/switches to learn about it.The value of Hello Interval is between 30 to 18724 seconds. The default value of Hello Interval is 30 seconds.

The second part called **PIM SM VLAN Settings**is used to configure VLAN interface for PIM SM. Note that you will need to configure VLAN interface as described in Section 2.10.2 so that you can select that particular VLAN interface from the **VLAN**drop-down list in this part. For each PIM SM VLAN interface, you will have to configure Designated Router (**DR**) **Priority**, **Route Distance**, and **Route Metric**. By default, every PIM interface has an equal probabity (priority = 1) of being selected as the DR. Configuring the interface's DR Priority helps ensure that changing an IP address does not alter forwarding model.

The third part called **Sparse Mode Settings** is a table of all current PIM Sparse Mode interfaces. Inside this part, you can remove any of the VLAN interface entries by checking the box infront of that entry and clicking **Delete** button. To view the lastest list of PIM SM interfaces, simply clicking on the **Update** button. Description of parameters in PIM Sparse Mode Settings are summarized in Table 2.30.

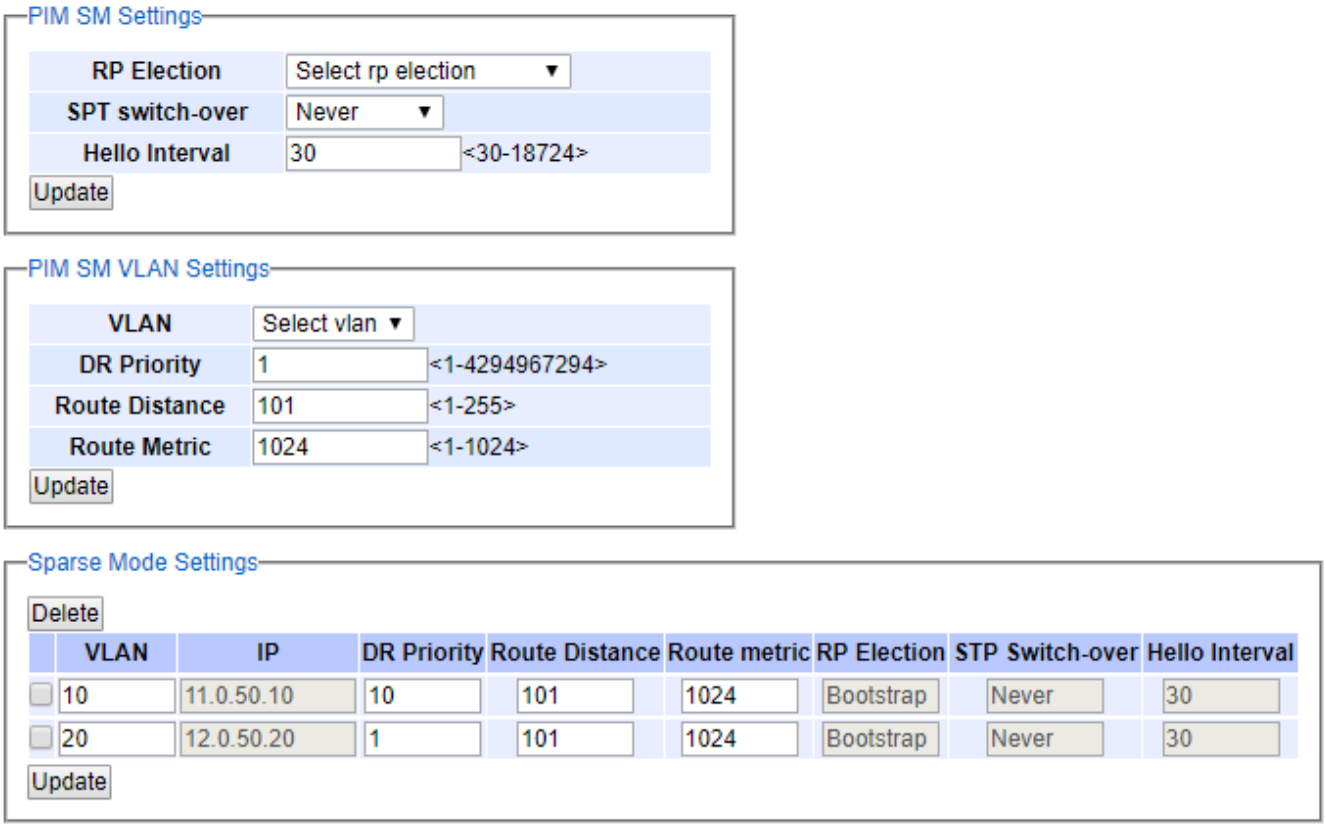


Figure 2.113 PIM Sparse Mode Setting Web Page

Table 2.30 Descriptions of PIM Sparse Mode Settings

Label	Description	Factory Default
RP Election	PIM SM Rendezvous Point election methods: Static or Bootstrap	-
SPT Switch-over	Shortest path switch-over is enabled/disabled	Enabled
Hello Interval	PIM Hello messages are sent periodically on each PIM-enabled interface. They allow a router to learn about neighboring PIM routers on each interface.	30 seconds
DR Priority	When there are multiple PIM routers on the same LAN the DR (Designated Router) is usually elected based on the highest numerical IP address. This setting can be used to control the DR Priority option in PIM Hello messages, When the DR Priority option is advertised by all PIM routers on the same LAN the highest priority router wins the DR election, regardless of its IP. If any router does not advertise the DR Priority option, or the same priority isadvertised by more than one router, the protocol falls back to using the IP address.	1
Route Metric	When there are multiple PIM enabled routers on a shared segment, it is possible that these routers encounter duplicate multicast traffic. PIM assert messages which are triggered when you receive a multicast packet on the Outgoing Interface List (OIL). These assert messages contain metrics which are then used to calculate who will become assert winner. When comparing assert_metrics, the rpt_bit_flag, metric_preference,and routemetric fields are compared in order, where the first lowervalue wins. If all fields are equal, the primary IP address of therouter that sourced the Assert message is used as a tie-breaker, withthe highest IP address winning.	1
Route Distance	The default route distance option has nothing to do with system default route, itis rather the default value for unicast routing protocol's administrative distance. It is used in PIM assert election to determine upstream router .	1

2.10.4.3.2 Statistics

This web page as shown in Figure 2.114provides information related to PIM Sparse Mode such as **Neighbor Table**, **Multicast Routing Table** and **Local Candidate Rendezvous Point Set**. The **Neighbor Table** will contain entries of VLANs, IP Addresses, and Neighbor IP Addresses which the Layer-3 Managed Switched learned from its neighbor's Hello message. The **Multicast Routing Table** summarizes the total number of multicast group based on **Group**'s IP Address and displays the Rendezvous Point (**RP**) **Address, Source**, and the state of multicast routing (which is represented by **(*,*)** notion. Note that Source is the address of node that sends multicast traffic to a multicast group. Also note that the state of multicast routing can be:

- (S,G) pronounced as "S comma G" which is the multicast routing table state for a shortest path tree rooted at the source. The incoming interface for this entry is the reverse path forwarding (RPF) interface to S. There is a (S,G) for each source sending to each group.
- (S,*) pronounced as "S comma star" which is a multicast routing table state for each source sending to any group. The incoming interface for this entry is the RPF interface to S.
- (*,G) pronounced as "star comma G" which is the multicast routing table state for the RP tree. The incoming interface for this entry is the RPF interface to the RP for sparse-mode groups. There is one (*,G) for each group.

The **Local Candidate Rendezvous Point Set** is a table that lists all known RP addresses in the network connected to Layer-3 Managed Switch. However, at the top of this table there is the current Bootstrap Router (BSR) IP address. Each entry in the table (each RP) will have information about **Incoming,** RP**Group** Address, RP **Priority**, and **Hold Time**.

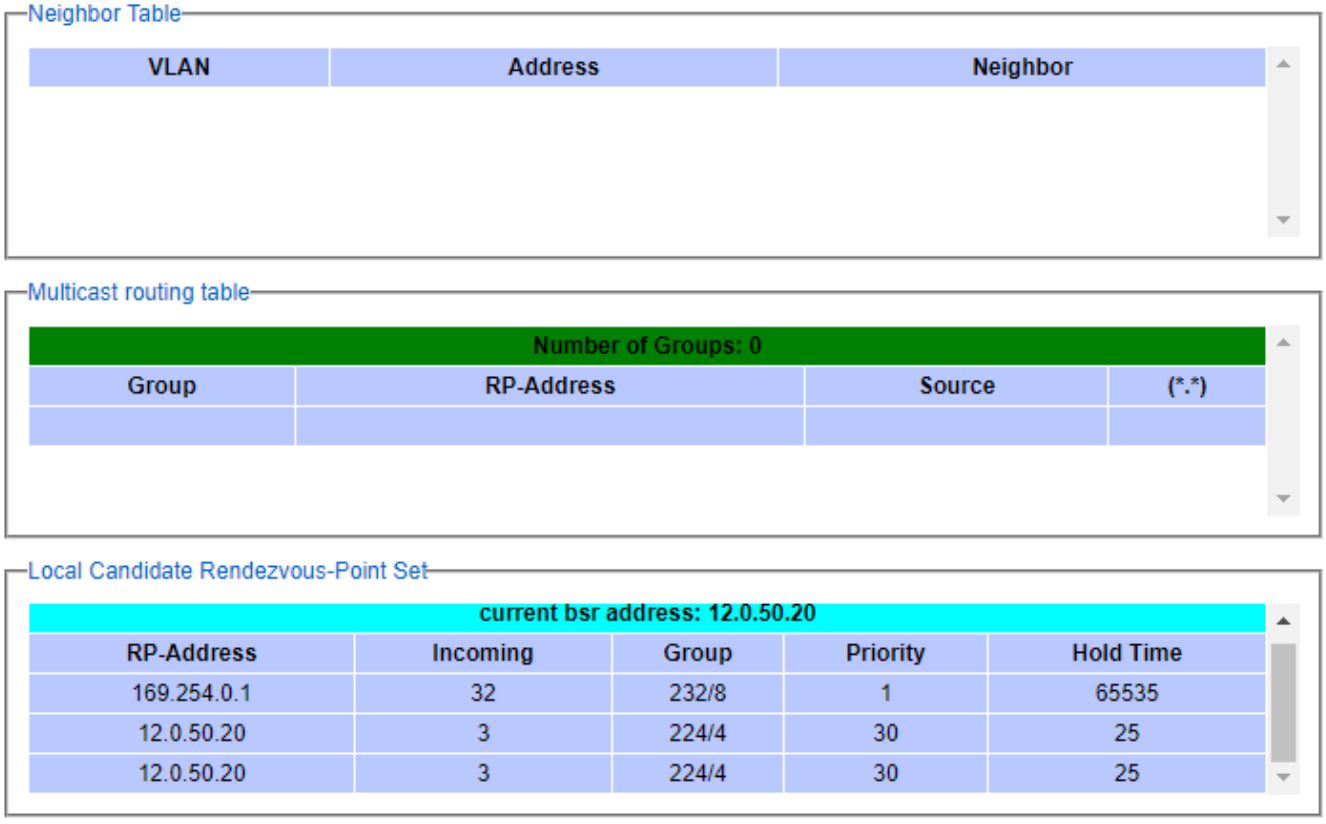


Figure 2.114 PIM Sparse Mode Statistics Web Page

Note that if the PIM Sparse Mode was not enabled as described in previous sections, you will be informed by an error message as shown in Figure 2.115.

Figure 2.115 Error Message when PIM Sparse Mode was not enabled

2.10.4.3.3 Restart

Figure 2.116 shows the **PIM Sparse Mode Restart** submenu that allows you to restart the PIM SM process inside the RHG96XX Layer-3 Managed Switch by simply clicking on the **Restart** button.

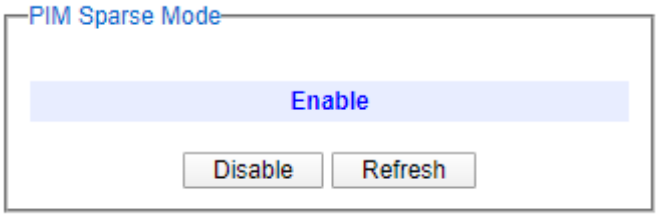


Figure 2.116 PIM Sparse Mode Restart Web Page

2.10.4.3.4 Rendezvous Point

RHG96XX Layer-3 Manage Switch currently supports two methods for Rendezvous Point (RP) setup for PIM Sparse Mode which are bootstrapping (**Bootstrap**) and**Static**. Note that RP is a router or switch that is a meeting point for multicast groups that operate in sparse mode. There could be more than one RP per multicast group and a router could be the RP for multiple multicast groups.

2.10.4.3.5 Bootstrap

RHG96XX Layer-3 Manage Switch can utilize Bootstrap Router (BSR) protocol for automatic Rendezvous Point (RP) selection. This is according to the **RP Election** option that is set to **Bootstrap Rendesvous**as described in Section 2.10.4.3.1. You can configure anyone of its VLAN interface to become the candidate for**Bootstrap Router** (C-BSR) by selecting the desired VLAN from the drop-down list as shown in **Rendezvous Point Bootstrap Settings** box of Figure 2.117. Each candidate **BSR** will advertise its **BSR Priority**, **IP Address**, and hash value to its neighbor. A candidate BSR that hears a higher-priority candidate BSR than itself then suppresses its sending of further BSR messages for some time.

The single remaining candidate BSR in the network then becomes the elected BSR and its BSR messages inform all the other routers in the domain that it is the elected BSR. To avoid BSR message looping in the network, when Layer-3 switch received BSR message on one interface (Reverse Path Forwarding), it will not accept the same BSR message from other interfaces (non-Reverse Path Forwarding). Additionally, BSR message with lower priority will be dropped. The **BSR Prioirty** can be set with value from 0 to 255. Default **BSR Priority** is 0.

CandidateRP routers or Layer-3 switches in the network will start sending unicast RP advertisement with their list of multicast groups to the elected BSR. Note that BSR is not responsible for electing the best RP for each multicast group. However, BSR will advertise the received information about RPs and corresponding multicast groups to all PIM routers/layer-3 switches. Other PIM routers/layer-3 switches in the network will choose appropriate RP for each group.

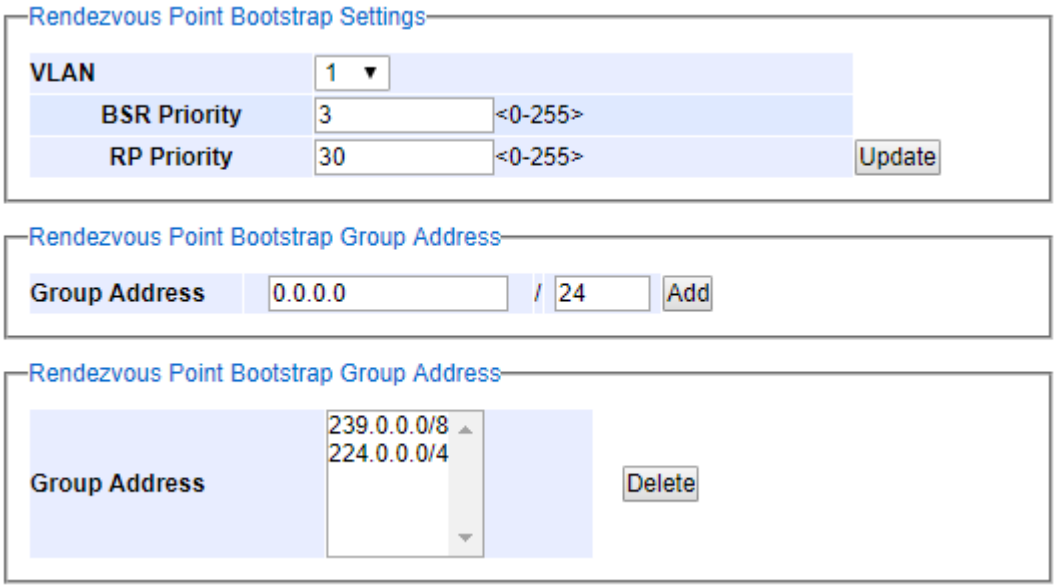


Figure 2.117 Rendezvous Point Bootstrap Settings Web Page

On the same page, you can also configure the same VLAN (selected as BSR above)as a Rendezvous Point (RP) by setting the **RP Priority** inside the **Rendezvous Point Bootstrap Settings** as shown in Figure 2.117. The **RP Priority** can be set with value from 0 to 255. Default **RP Priority** is 0. Once configuring all information, clicking on **Update** button.The next two parts on this page are dedicated to adding and removing multicast Group Addresses to the candidate BSR or candidate RP. To add a **Group Address**, you can enter the multicast IP address and its number of subnet mask bits then click on the **Add** button. Note that multiple Group Addresses can be add to the same BSR and RP. The Layer-3 switch will start advertising itself as the RP for multicast groups. To remove a **Group Address** from the list, you can select it from the list in Figure 2.117 and then click on the **Delete** button.

2.10.4.3.6 Static

This **Static** web page under the **Rendezvous Point**menu allows you to configure one or multiple static RPs. You can fill in the **RP Static Address** and its corresponding multicast **Group Address**as shown inFigure 2.118. Then clicking on the **Add** button to add a new entry into the list or table in the **Rendezvous Point Static Settings** box. To remove any existing static RP from the list, you can check the box infront of that particular entry and then clicking on the **Delete** button.

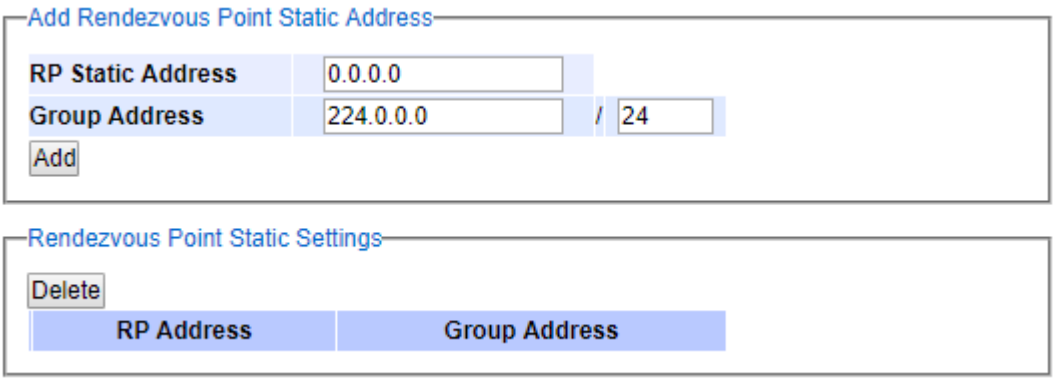


Figure 2.118 Rendezvous Point Static Setting Web Page

2.10.4.4 SSM

PIM SourceSpecific Mode(**SSM**) uses a subset of PIM Sparse Mode and IGMP version 3 (IGMPv3). It allows a client to receive multicast traffic directly from a source which is more secure and scalable. PIM SSM only supports the one-to-many multicasting model. Thus, it is simpler than the PIM Sparse Mode. It is suitable for most broadcasting of content such as Internet video applications. An SSM group, called a channel, is identified as (S,G) where S is the source address and G is the group address. The IPv4 address range reserved for mulitcast group of SSM is 232.0.0.0/8 but it can technically be used in the entire 224/4 multicast address range.

PIM SSM builds shortestpath trees (SPTs) rooted at the source immediately after receivers issued join message (or subscribing message) toward the source. It bypasses the procedures of Rendezvous Point (RP) connection as used in PIM SM and goes directly to the source-based distribution tree. Since PIM SSM does not rely on RP mechanism, it may require manual configuration or external method to learn in advance about the address of multicast source(s). In RHG96XX Layer-3 Managed Switch, you will need to know the **Source Address** and enter it in the **IGMP join/leave** message as described in Section2.10.4.2.

Figure 2.119 shows the menu and submenus for **PIM SSM** which consists of **Setting**, **Restart** and **Statistics**.

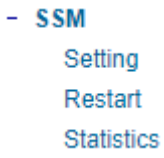


Figure 2.119 Menu and Submenus of PIM SSM

To enable PIM Source Specific Mode (SSM) on RHG96XX Layer-3 Managed Switch, you can click on the **Enable** button inside the **Running Status** box on the **SSM** submenu under **PIM** as shown in Figure 2.120. However, you will need to prepare a VLAN interface as described in Section 2.10.2 (PIM) and also need to setup parameters for PIM Source Specific Mode VLAN in the **SSM Setting** page as explained in the next section. At least one SSM VLAN must be configured before enabling the PIM SSM.

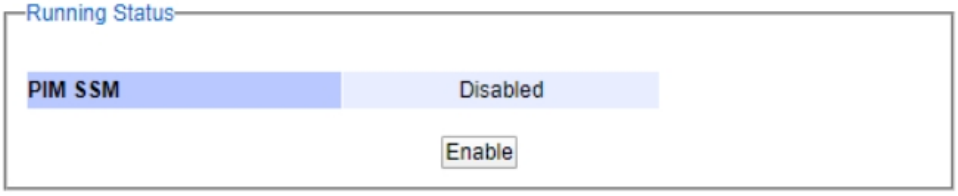


Figure 2.120 PIM Source Specific Mode Running Status Web Page

Note that if you did not follow the steps described in Section 2.10.2 (PIM) and Section 2.10.4.4.1 (SSM Setting) before enabling PIM Source Specific Mode here. You will be notified by error messages such as no SSM VLAN interface is configured as shown in Figure 2.121.

Figure 2.121 Error Message when no PIM SSM VLAN was configured

2.10.4.4.1 Setting

Before enabling the PIM Source Specific Mode in the previous subsection, you must configure PIM SSM's parameters and VLAN interface under the**PIM SSM Setting**web page as shown in Figure 2.122. There are four sections on this web page which are **PIM SSM Settings**, **PIM SSM Group Settings**, **PIM SSM VLAN Settings** and **SSM Settings**. The first section called **PIM SSM Settings**contains the **Hello Interval** which can be set from 30 to 18724

seconds. The default value for **Hello Interval** is 30 seconds. If you change the **Hello Interval** value, do not forget to click the **Update** button.
The second section called **PIM SSM Group Settings**is where you can specify the**Source Group Address** or the multicast group address and the number of bits for subnet mask. You can click the **Add** button to add this address to the **PIM SSM Group** or click the **Delete** button to remove it. The third section called **PIM SSM VLAN Setttings** is where you configure a VLAN interface for the PIM SSM. Here you first select a VLAN ID from the drop-down list and then set the Designated Router (**DR**) **Priority, Route Distance** and **Route Metric**. Clicking on the Update button once all the parameters are set.

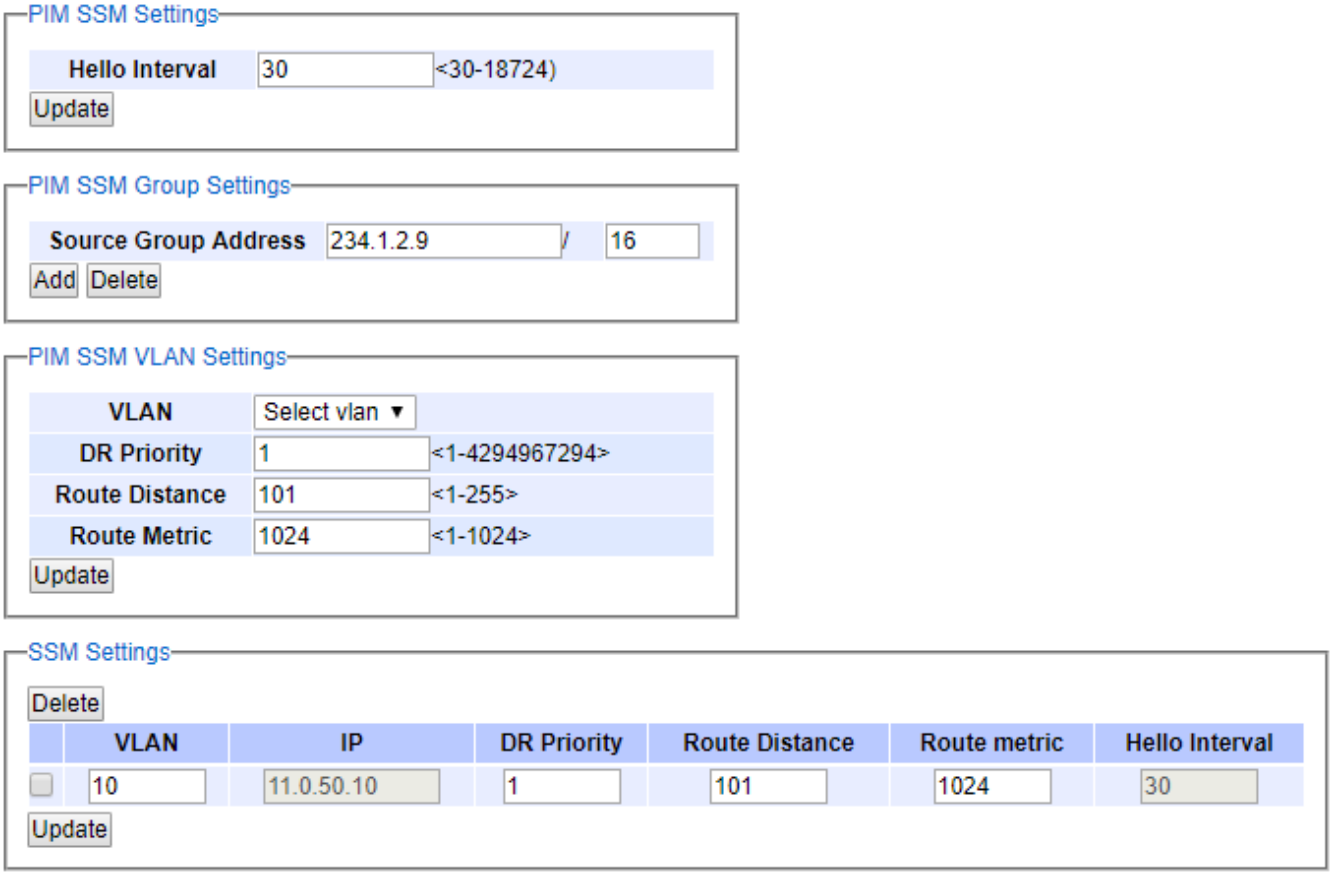


Figure 2.122 PIM Source Specific Mode (SSM) Setting Web Page

The last section is the list of configured PIM SSM VLAN interfaces. Figure 2.122 shows an example of SSM VLAN interface inside the **SSM Settings**box. If you want to remove an SSM VLANinterface, checking the box infront of that VLAN ID entry and then clicking on the **Delete** button. Clicking on the **Update** button to refresh the list.

2.10.4.4.2 Restart

Figure 2.123shows the **PIM SSM Restart**web page that allows you to restart the PIM Source Specific Mode process inside the RHG96XX Layer-3 Managed Switch by simply clicking on the **Restart** button.

Figure 2.123 PIM Source Specific Mode Restart Web Page

Once you restarted the PIM SSM process, you can then manually send an IGMP Joint message out to subscribe a known SSM multicast group or send anIGMP Leave message to unsubscribe SSM multicast group. Figure 2.124 shows an example of **IGMP join/leave** web page in which a IGMP Join Message is prepared to be sent with Source Address = 10.0.60.70 and Group Address = 232.4.4.4 with VLAN ID = 1.

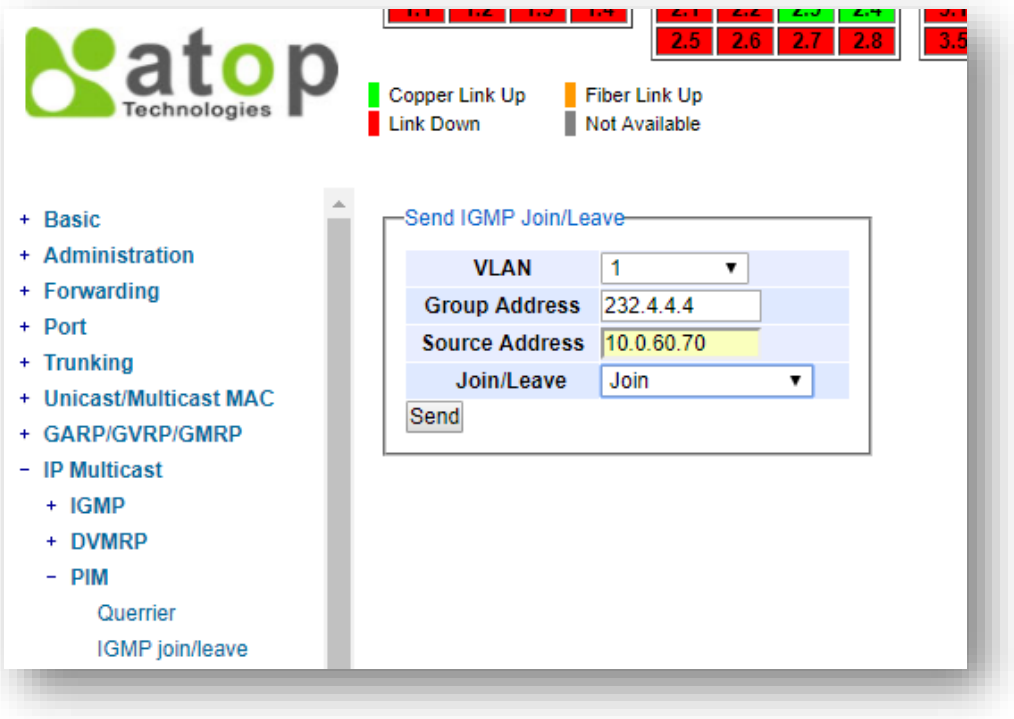


Figure 2.124 Example of Sending IGMP Join to an SSM Source Address

2.10.4.4.3 Statistics

Under SSM's**Statistics** web page as shown inFigure 2.125, you can check the current PIM SSM's **Neighbor Table** and **Multicast routing table** on the RHG96XX Layer-3 Managed Switch.The **Neighbor Table** will list the **Neighbor**'s IP address that can be discovered through each SSM **VLAN** Interface and its corresponding VLAN's IP **Address**. Inside the **Multicast routing table**, you can see the **number of** SSM **Groups** and the list of Groups which has three columns: **Group** address, **Source** address and the state of the multicast routing with notation "(*.*)".Note that (S,G) pronounced as "S comma G" which is a multicast routing table state for a source sending to a group. The incoming interface for this entry is the RPF interface to S.

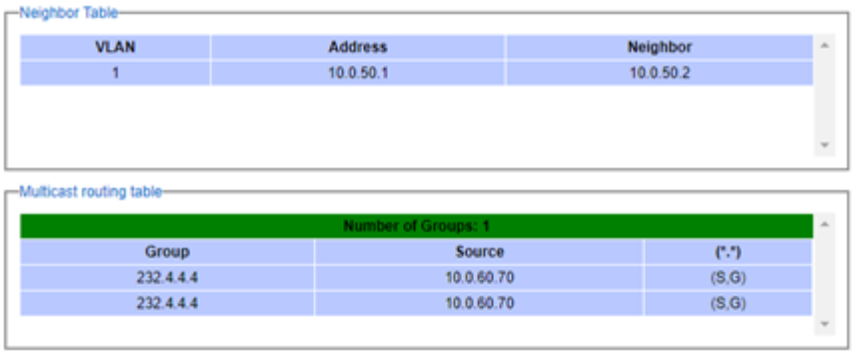


Figure 2.125 PIM Source Specific Mode (SSM) Statistics Web Page

Note that if the PIM SSM was not enabled and configured propertly, when you click on the SSM's **Statistics** web page, you will be notified with the error message as shown in Figure 2.126.

Figure 2.126 Error Message on Statistics web page when PIM SSM was not enabled

2.10.4.5 Dense Mode

PIM Dense Mode (PIM DM) is a multicast routing protocol which is designed under the assumption that the receivers for any multicast group are distributed densely throughout the network. Its assumption is opposite to the PIM Sparse Mode.As a PIM protocol, PIM DM utilizes unitcast routing tables built by other routing protocol. PIM DM control message processing and data packet forwarding is integrated with PIM SM operations such that a single router or Layer-3 switch can run different PIM modes for different multicast groups.

Multicast packet is initially sent to all hosts in the network.PIM DM relies on Reverse Path Multicasting (RPM)in which multicast packet is forwarded if the receiving interface is the one used to forward unicast packets to the source of the packet. If not, the packet is dropped. This mechanism prevents forwarding loops from occurring. The multicast packet is then forwarded out on all other interfaces. PIM Dense Mode uses explicit trigger grafts/prunes to manage its source-based acyclic tree. Routers that do not have any interested hosts then send PIM Prune messages to remove themselves from the tree. Note that graftsare messages sent towards known sources and used by new members to add themselves onto an existing distribution tree. Prunes are messages sent toward a source by a router when it wants to leave the distribution tree.

A node in PIM DM such as RHG96XX will create a multicast forwarding entry for a particular source-rooted distribution tree when a data packet from that source to the group first arrives. PIM DM only uses source-based trees. As a result, it does not use Rendezvous Points (RPs), which makes it simpler than PIM SM to implement and deploy. It is an efficient protocol when most receivers are interested in the multicast data but it does not scale well across larger domains in which most receivers are not interested in the data.

Figure 2.127 shows the menu and submenus for **PIM Dense Mode** which consists of **Setting**, **Restart** and **Statistics**.

Figure 2.127 PIM Dense Mode Menus

To enable PIM Dense Mode on RHG96XX Layer-3 Managed Switch, you can click on the **Dense Mode** submenu under **PIM** as shown in Figure 2.128. Then inside the **Running Status** box, clicking on the **Enable** button. However, you will also need to set up VLAN Interface as described in Section 2.10.2 and perform PIM Dense Mode **Setting** such as PIM DM VLAN interfaces, route preference and route metric first as described in the next section (Section 2.10.4.5.1).

Figure 2.128 PIM Dense Mode's Running Status Web Page

If the IP routing was not enabled, the PIM Dense Mode cannot be enabled as shown in Figure 2.129. To enable the IP routing, you can enable this function in Section 2.21.1. If you did not configure PIM Dense Mode VLANs, you will be notified with the error message as shown in Figure 2.130.

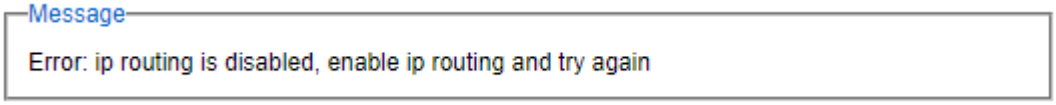


Figure 2.129 Error Message when IP Routing is Disabled

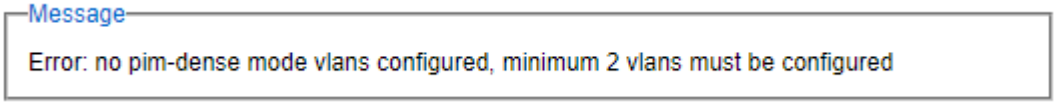


Figure 2.130 Error Message when It has insufficient configured VLANs

2.10.4.5.1 Setting

This **PIM DM Setting** web page as shown inFigure 2.131is used to configure VLAN interface for PIM DM. This setting has to be done before enabling the PIM DM in the previous section. Inside the upper part (**PIM DM Settings** box), you first select **VLAN** ID from the drop-down list and enter the **Route Preference** and the**Route Metric**. Note that the **Route Preference** is used by assert elections to determine upstream routers.**Route Reference** can be configured with the value from 1 to 255 and the default value is 101. The **Route Metric** is thecost of the path through which the packet is to be sent. The Route Metric can be selected with the value from 1 to 1024 and the default value is 1024. After finished configuring an VLAN interface for PIM DM, you should click on the **Add VLAN** button. The configured interface will be listed in the lower part of the page. You can remove a VLAN interface for PIM DM from the list by checking the box infront of that VLAN entry and clicking on **Delete** button. To obtain the lastest status of the PIM DM Settings, you can click on the **Update** button.

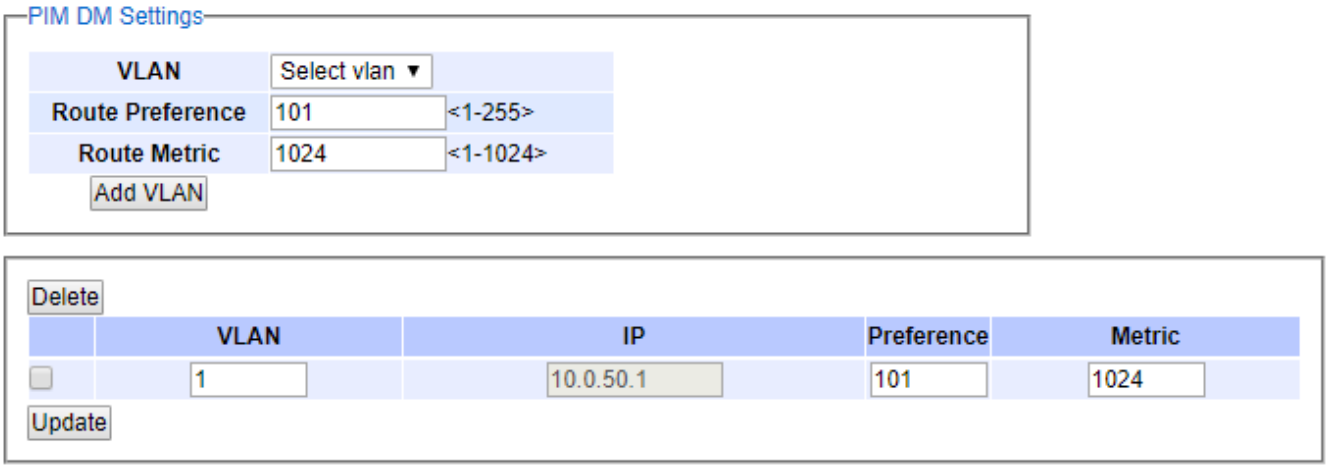


Figure 2.131 PIM Dense Mode Settings Web Page

2.10.4.5.2 Restart

Figure 2.132shows the **PIM Dense Mode Restart** web page that allows you to restart the PIM Dense Mode process inside the RHG96XX Layer-3 Managed Switch by simply clicking on the **Restart** button.

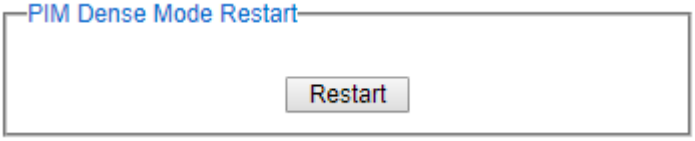


Figure 2.132 PIM Dense Mode Restart Web Page

2.10.4.5.3 Statistics

Under Dense Mode's **Statistics** web page as shown inFigure 2.133, you can check the current PIM Dense Mode's **Neighbor Table** and **Multicast routing table** on the RHG96XX Layer-3 Managed Switch. The **Neighbor Table** will list the **Neighbor**'s IP address that can be discovered through each PIM DM**VLAN**'s IP **Address**. Inside the **Multicast routing table**, you can see the **number of** PIMDense Mode **Groups** and the list of Groups which has two columns: **Source**address and **Group** address.

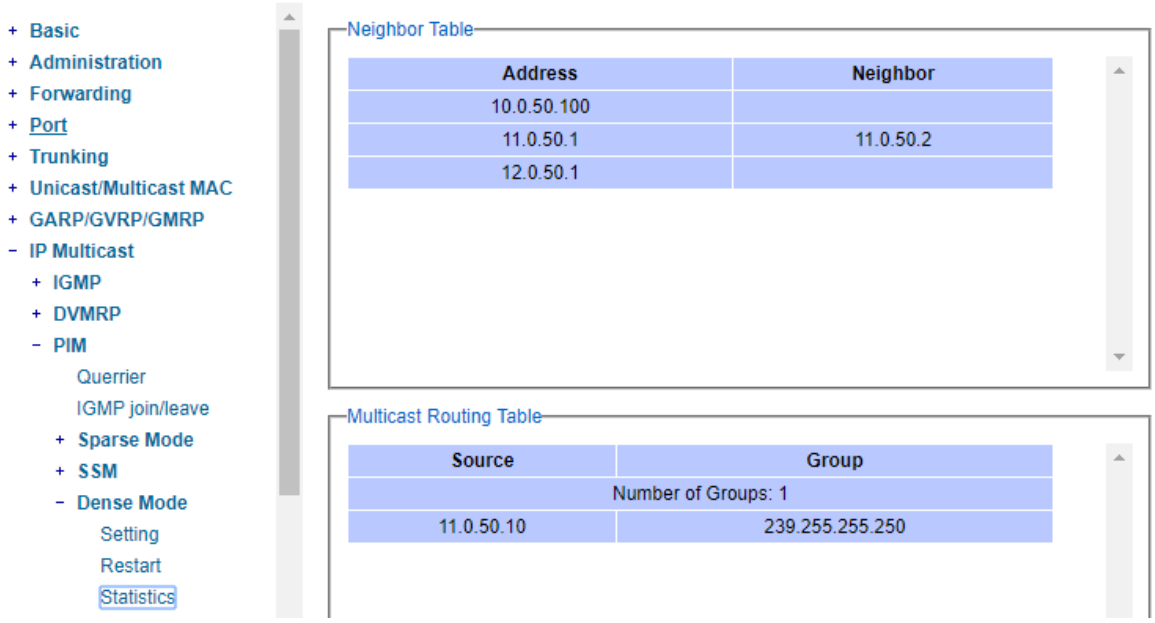


Figure 2.133 PIM Dense Mode Statistics Web Page

Note that if the PIM Dense Mode was not enabled and configured propertly, when you clicked on the Dense Mode's **Statistics** web page, you will be notified with the error message as shown in Figure 2.134.

Figure 2.134 Error Message when PIM Dense Mode is not enabled.

2.10.5 Static IP Multicast

This subsection allows the users to manually add new or remove existing static IP multicast and the joined port(s).Figure 2.135shows the Static IP Multicast webpage where the upper part of the page is a table of existing IP Multicast Address entries and the lower part of the page contains the fields for adding new IP Multicast Address entry to the table. The users are required to supply the IP Multicast Address, VLAN ID(**VID**), and the lists of the port numbers which will join the static IP multicasting group(joined port).

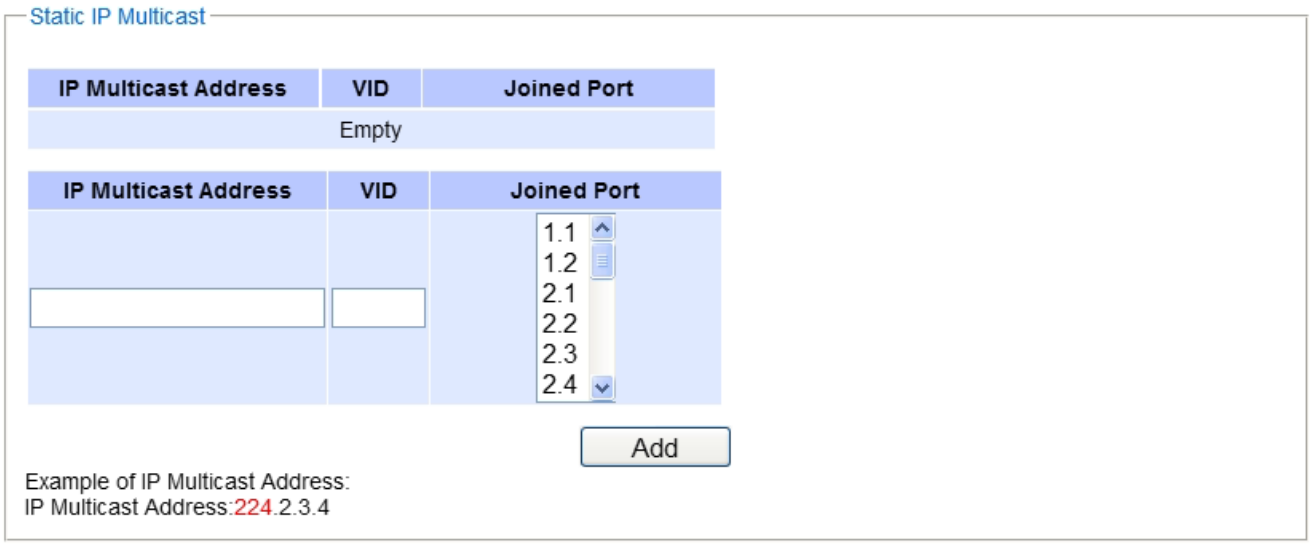


Figure 2.135 Static IP Multicast Setting Webpage

An example of an entry of IP multicast group is shown in Figure 2.136where there is an existing IP Multicast Address of 224.2.3.4 which belongs to VLAN 1 and has port number 2, 3, and 6 in the group. The following procedures outline how to add a new IP multicast group. For example, an IP multicast group address is224.1.1.1 and the joining ports are Port1, Port2 and Port5 with VLAN=1.

- First, the users should enter the IP=224.1.1.1 in the **IP Multicast Address** column.
- Then, the users should enter the VLAN ID =1 in the VLAN ID(**VID**) column.
- Then,while holding the "Ctrl"key on the keyboard, click on all corresponding port numbers under the Join Port column(Port1, Port2, and Port5 in this example)to select which port(s)will join in the IP multicast group.
- Finally, click on the Add button.The IP address is then added as it shows onFigure 2.136.
- To remove an existing static IP multicast addressfrom the table, click the Remove buttonof that entry.

These procedures are similar to the procedures for adding or removing the Unicast/Multicast MAC address explained in Section 2.8.1. The only difference is that the IP multicast address has the form of 224.XX.XX.XX. Note that IPv4 multicast address (Class D) is in between 224.0.0.0 and 239.255.255.255.

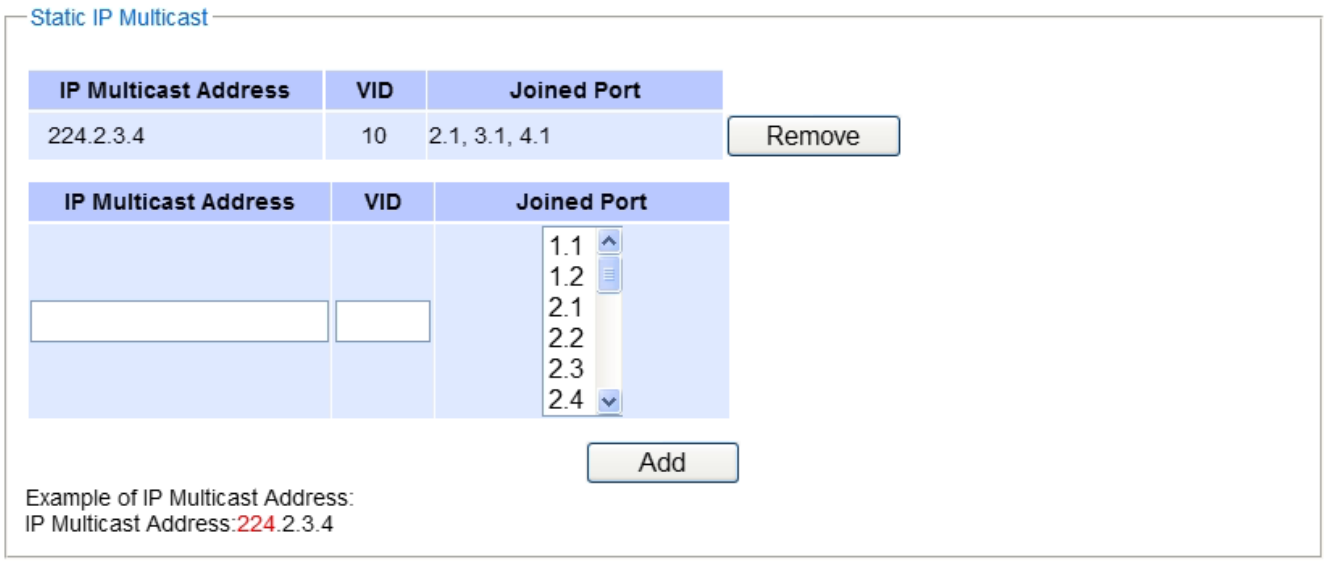


Figure 2.136Example of Static IP Multicast Setting

2.11 SNMP

Simple Network Management Protocol(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. TheSNMP settinghas four categoriesand its dropdown menu is shown inFigure 2.137, which are:

- SNMP Agent
- SNMP V1/V2c Community Setting
- Trap Setting
- SNMP V3 Authentication (Auth.)Setting

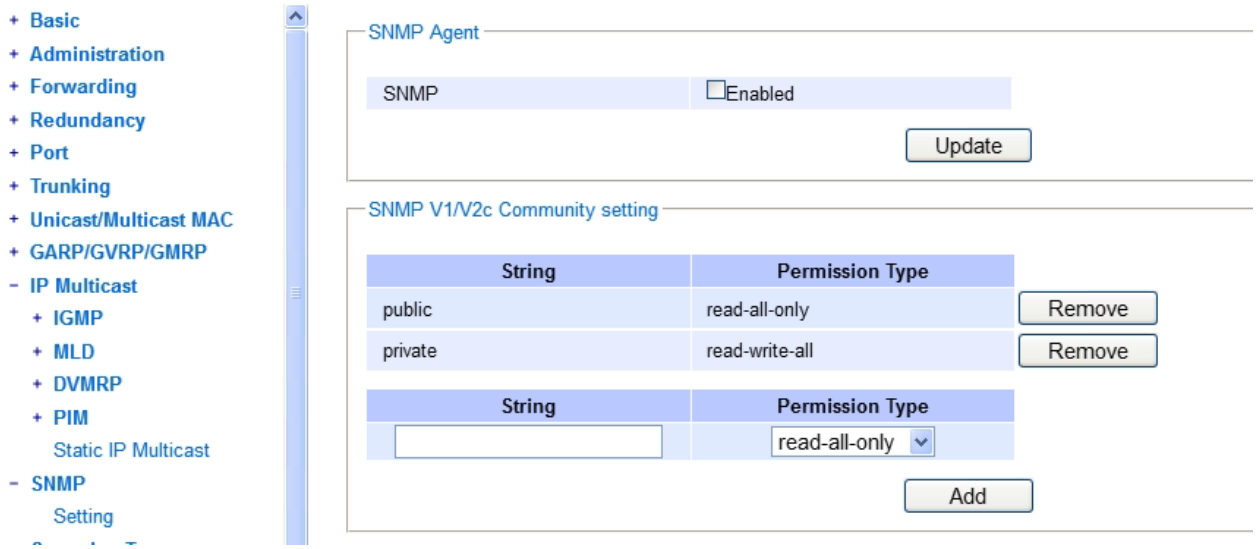


Figure 2.137 SNMP Dropdown Menu

2.11.1 SNMP Agent

To enable SNMP agent on the managed switch, please check the **Enabled** box and click **Update** button as shown in Figure 2.138.The SNMP version 1(V1), version 2c (V2c)and version 3 are supported by Atop's managed switches as summarized in Table 2.31. Basically, SNMPV1 and SNMP V2c have simple community string-based authentication protocol for their security mechanism, while SNMP V3 is improved with cryptographic security.

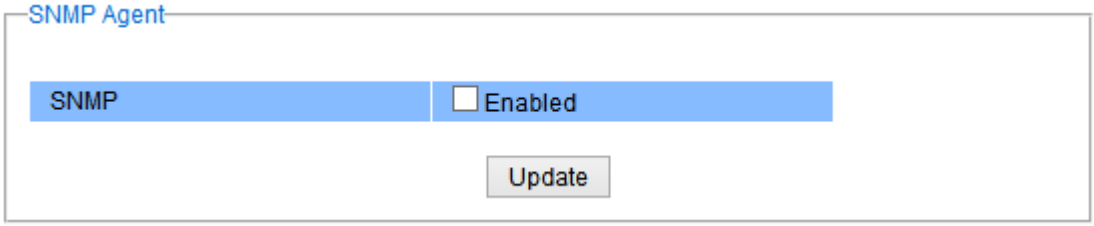


Figure 2.138 SNMP Enabling Box

Table 2.31Description of SNMP Setting

Label	Description	Factory Default
SNMP	Checkthe box to enable SNMP V1/V2c/V3.	Disabled

2.11.2 SNMP V1/V2c Community Setting

The managed switchsupports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string matching for authentication.This authentication will allow network management software to access the information or data objects defined by Management Information Bases(MIBs) on the managed switch.Note that this simple authentication is considered a weak security mechanism. It is recommended to use SNMP V3, if possible. There are two levels of authentications or permission type in RHG96XX series, which are read-all-only or read-write-all. For example, in our default setting as shown in Figure 2.139,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.

This community string option allows the users to set a community string for authentication or remove existing community string from the list by clicking on the **Remove** button at the end of each community string item. The users can specify the string names on the **String** field and the type of permissions from the dropdown list as shown inFigure 2.139. Table 2.32briefly provides descriptions of SNMP's community string setting.

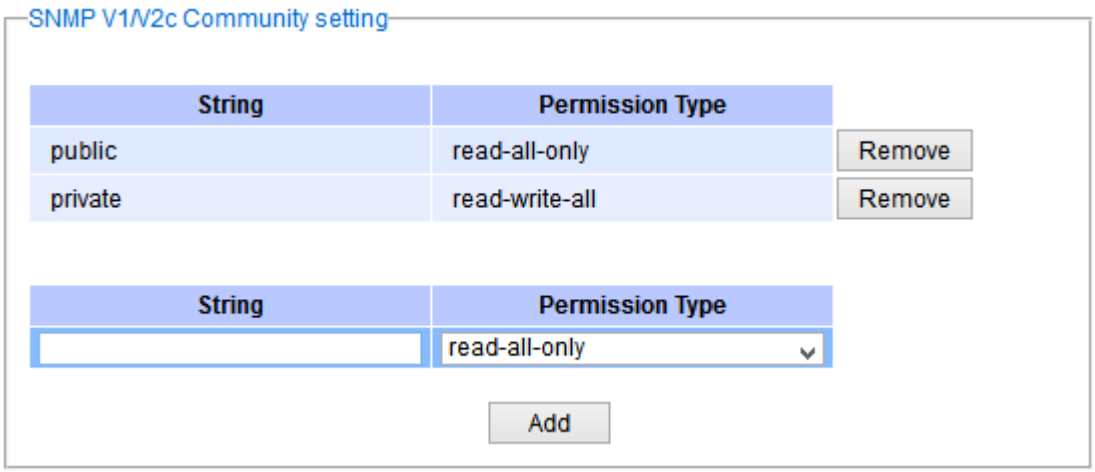


Figure 2.139 SNMP Community Strings

Table 2.32Descriptions of Community String Settings

Label	Description	Factory Default
(Community) Strings	Define name of stringsfor authentication. Max. 15 Characters	**Public**(read-all-only) **Private**(read-write-all)
Permission Type	Choose a type from the dropdown list:read-all-only and read-write-all. See notes below for a briefed explanation.	-

***NOTE:**
Read-all-only:permission to read OID 1 Sub Tree.
Read-write-all:permission to read/write OID 1 Sub Tree.

2.11.3 Trap Setting

The managed switchprovides 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 could 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 optionallows users to configure SNMP Trap Setting by setting the destination IP Address of the Trap server, Port Number of the Trap server, and Community String for authentication. Figure 2.140shows these Tap Setting's options. The first line enables the users to select the Trap Mode which can be either **Trap** or **Inform**. Please click on the **Update** button after selecting

the desired Trap Mode. After entering all required fields for Trap Setting in the last line, please click on the **Add** button. Table 2.33summarizes the descriptions of trap receiver settings.

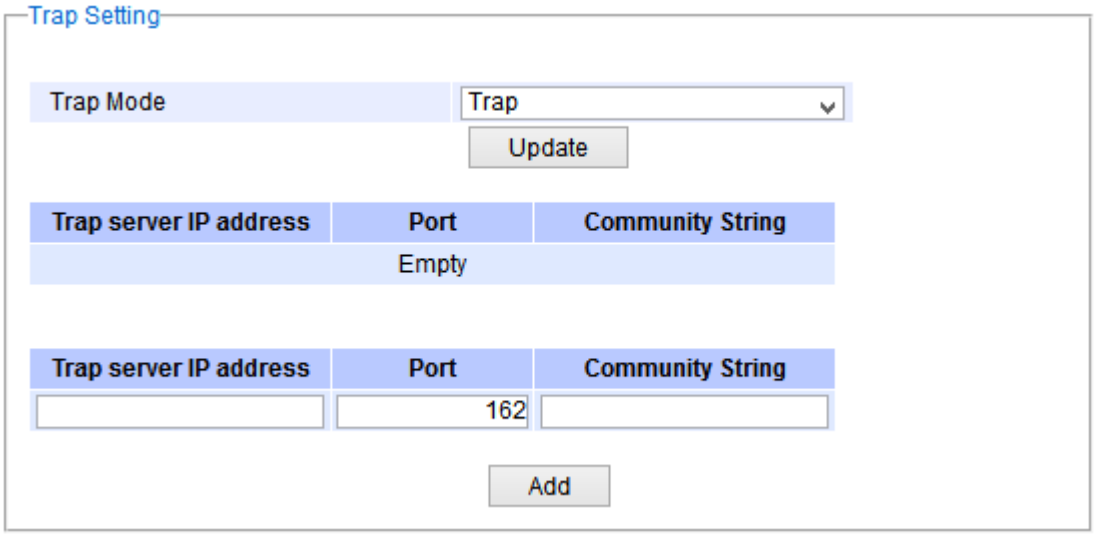


Figure 2.140Example of Trap Receiver Setting

Table 2.33Descriptions of Trap Receiver Settings

Label	Description	Factory Default
Trap Mode	Choose between Trap and Inform	Trap
Trap server IP address	Enter the IP address of your Trap Server.	NULL
Port	Enter the trap Server service port.	162
Community String	Enter the community string for authentication. Max.15 characters.	NULL

2.11.4 SNMPv3 Auth. Setting

As mentioned earlier, SNMP V3 is a more secure SNMP protocol. 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 SNMP V3'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 2.141shows the SNMP V3 Authentication Setting'options. The users can view existing SNMP V3 users' setting on the upper table where it provides information about user name, authentication type, and data encryption. The users have an option to remove existing SNMP V3 user by clicking on the **Remove** button in the last column of each entry. To add a new SNMP V3 user, the users have to select the user **Name** from the dropdown list which can be either **Admin** or **User**. Then, the authentication password with a maximum length of 31 characters has to be entered in the **Auth. Password** field and re-entered again in the **Confirmed Password** field. Note that if no password is provided, there will be no authentication for SNMP V3. Finally, the encryption key with a maximum length of 31 characters can be enteredin the **Encryption Key** and re-entered again in **Confirmed Key** field. After filling all the required fields, please click on **Add** button to update the information on the managed switch. Table 2.34lists the descriptions of SNMP V3 settings.

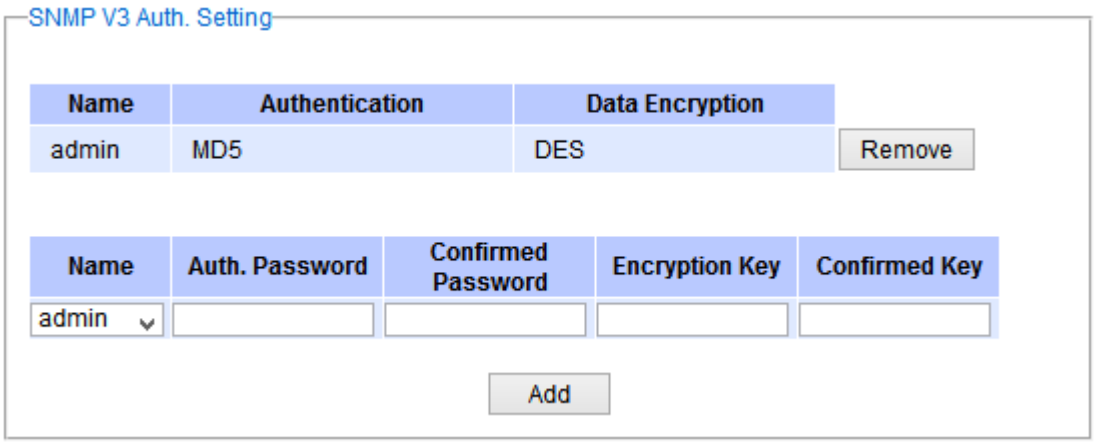


Figure 2.141 SNMPv3 Users' Options

Table 2.34Descriptions of SNMP V3 Settings

Label	Description	Factory Default
Name	Choose from one of the following options: **Admin**:Administration level. **User**:Normal user level.	Admin
Auth. (Authentication) Password	Set an authentication password for the user name specified above. If the field is left blank, there will be no authentication. Note that the authentication password is based on MD5. Max. 31 characters.	NULL
Confirmed Password	Re-type the Authentication Password to confirm.	NULL
Encryption Key	Set encryption key for more secure protection of SNMPcommunication. Note that the encryption algorithm is based on DES. Max. 31 characters.	NULL
Confirmed Key	Re-type the Encryption Key	NULL

2.12 Spanning Tree

IEEE 802.1DStandard spanning tree functionality is supportedby Atop's managed switches. The **S**panning **T**ree **P**rotocol (**STP**)provides afunction to prevent switching loops and broadcast radiationat the OSI layer 2. A switching loopoccurs 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 createa broadcast radiation, which is the accumulation of broadcast and multicast trafficsin 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 arenot part of the spanning tree, which leaves only a single active path between two nodes. This function canavoid 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 (**R**apid**S**panning **T**ree **P**rotocol), IEEE 802.1W,is also supportedin 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(**M**ultiple **S**panning **T**ree**P**rotocol) 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.

This section describes how to setup the spanning tree protocol (STP), rapid spanning tree protocol(RSTP), and Multiple Spanning Tree Protocol (MSTP). Figure 2.142depicts the dropdown menu for Spanning Tree.

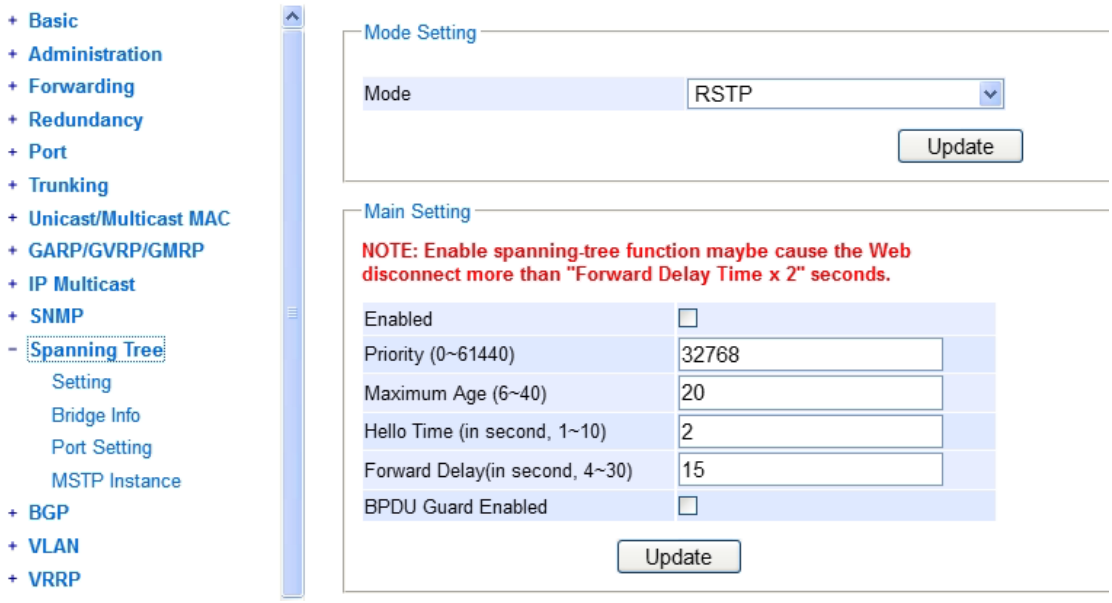


Figure 2.142 Spanning Tree Dropdown Menu

2.12.1 Spanning Tree Setting

The users can select the spanning tree mode which are based on different spanning tree protocols in this webpage. Figure 2.143shows the mode setting for spanning tree. There are three spanning tree modes to choose from the dropdown menu, which are spanning tree protocol (STP), rapid spanning tree protocol(RSTP), and multiple spanning tree protocol (MSTP). After choosing the desired mode, please click **Update**button to allow the change to take effect.

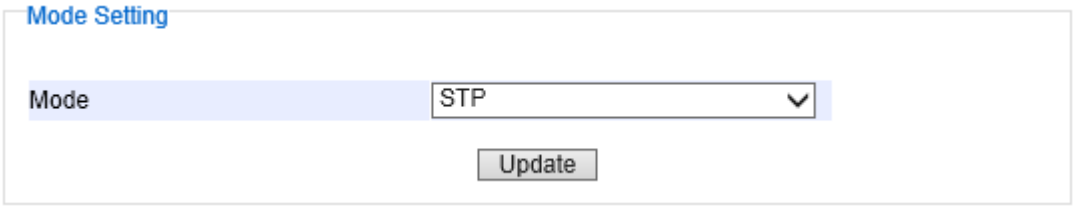


Figure 2.143 Spanning Tree Mode Setting

Under the mode setting, there is a box for Main Setting of spanning tree's parameters as showed inFigure 2.144.The users can enable or disable spanning tree protocol in the**Main Setting** by checking the box behind the **Enabled** option. The users can fine tune the **Priority**, **Maximum Age**, **Hello Time**, and**Forward Delay**. Also you may enable **BPDU Guard Enabled** option.After configuring the spanning tree's main parameters, please click **Update**button to allow the change to take effect. The description of each parameter is listed inTable 2.35.

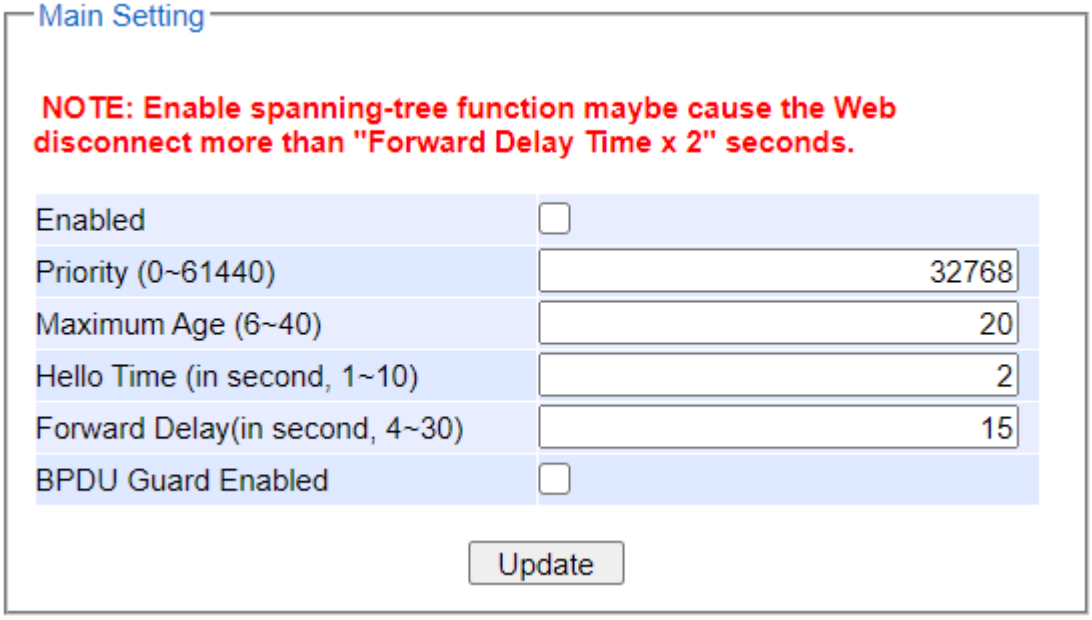


Figure 2.144 Spanning Tree Main Setting for STP and RSTP

When the users change the spanning tree mode setting to **MSTP** and click the **Update**button in the **Mode Setting** box Figure 2.143, the **Main Setting** box in Figure 2.144will be changed to Figure 2.145. The user can notice that the **Priority** field is disappeared while there are three more fields show up which are **Max Hops**, **Revision Level**, and

Region Name. Additionally, there will be a note add to the Per-port Setting box that currently MSTP mode does not support trunk port now.

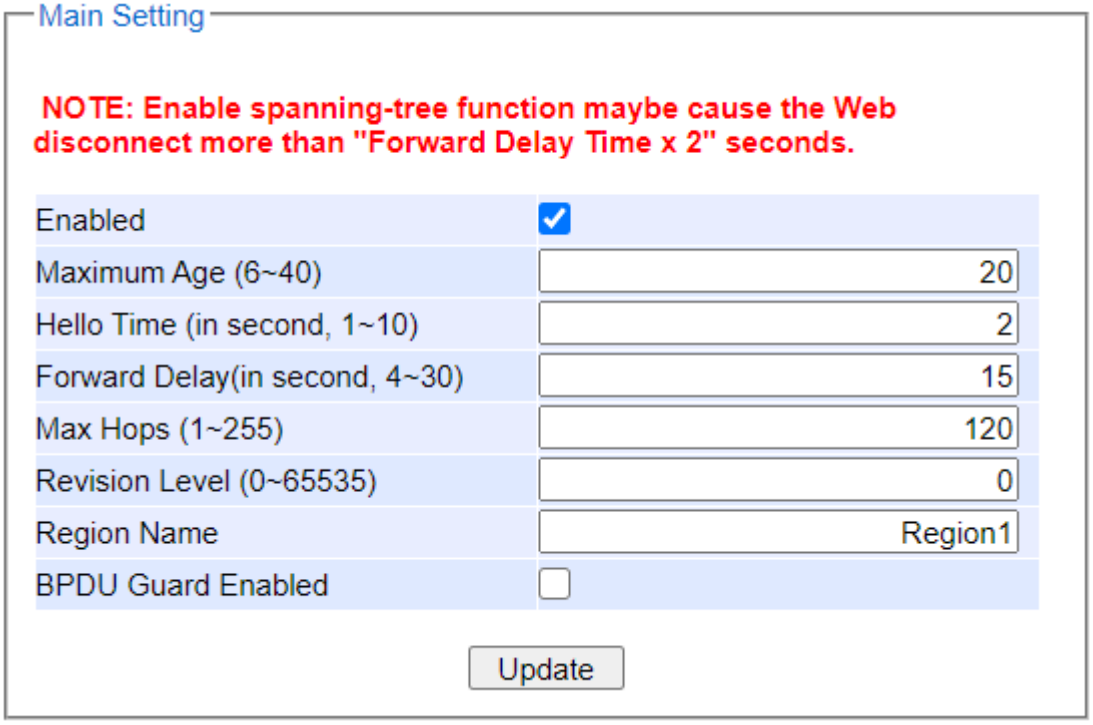


Figure 2.145 Spanning Tree Main Setting for MSTP

Table 2.35 Descriptions of Spanning Tree Parameters

Label	Description	Default Factory
Enabled	Check the box to enable spanning tree functionality.	Disable
Priority	Enter a number to set the device priority. The value is in between 0 and 61440. The lower number gives higher priority.	32768
Maximum Age	Maximum expected arrival time for a hello message. It should be longer than Hello Time.	20
Hello Time	Hello time interval is given in seconds. The value is in between 1 to10.	2
Forward Delay	Specify the time spent in the listening and learning states in seconds. The value is in between 4 to 30.	15
Max Hops(Only for MSTP)	The value is between 1 to 255.	120
Revision Level(Only for MSTP)	The value is between 0 to 65535.	0
Region Name (Only for MSTP)	Text string indicate the region name	Region1
BPDU Guard Enabled	Check the box to enable BPDU guard	Disable

The bottom part of the Spanning Tree Setting is the Per-port setting as shown in Figure 2.146. The users can enable spanning tree functionality individually on each port or on all port by checking on the box under the **Port Enable** column. The default setting is checking on all port. After making any change on the per-port setting, please click on the **Update** button to update the change on the managed switch.

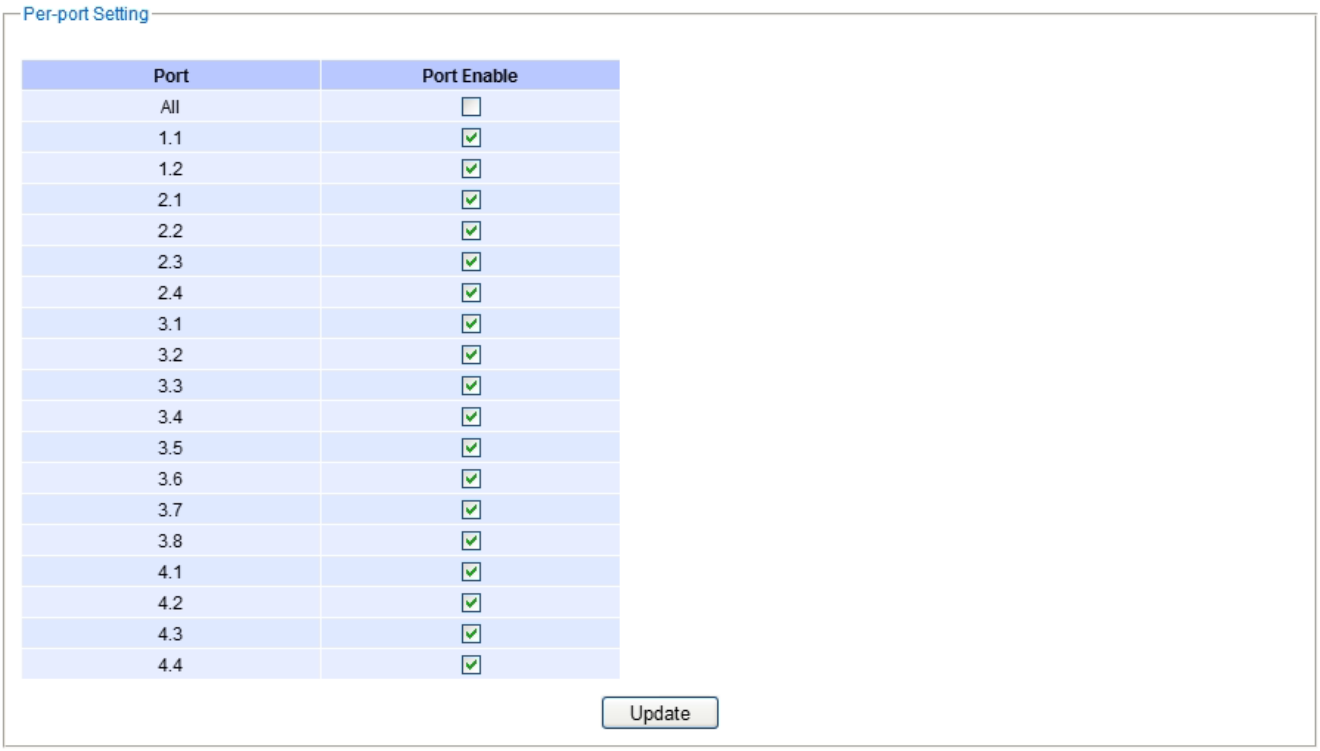


Figure 2.146 Spanning Tree Per-port Setting for STP and RSTP

2.12.2 Bridge Info

Bridge Info (information) provides the statistical value of spanning tree protocol as shown in Figure 2.147.The information is further divided into two parts:Root Information and Topology Information. To check the latest information, please click on the **Refresh** button. Table 2.36 and Table 2.37 summarize the descriptions of each entry in the root information table and topology information table, respectively.

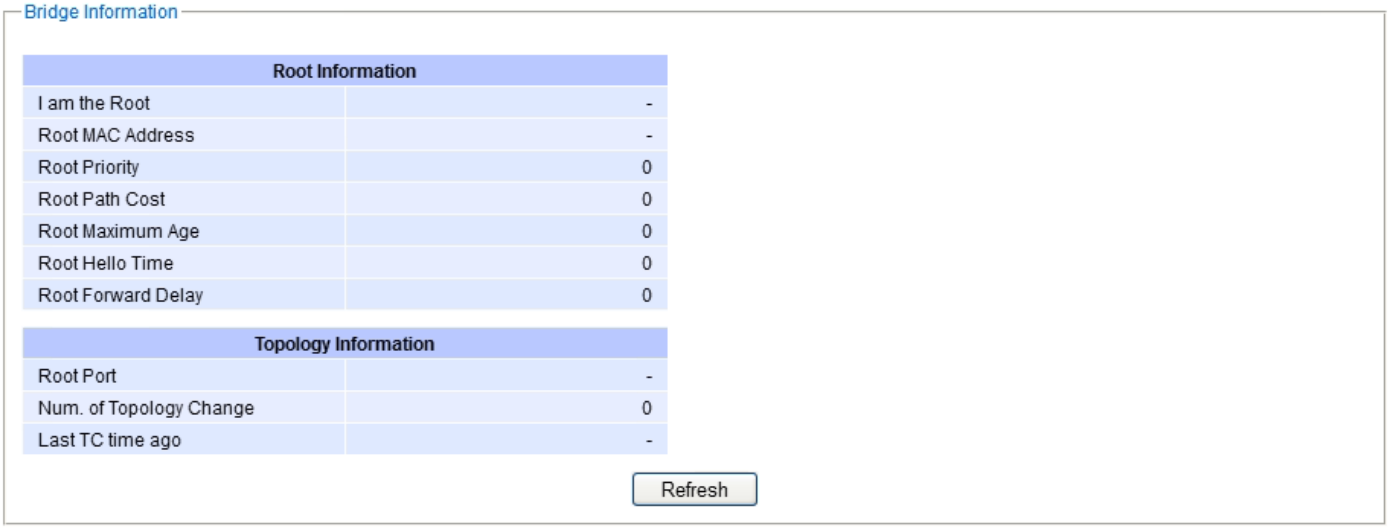


Figure 2.147Bridge Information Webpage

Table 2.36Bridge Root Information

Label	Description	Factory Default
I am the Root	Indicator that this switch is elected as the root switch of the spanning tree topology	-
Root MAC Address	MAC address of the root of the spanning tree	-
Root Priority	Root's priority value: the switch with highest priority has the lowest priority value and it will be elected as the root of the spanning tree.	0
Root Path Cost	Root's path cost is calculated from the data rate of the switch's port.	0
Root Maximum Age	Root's maximum age is the maximum amount of time that the switch will maintain protocol information received on a link.	0
Root Hello Time	Root's hello time which is the time interval for RSTP to send out a hello message to the neighboring nodes to detect any change in the topology.	0
Root Forward Delay	Root's forward delay is the duration that the switch will be in learning and listening states before a link begins forwarding.	0

Table 2.37Bridge Topology Information

Label	Description	Factory Default
Root Port	A forwarding port that is the best port from non-root bridge/switch to root bridge/switch. Note that for a root switch there is no root port.	-
Num. of Topology Change	The total number of spanning topology change over time.	0
Last TC time ago	The duration of time since last spanning topology change.	-

2.12.3 Port Setting

Spanning Tree Port Setting shows the configured value of spanningtree protocol for each port, as shown inFigure 2.148. The configured information for each port is state, role, path cost, path priority, link type, edge, BPDU guard, cost, and designated information. To check the latest update on the statistics, please click on the **Refresh** button. Table 2.38summarizes the descriptions of spanning three port setting when MSTP is enabled. Note that if STP or RSTP is enabled there will be no Instance ID option at the top of the table. If Spanning Tree is enabled, the table below becomes editable. Use the **Update** button to save the settings.

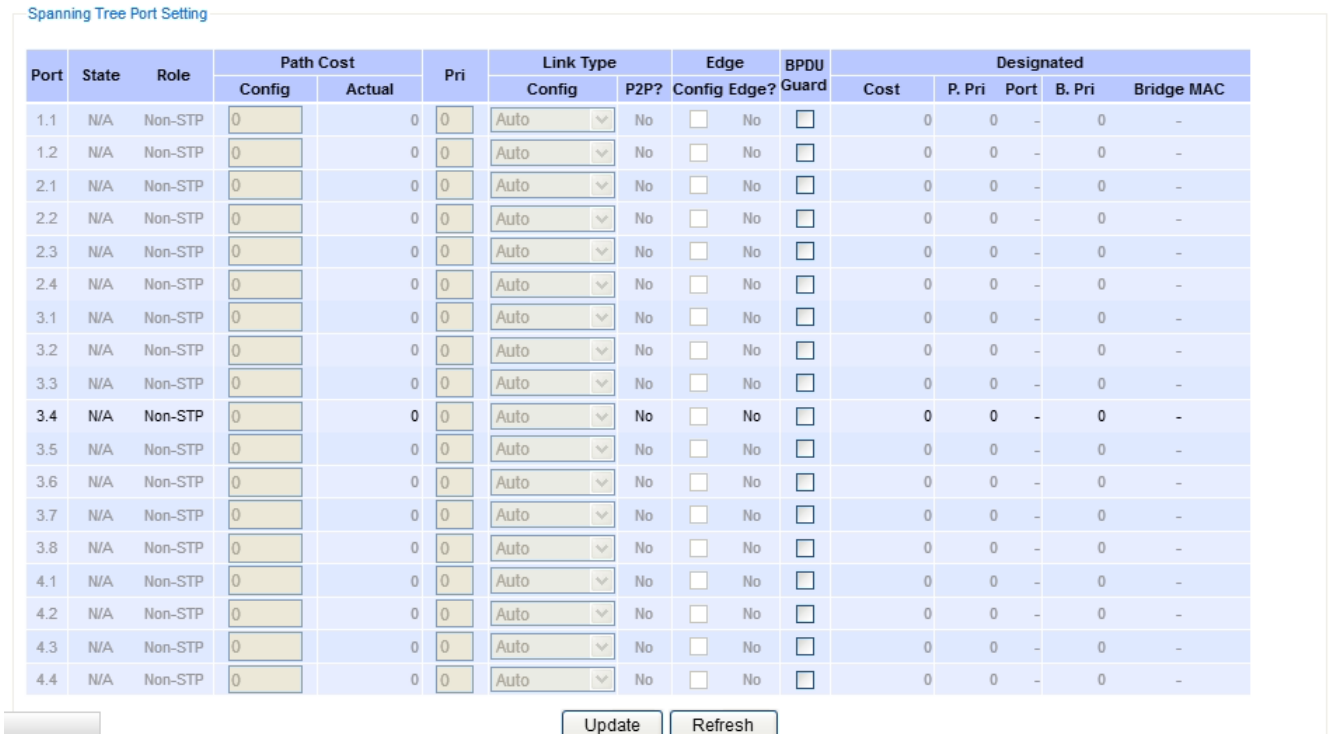


Figure 2.148Spanning Tree Port SettingWebpage

Table 2.38 Descriptions of Spanning Tree Port Setting

Label		Description	Factory Default
Port		The name of the switch port	-
State		State of the port: '**Disc**':Discarding -No user data is sent over the port. '**Lrn**':Learning -The port is not forwarding frames yet, but it is populating its MAC Address Table. '**Fwd**':Forwarding -The port is fully operational.	N/A
Role		Non-STP or STP RSTP bridge port roles: '**Root**'- A forwarding port that is the best port from non-root bridge to root bridge. '**Designated**'-A forwarding port for every LAN segment. '**Alternate**'-An alternate path to the root bridge.This path is different from using the root port. '**Backup**'-A backup/redundant path to a segment whose another bridge port already connects. '**Disabled**'-Note strictly part of STP, a network administrator can manually disable a port.	Non-STP
Path Cost		Setting the path cost for each switch port	
	Config	Setting path cost (default: 0, meaning that using the system default value (depending on link speed))	0
	Actual	The actual value path cost(For STP and RSTP, please see Note 1 below and Table 2.39.)	0
Pri		Setting the port priority, used in the Port ID field of BPDU packet, value = 16 × N, (N:0~15) See Note 2 below.	128
		The connection between two or more switches (for RSTP)	

Label		Description	Factory Default
Link Type	Config	Setting of the Link Type **P2P**: A port that operates in full-duplex mode is assumed to be point-to-point link. **Non-P2P**:A half-duplex port (through a hub) **Auto**:Detect link type automatically	Auto
	P2P?	**Yes**:This port is a Point-to-Point (P2P). **No**:This port is not Point-to-Point (Non-P2P).	No
Edge		Edge port is a port which no other STP/RSTP switch connect to (for RSTP).An edge port can be set to forwarding state directly.	
	Config	Edge functional is set: **Yes** or **No**	No
	Edge?	**Yes**: This port is an edge port. **No**: This port is not an edge port.	No
Designated		This shows some information of the best BPDU packet through this port.	
	Cost	Root path cost	0
	P.Pri.(Port Priority)	Port priority (high 4 bits of the Port ID), Value = 16 × N, (N:0~15)	128
	Port	Interface number (lower 12 bits of the Port ID)	-
	Bri.Pri.(Bridge Priority)	Bridge priority, (value =4096 × N, (N:0~15)	32768
	Bridge MAC	The MAC address of the switch which sent this BPDU	-

Note:

1. In general, the path cost is dependent on the link speed. Table 2.39 lists the default values of path cost for STP and RSTP.

Table 2.39 Default Path Cost for STP and RSTP

Data Rate	STP Cost (802.1D -1998)	RSTP Cost (802.1W-2004)
4 Mbits/s	250	5,000,000
10 Mbits/s	100	2,000,000
16 Mbits/s	62	1,250,000
100 Mbits/s	19	200,000
1 Gbits/s	4	20,000
2 Gbits/s	3	10,000
10 Gbits/s	2	2,000

2. The sequence of events to determine the best received BPDU (which is the best path to the root).

- Lowest root bridge ID determines the root bridge.
- Lowest cost to the root bridge favors the upstream switch with the least cost to root.
- Lowest sender bridge ID serves as a tie breaker if multiple upstream switches have equal cost to root.
- Lowest sender port ID serves as a tie breaker if a switch has multiple (non-Ether channel)links to a single upstream switch.

Bridge ID =priority (4 bits)+ locally assigned system ID extension (12 bits) +ID [MAC Address]48 bits
The default bridge priority is 32768.
Port ID =priority (4 bits) +ID (Interface number)(12 bits)
The default port priority is 128.

2.12.4 MSTP Instance

MSTP enables the grouping and mapping of VLANs to different spanning tree instances. Therefore, an MST Instance (MSTI)is a particular set of VLANs that are all using the same spanning tree. Note that MSTI is identified by MSTI number and locally significant within MST region. Figure 2.149illustrates the MSTP Instance webpage. In this section, the uses can add or remove MSTP instance. The upper part of the webpage is a table of existing MSTP instance in the managed switch. The users can add a new MSTP instance by choosing an Instance ID from the dropdown list, enter the VLAN Identification number in the VID field, and set the desired priority in the Priority field. After filling all information, please click the **Add/Modify** button to update the MSTP instance. The procedure forsetting up an MSTP instance is as follows:

- Enable MSTP protocol in Section 2.12.1
- Modify spanning tree main setting as described in Section 2.12.1
- Select ports that you want to enable MSTP function in Section 2.12.1.
- Add a Multiple Spanning Tree Instance (MSTI)in MSTP Instance webpage(this section).
    - Choose an Instance Identification
    - Add VLAN Identification numbers(VIDs)that will be member(s) of MSTP instance.
    - Set Priority value of the switch.
    - Click **Add/Modify** button.

Table 2.40 summarizes the descriptions of MSTP Information.

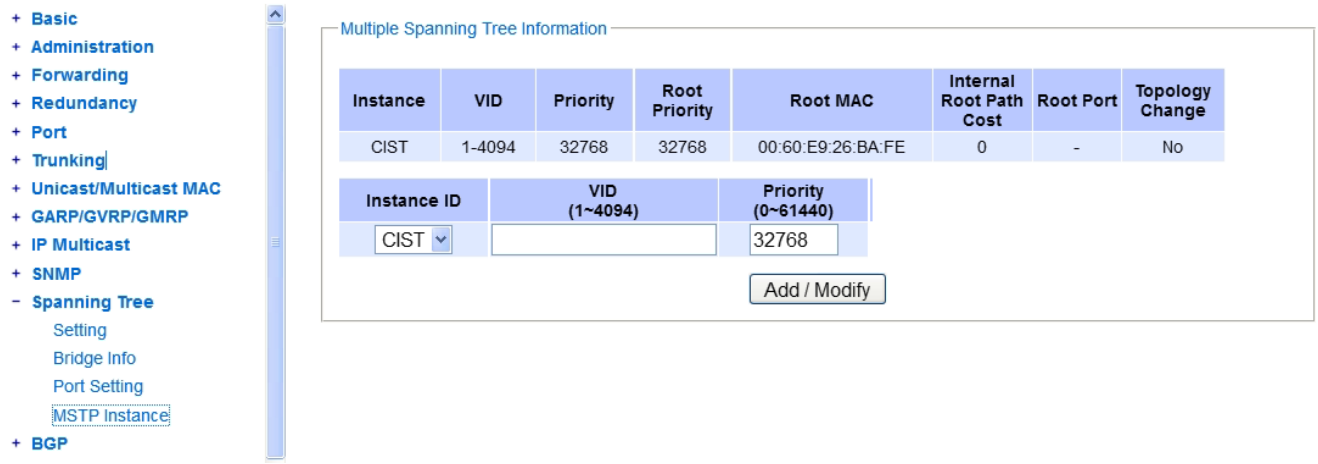


Figure 2.149 MSTP Instance Webpage

Table 2.40 Description of MSTP Information

Label	Description	Factory Default
Instance ID	Choose from dropdown list of CIST (Common and Internal Spanning Tree) or choose value from 1 to 63	CIST
VID	Enter a value for VLAN ID between 1 to 4094	-
Priority	Enter a value for priority value for the managed switch between 0 – 61440. The lower value means the higher priority. If the priority value is 0, the switch will be the Root Bridge in this MSTI.	32768
Root Priority	Display root priority value	32768
Root MAC	Display MAC address of the Root Bridge	-
Internal Root Path Cost	Display internal root path cost	0
Root Port	Display root port	-
Topology Change	Display Yes or No	No

2.13 BGP

A **B**order **G**ateway **P**rotocol (**BGP**)is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous system (AS) on the Internet. It is an interdomain routing protocol that is designed to provide loop-free routing between organizations. There are totally four submenus under this menu including BGP Setting, BGP Neighbor Setting, BGP Proto Setting, and BGP IP Setting, as shown in Figure 2.150. Details of each submenu will be described in the following subsections.

Figure 2.150 BGP Dropdown Menu

2.13.1 BGP Setting

The first menu under the **BGP** section is the **BGP Setting**. Within it, there are two submenus as shown in Figure 2.151. The submenus are Setting and Restart.

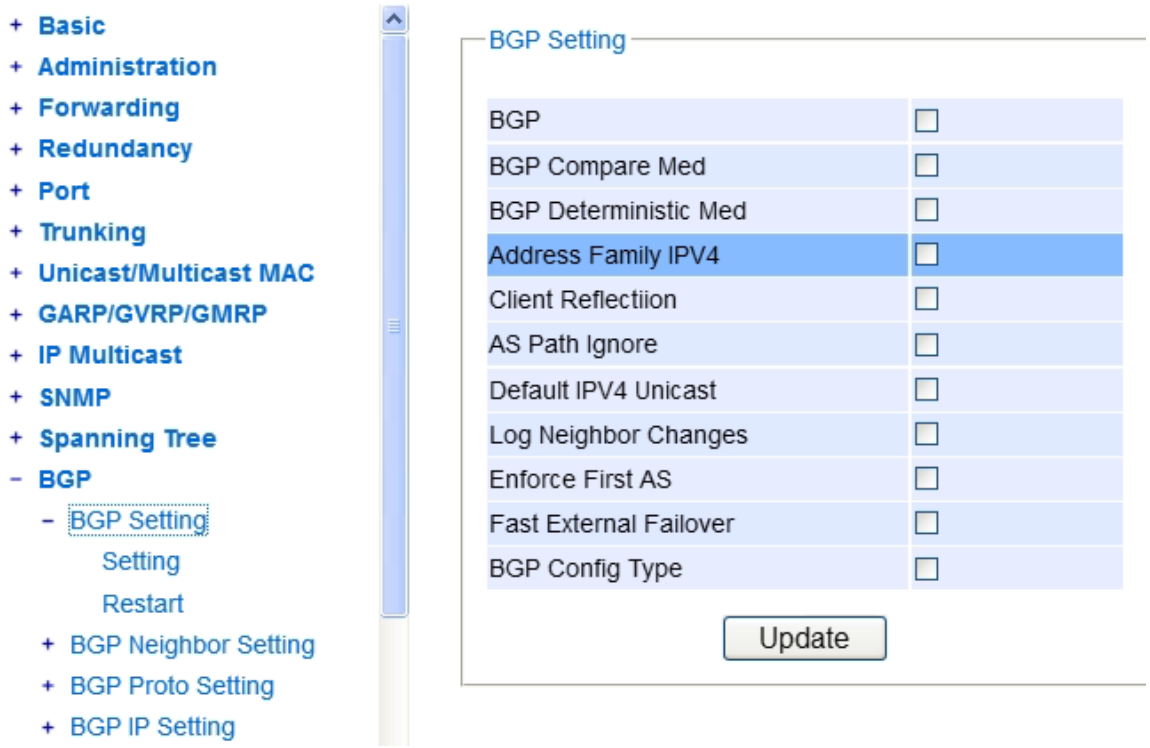


Figure 2.151 BGP Setting Submenu

2.13.1.1 Setting

In the first sub-menu of ***BGP Setting*** is ***Setting*** as shown in Figure 2.152. Here, user can click to select or de-select a check-box to enable or disable any ofthe following BGP features: BGP, BGP Compare Med, BGP Deterministic Med, Address Family IPV4, Client Reflection, AS Path Ignore, Default IPv4 Unicast, Log Neighbor Changes, Enforce First AS, Fast External Failover, and BGP Config Type. After making any change, click on the **Update** button to take effect.

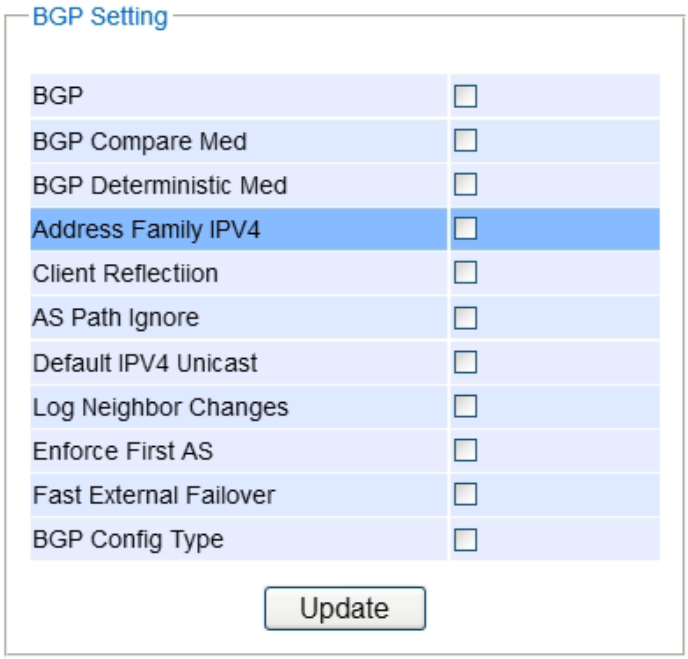


Figure 2.152 *Setting* inside the *BGP-> BGP Setting* Submenu

Table 2.41 Description of each Feature inside the BGP-> BGP Setting Submenu

Field	Description
Compare MED	When enabled this option,the switch will make sure that BGP compares the Multi-Exit Discriminator (MED) for paths from neighbors in**different** autonomous systems (ASs). MED is an external attribute of a route that indicates preferred path into an AS.
Deterministic MED	When enabledthis option,the switch will make sure that BGP compares the Multi-Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the **same** autonomous system (AS).
Address Family IPv4	This option allows the exchanging of IPv4 address family in BGP.
Client Reflection	This option allows configuring the routers as route reflectors. Route reflectors reduce the number of connections required in an AS. A single router (or two for redundancy) can be made a route reflector. Other routers in the AS need only to be configured as peers to them. A route reflector offers an alternative to the logical full-mesh requirement of internal border gateway protocol (IBGP). That is the route reflectors are used when all iBGP speakers are not fully meshed.
AS Path Ignore	This option allows a configuration that prevents a router from considering AS-path as a factor in the algorithm for choosing a route.
Default IPv4 Unicast	If this option is enabled, IPv4-unicast is activated for a peer and BGP exchanges IPv4 prefixes between the XHG76XX device and that peer. If this option is disabled, the BGP routing process will no longer exchange IPv4 addressing information with BGP neighbor routers. Note that disabling the exchange of IPv4 prefixes will also enable an IPv6 only BGP4+ network.
Log Neighbor Changes	If this option is enabled, changing status message will be logged without turning on debug bgp commands.
Enforce First AS	If this option is enabled, eBGP (External Border Gateway Protocol) updates in which the neighbor's AS number is not the first AS in the AS-path attribute will be denied.
Fast-External Failover	If this option is enabled,the BGP session is reset immediately when the interface used for BGP connection goes down.
BGP Config Type	If this option is enabled, the BGP Configuration Type can be configured.

2.13.1.1 Restart

The second sub-menu of ***BGP Setting*** is ***Restart*** as shown inFigure 2.153. Here, user can click Restart button to restart BGP service.

Figure 2.153*BGP Restart inside BGP->BGP Setting Submenu*

Before clicking **BGP Restart** button, user should enable the IP Routing first. Otherwise, the error message will appear as shown below in Figure 2.154. To enable **IP Routing**, select **Enabled** and click **update button** within the **IP routing** menu to take the effect.

Figure 2.154 Error Message of BGP Restart

2.13.2 BGP Neighbor Setting

The second menu under the **BGP** section is the **BGPNeighbor Setting** as shown in Figure 2.155. Under this menu, there are fourteensubmenus: Remote AS, Local AS, Description, Route map, Prefix list, Advertisement Interval, Timers, Allow AS IN, Password, Peer Group, Shutdown, Activate, Route Reflector client, and Remove Private AS.

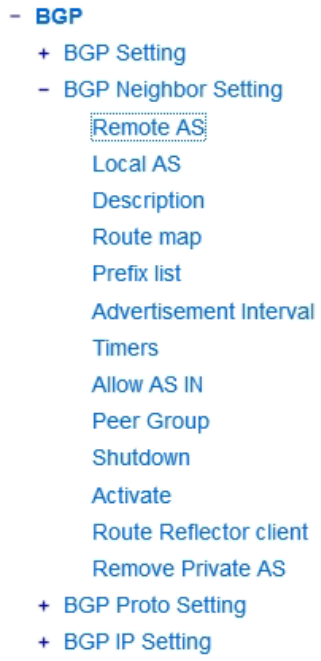


Figure 2.155BGP Neighbor Setting Menu

2.13.2.1 Remote AS

The first sub-menu of ***BGP Neighbor Setting*** is ***Remote AS***, as shown in Figure 2.156. The user can configure an internal or external BGP (iBGP or eBGP) peering relationship with another router. The user needs to fill in the information in two fields: Neighbor ID and Remote AS. *Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. Remote AS< *1-4294967295*> field is the the Neighbor's Autonomous System (AS) number. After entering new information, click the **ADD/Modify** button to change the setting.

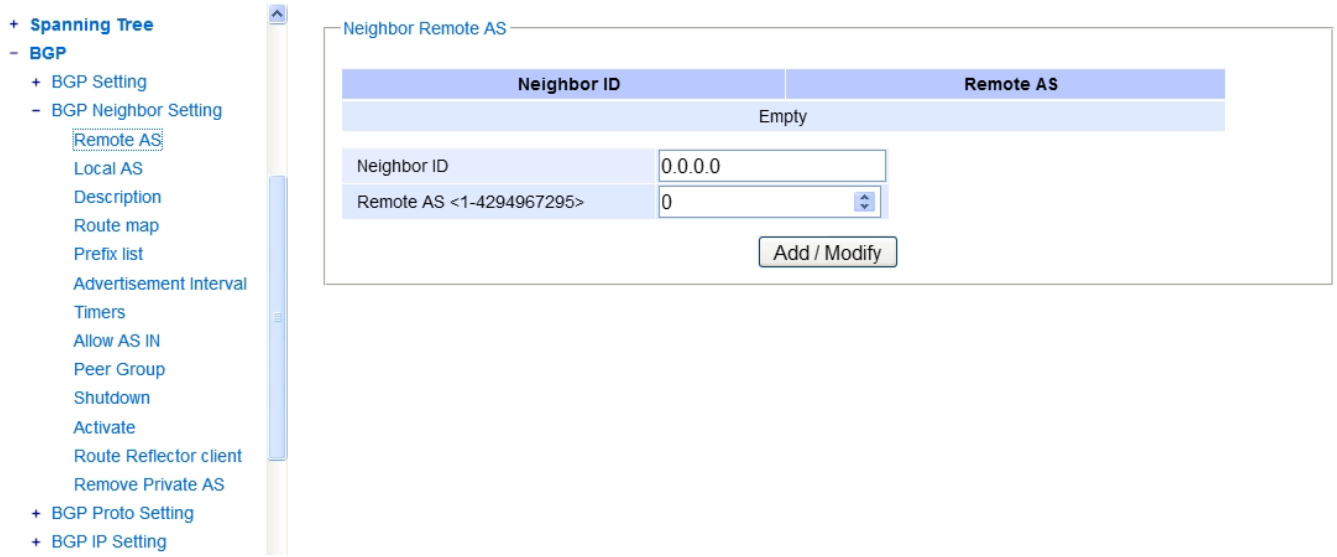


Figure 2.156*Remote AS*Submenu inside the *BGP Neighbor Setting*

2.13.2.2 Local AS

The second sub-menu of ***BGP Neighbor Setting*** is ***Local AS***, as shown in Figure 2.157. The user can configure a local AS number for the specified BGP or BGP4+ neighbor. The user needs to fill in the information in two fields: Neighbor ID and Local AS. *Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format,

e.g., A.B.C.D. *Local AS* field is the Neighbor's Autonomous System (AS) number which can be set from *1* to *4294967295*. After the new information is entered, click the **ADD/Modify** button to change the setting.

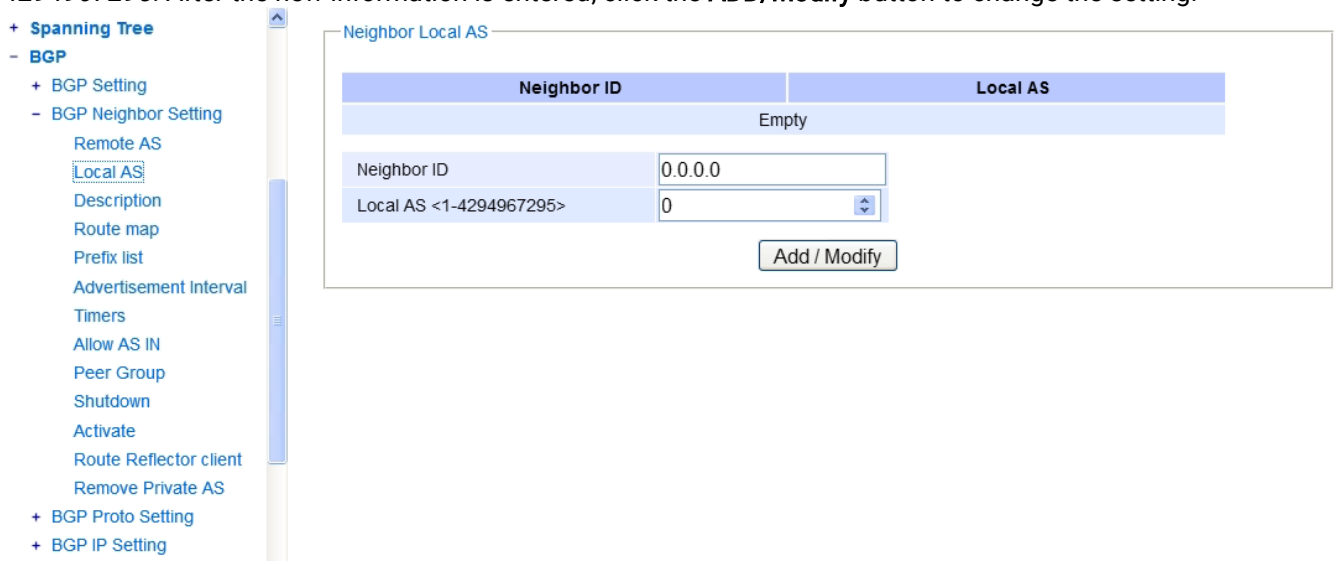


Figure 2.157 *Local AS* Submenu inside the *BGP Neighbor Setting*

2.13.2.3 Description

The third sub-menu of ***BGP Neighbor Setting*** is ***Description***, as shown in Figure 2.158. By using this option, the device can associate a description with a BGP or a BGP4+ neighbor. Adding description to each neighbor is recommended for defining it. The user needs to fill in two fields: *Neighbor ID* and *Description*. *Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. In the *Description* field, the user can input up to 80 characters to describe a neighbor. After new information is keyed in, click the **ADD/Modify** button to take the effect.

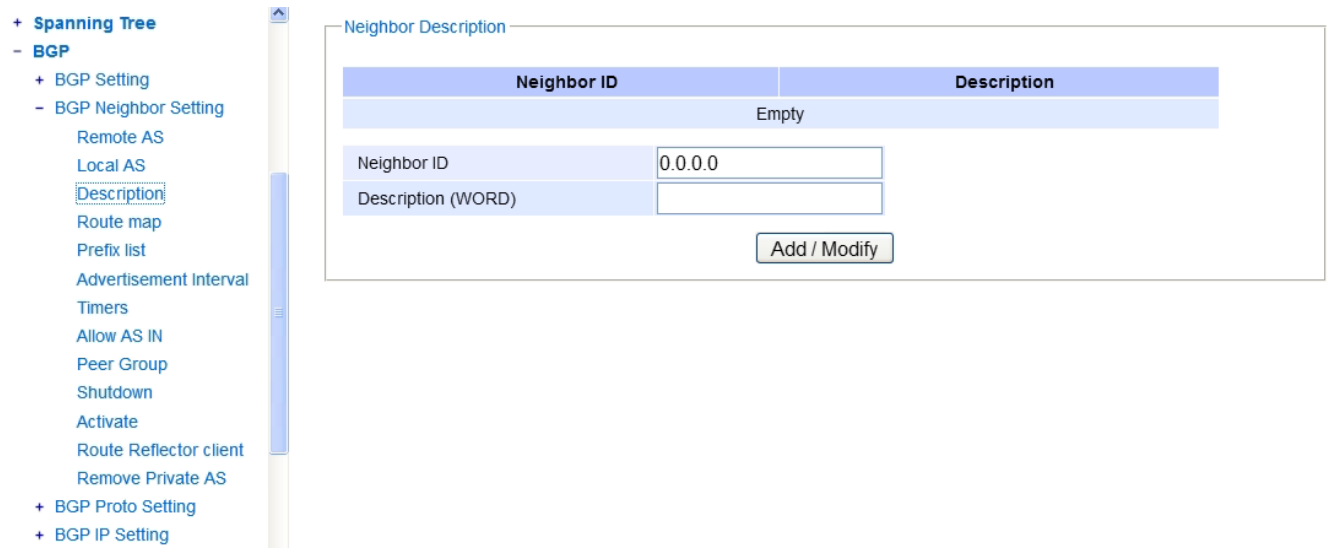


Figure 2.158 *Description* Submenu inside the *BGP Neighbor Setting*

2.13.2.4 Route Map

The fourth sub-menu of ***BGP Neighbor Setting*** is ***Route Map***, as shown in Figure 2.159. The user can use this option to apply a route map to incoming/outgoing routes for BGP/BGP4+. The user needs to fill in two fields: *Neighbor ID* and *Mapname* and to select one dropdown input field called *Type*. *Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. In the *Mapname* field, name of the route-map can be specified. For selectable *Type* field, *"in"* specifies that the access list will be applied to any incoming advertisements, and *"out"* specifies that the access list will be applied to any outgoing advertisements. After new information is keyed in or selected, click the **ADD/Modify** button to take the effect.

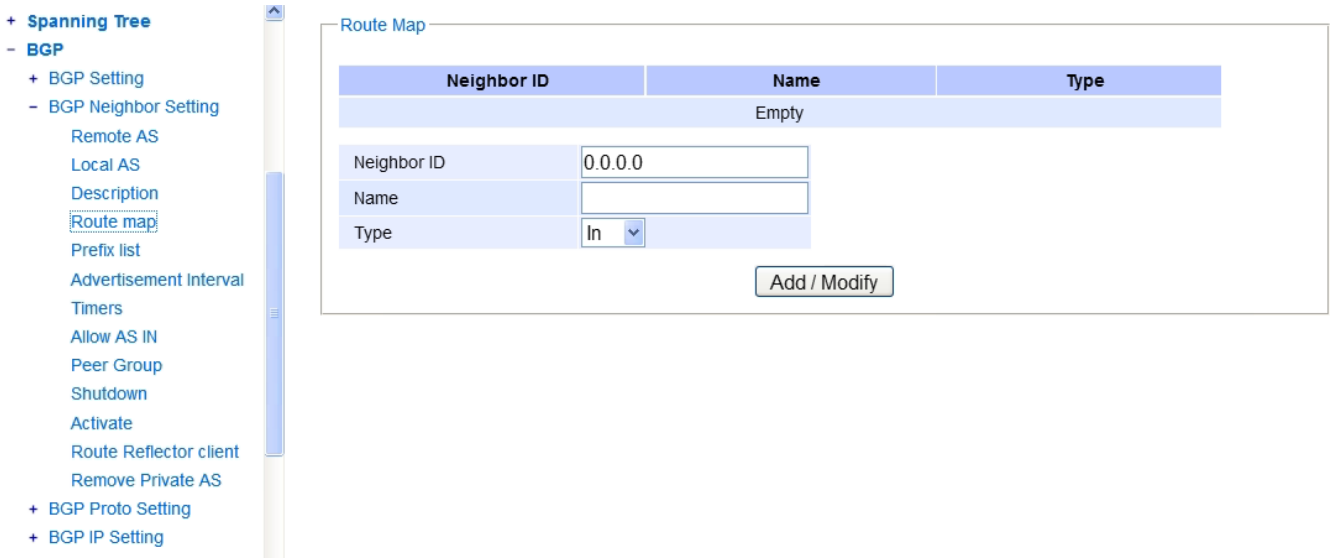


Figure 2.159 *Route Map* Submenu inside the *BGP Neighbor Setting*

2.13.2.5 Prefix List

The fifth sub-menu of ***BGP Neighbor Setting*** is ***Prefix List***, as shown in Figure 2.160. In this option, the user can set how to distribute BGP and BGP4+ neighbor information through a prefix list. The user needs to input and select information for three fields: *Neighbor ID*, *Name, and Type*. *Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. In *Name* field, the user can specify name of the IP Prefix List. For selectable *Type* field, *"in"* specifies that the IP Prefix List will be applied to any incoming advertisements. *"out"* specifies that the IP Prefix List will be applied to any outgoing advertisements. After new information is keyed in or selected, click the **ADD/Modify** button to take the effect.

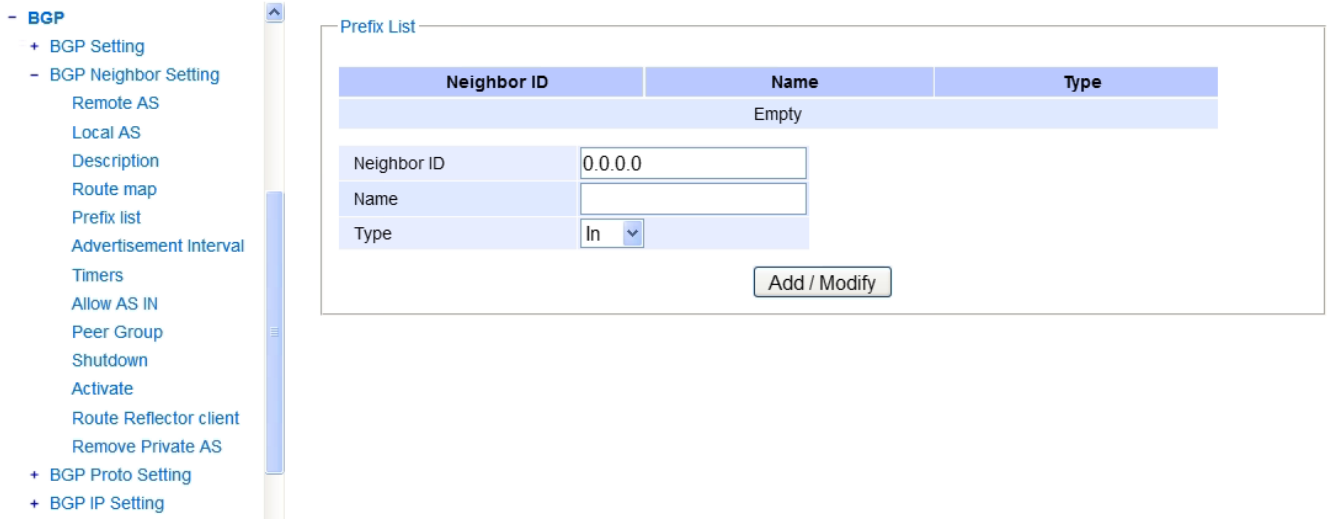


Figure 2.160 *Prefix List* Submenu inside the *BGP Neighbor Setting*

2.13.2.6 Advertisement Interval

The sixth sub-menu of ***BGP Neighbor Setting*** is ***Advertisement Interval*** as shown in Figure 2.161. In this option, the user can set the minimum interval of the iBGP/eBGP routing update for a given route. This option reduces the flapping of an individual route. The user needs to input two fields: *Neighbor ID* and *Advertisement Interval*. *Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. In *Advertisement Interval* field, the user can set the value of anadvertisement interval in seconds, ranging from *1* to *600*. After the new information is keyed in, click the **ADD/Modify** button to take the effect.

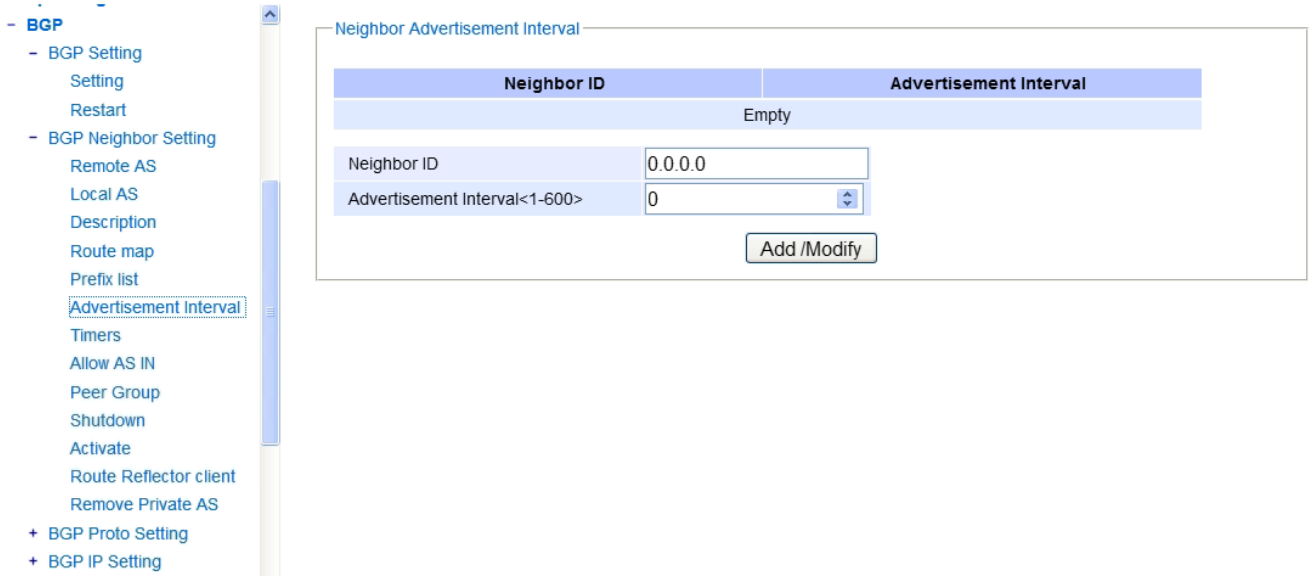


Figure 2.161 *Advertisement Interval* Submenu inside the *BGP Neighbor Setting*

2.13.2.7 Timers

The seventh sub-menu of ***BGP Neighbor Setting*** is ***Timers*** as shown in Figure 2.162. In this option, the user can configure timers to set keepalive, hold-time, and connection timer for a specific BGP or BGP4+ neighbor. Here, the user needs to input three fields: *Neighbor ID*, *Timer1,* and *Timer2*. *Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. In *Timer1* field, the user can set frequency (in seconds) at which a router sends keepalive messages to its neighbor. The value can be set from *0* to *65535*. In *Timer2* field, the user can set Interval (in seconds) after which it did not receiving any keepalive message, the router declares a neighbor is dead. The interval can be set from *0* to *65535*. After the new information is keyed in, click the **ADD/Modify** button to take the effect.

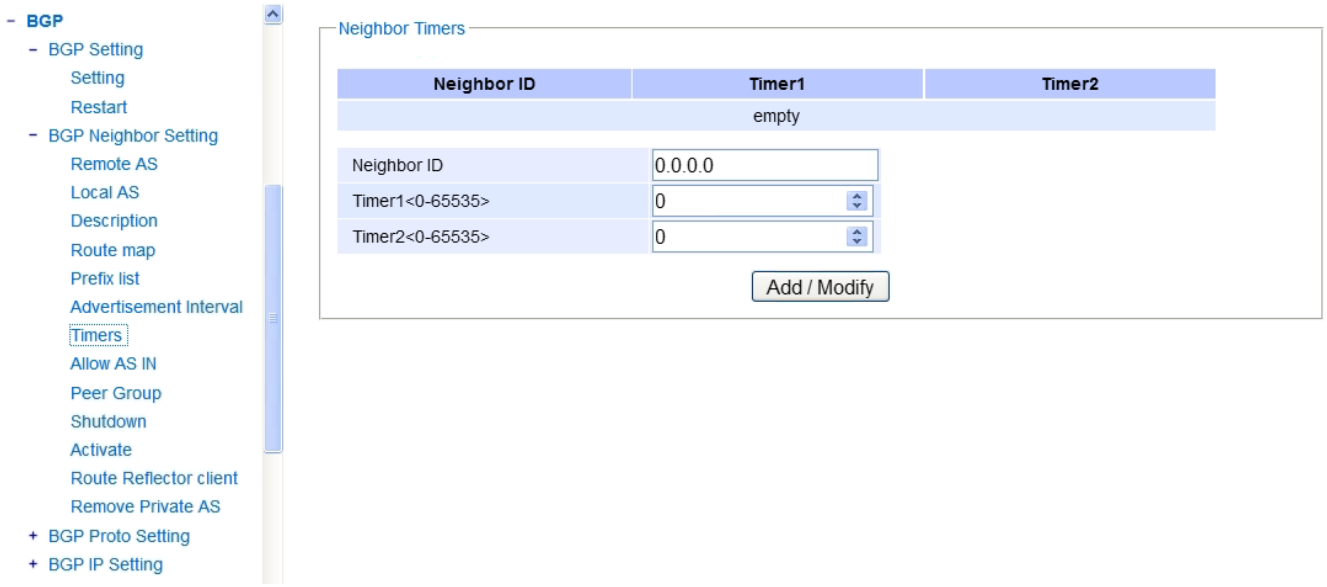


Figure 2.162 *Timers* Submenu inside the *BGP Neighbor Setting*

2.13.2.8 Neighbor Allow AS IN

The eighth sub-menu of ***BGP Neighbor Setting*** is ***Allow AS IN***, as shown in Figure 2.163. The user can use this option to accept an AS_PATH with the specified Autonomous System (AS) number from inbound updates for both BGP and BGP4+ routes. Here, the user needs to input two fields: *Neighbor ID* and *Allow AS in*. *Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. For *Allow AS in* field, the value can be set from *1* to *10.*After the new information is keyed in, click the **ADD/Modify** button to take the effect.

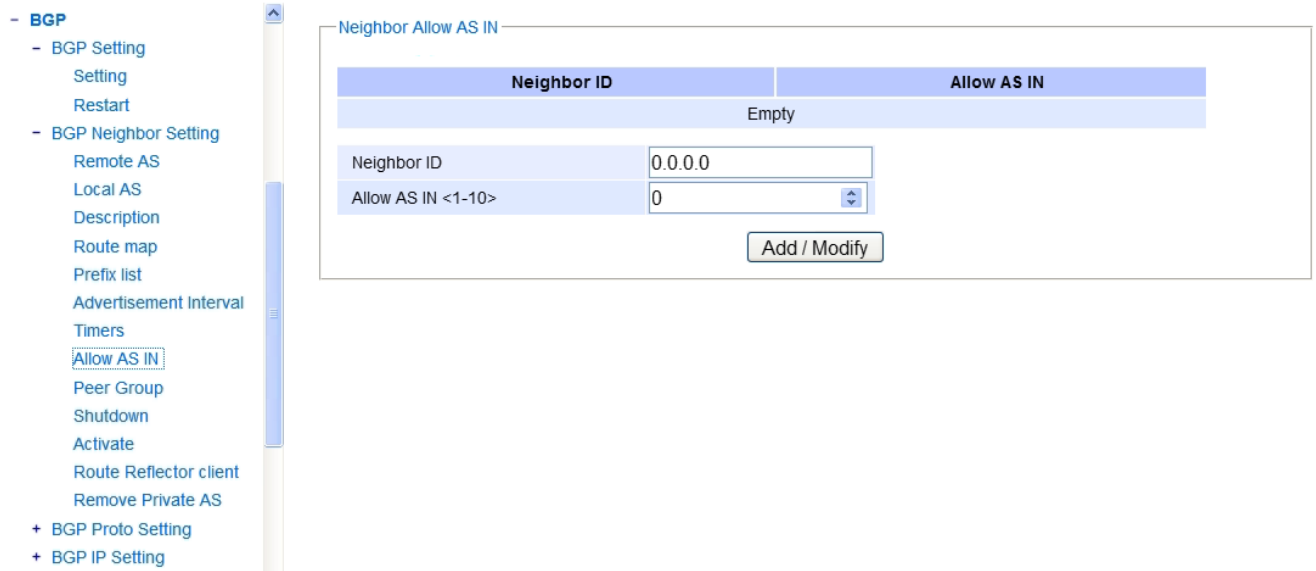


Figure 2.163*Allow AS IN*Submenu inside the *BGP Neighbor Setting*

2.13.2.9 Peer Group

The tenth sub-menu of ***BGP Neighbor Setting*** is ***Peer Group*** as shown in Figure 2.164. In this option, the user can add a BGP or a BGP4+ neighbor to an existing peer-group. Two fieldsare needed to be input:*Neighbor ID* and *Peer Group (Word).Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. In the *Peer Group* field, the user can enter the name of the peer-group, which will be applied on all peers in the specified group. Remember to click **ADD/Modify**Button to take the effect after the new information is keyed in.

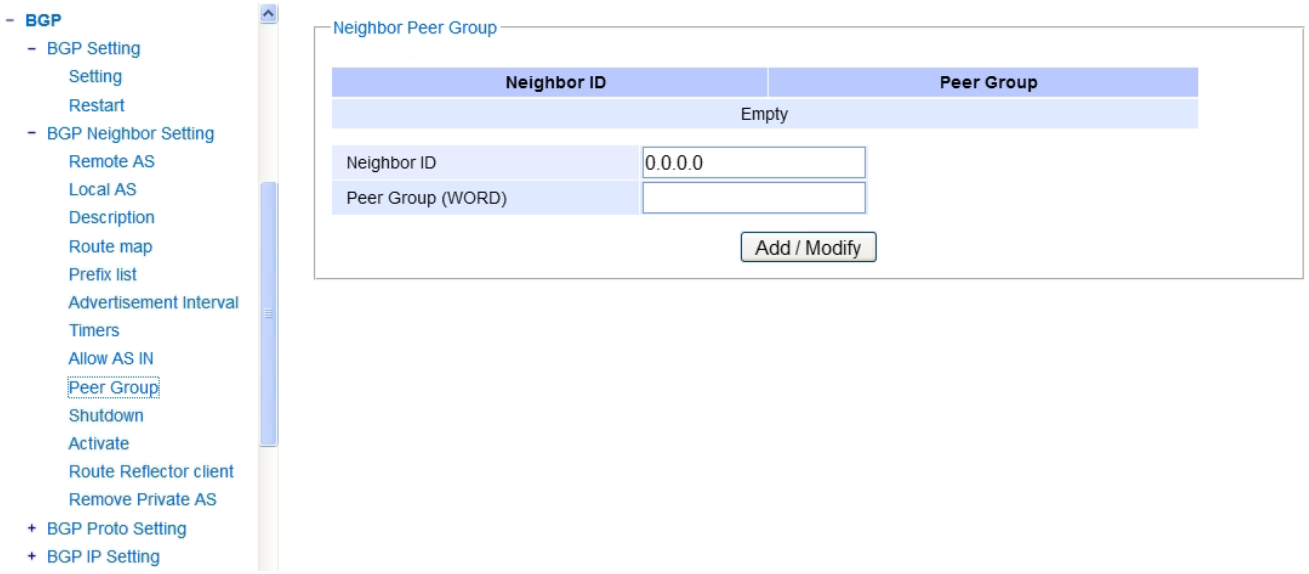


Figure 2.164*Peer Group* Submenu inside the *BGP Neighbor Setting*

2.13.2.10 Shutdown

The eleventh sub-menu of ***BGP Neighbor Setting*** is ***Shutdown***, as shown inFigure 2.165. The user can disable a peering relationship with a BGP or BGP4+ neighbor. Only one field is needed to be filled here: *Neighbor ID. Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. After the new information is keyed in, click the **ADD**button to take the effect.

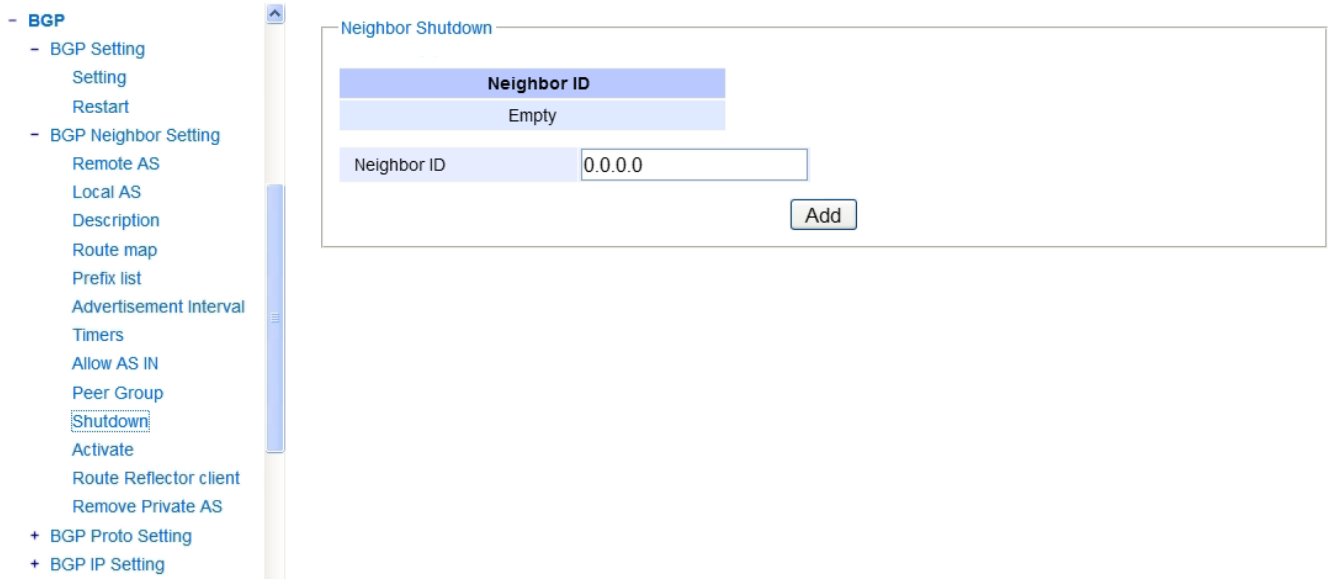


Figure 2.165*Shutdown* Submenu inside the *BGP Neighbor Setting*

2.13.2.11 Activate

The twelveth sub-menu of ***BGP Neighbor Setting*** is ***Activate***, as shown inFigure 2.166. In this option, the user can enable the exchange of BGP IPv4 routes with a neighboring router. Only one field is needed to be filled here: *Neighbor ID. Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. After the new information is keyed in, click the **ADD** button to take the effect.

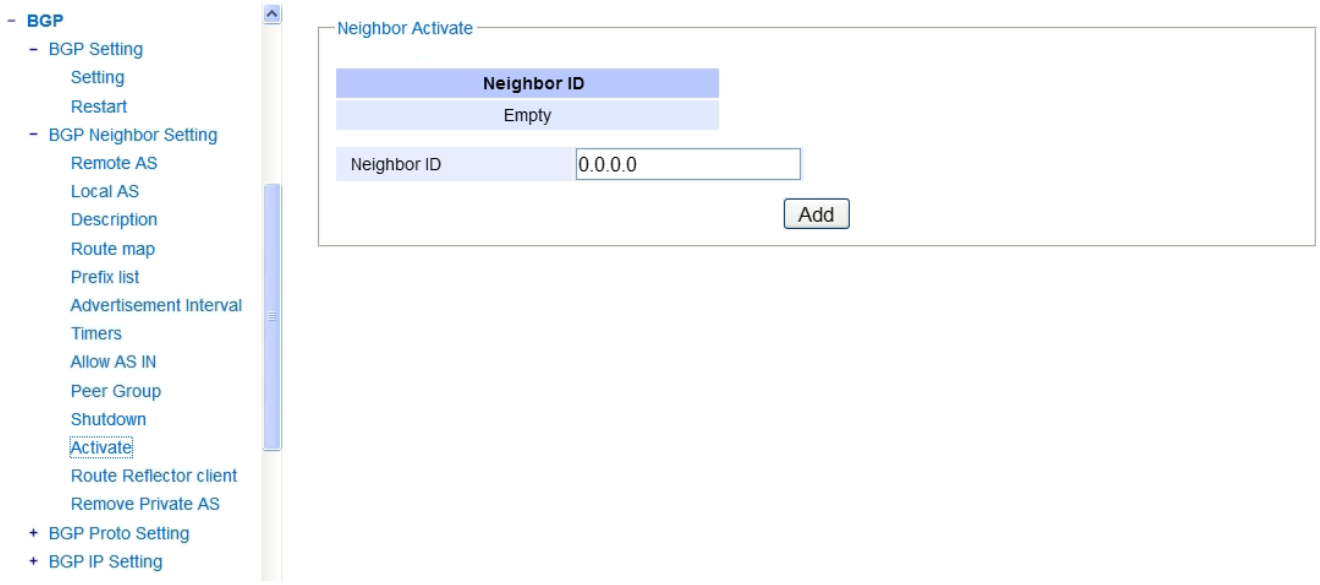


Figure 2.166*Activate* Submenu inside the *BGP Neighbor Setting*

2.13.2.12 Route Reflector Client

The thirteenth sub-menu of ***BGP Neighbor Setting*** is ***Route Reflector Client***, as shown inFigure 2.167. In this option, the user canconfigure the device as a BGP route reflector and configure the specified neighbor as its client. Only one field is needed to be filled here: *Neighbor ID. Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. After the new information is keyed in, click the **ADD** button to take the effect.

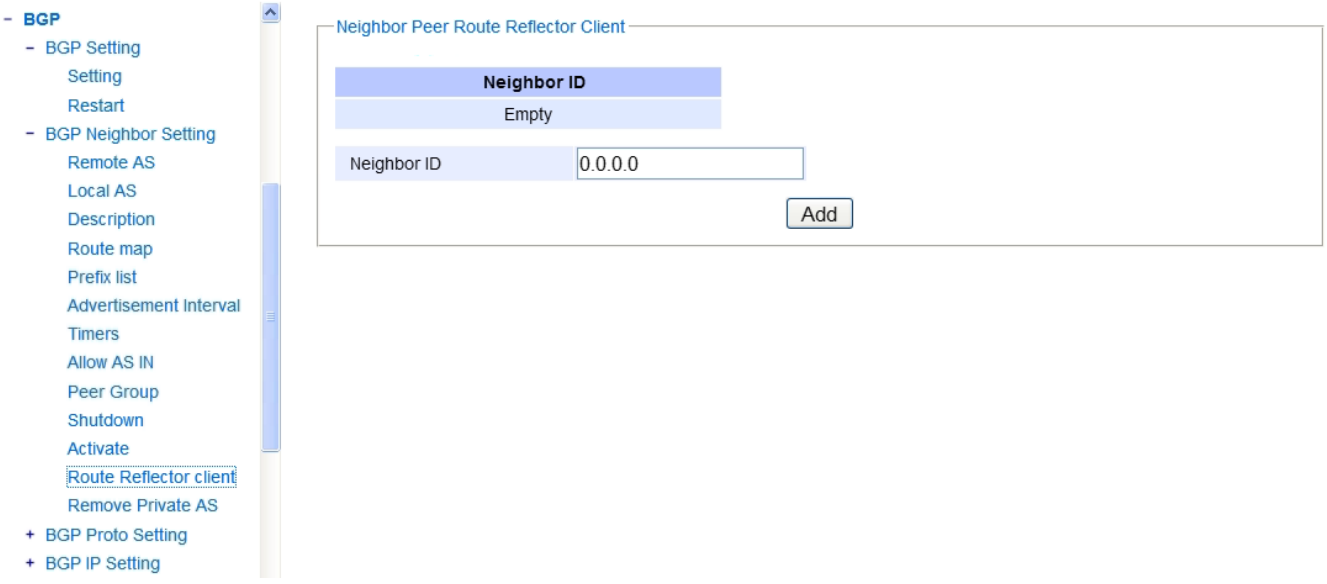


Figure 2.167*Route Reflector Client* Submenu inside the *BGP Neighbor Setting*

2.13.2.13 Remove Private AS

The forteenth sub-menu of ***BGP Neighbor Setting*** is ***Remove Private AS***, as shown inFigure 2.168. In this option, the user canremove the private Autonomous System (AS) number from external outbound updates. Only one field is needed to be filled here: *Neighbor ID. Neighbor ID* specifies the address of an IPv4 BGP neighbor in a dotted decimal format, e.g., A.B.C.D. After the new information is keyed in, click the **ADD** button to take the effect.

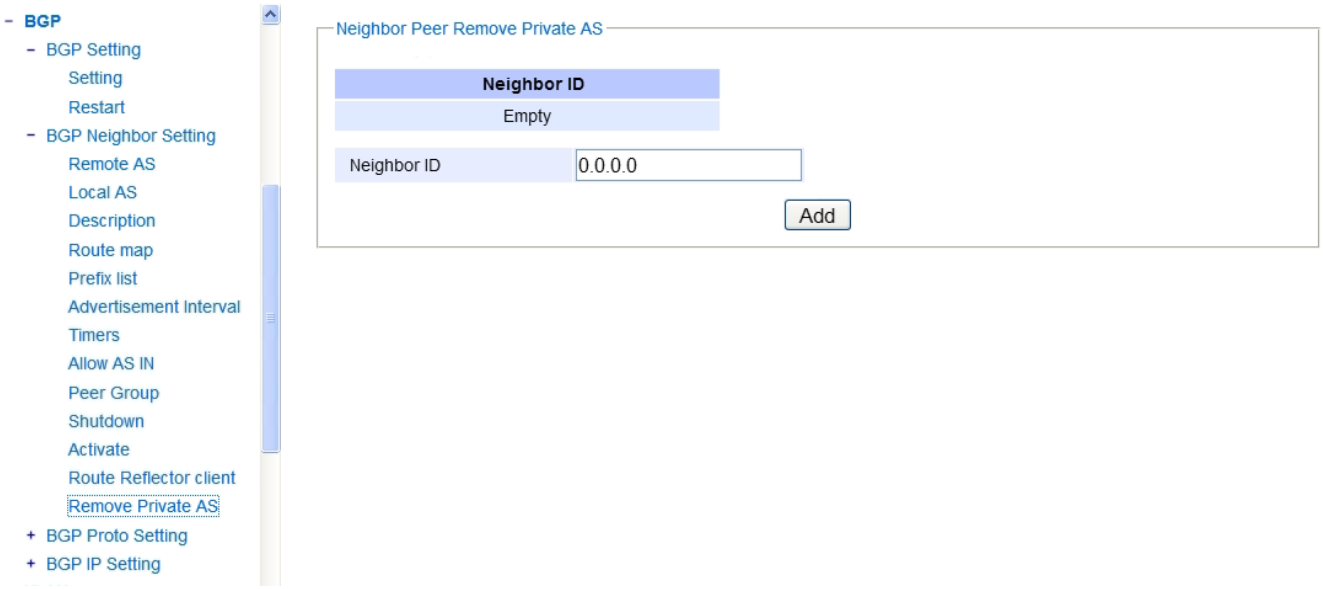


Figure 2.168*Remove Private AS* Submenu inside the *BGP Neighbor Setting*

2.13.3 BGP Proto Setting

The third menu under the BGP section is the BGP Proto Setting as shown inFigure 2.169. Under it, there are thirteen submenus: BGP Router ID, Router BGP ASN, Set AS Path Prepend, BGP Timers, Dampening, Route Map, Network IP, Confed. Peers, Confed. Identifier, Aggregate IP, Maximum Path, Redistribute, and Match Setting.

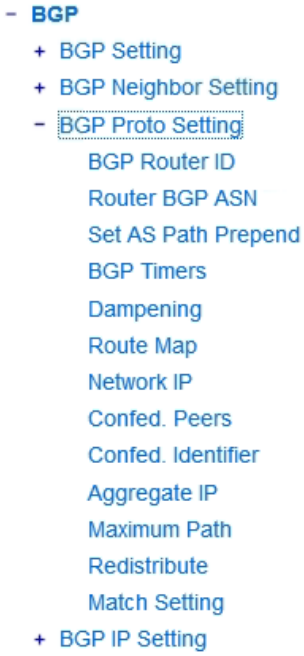


Figure 2.169BGP Proto Setting Menu

2.13.3.1 BGP Router ID

This sub-menu of ***BGP Proto Setting*** is called ***BGP Router ID***, as shown inFigure 2.170. In this option, the user can configure the router identifier (ID). In this option, only one field is needed to be filled here: *Router ID.* In *Router ID*, the user can specify the IPv4 address without mask for a manually configured router ID, in the format A.B.C.D. After the new information is keyed in, click the **ADD** button to take the effect.

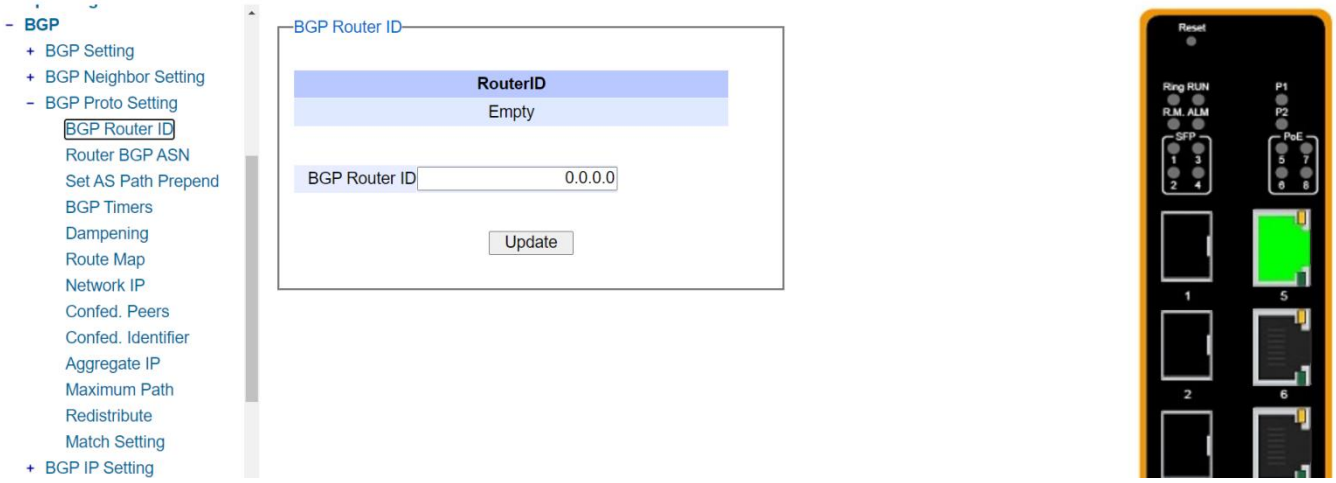


Figure 2.170 *BGP Router* ID Submenu inside the *BGP Proto Setting*

2.13.3.2 Router BGP ASN

This sub-menu of ***BGP Proto Setting*** is called ***Router BGP ASN***, as shown inFigure 2.171. In this option, the user can set the BGP and BGP4+ connections for peers in the specified Autonomous System Number (ASN). In this option, only one field is needed to be filled here: *Router BGP ASN.* In *Router BGP ASN* field, the user can specify an AS number, ranging frin 1 to 4294967295. After the new information is keyed in, click the **ADD** button to take the effect.

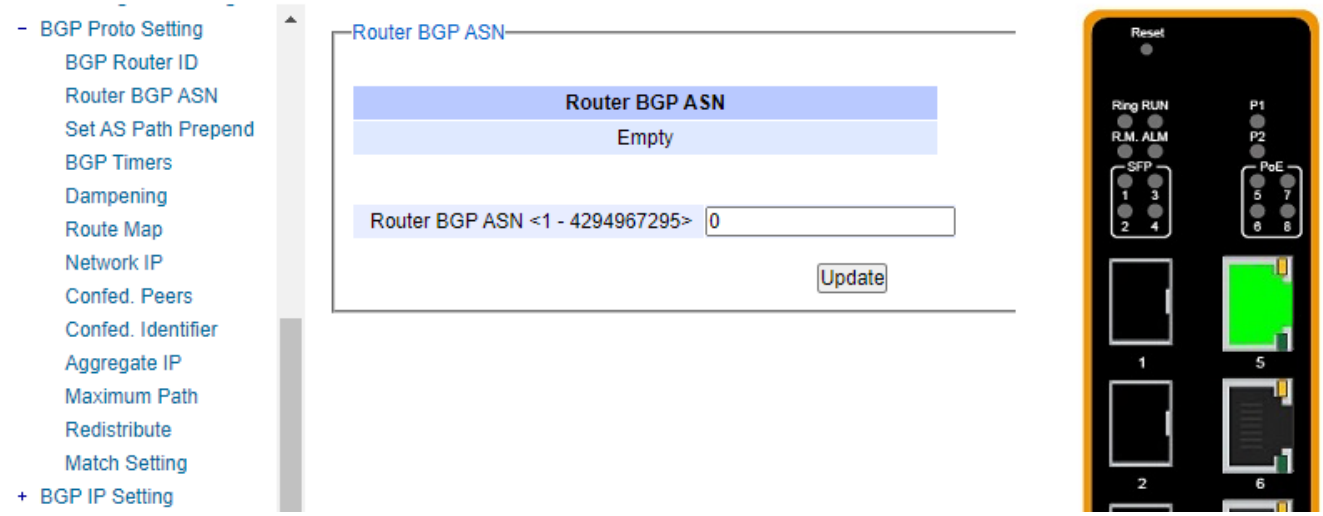


Figure 2.171 *Router BGP ASN* Submenu inside the *BGP Proto Setting*

2.13.3.3 Set AS Path Prepend

This sub-menu of ***BGP Proto Setting***is called ***Set AS Path Prepend***, as shown inFigure 2.172. In this option, the user canadd or prepend an Autonomus System (AS) path set clause to a route map entry. In this option, two fields are needed to be filled here: *AS1*, *AS2.* In *AS1*, the user can input the peer's AS-number, ranging from 1 to 4294967295. In *AS2*, user can input number of times to insert, ranging from 1 to 10. After the new information is keyed in, click the **ADD** button to take the effect.

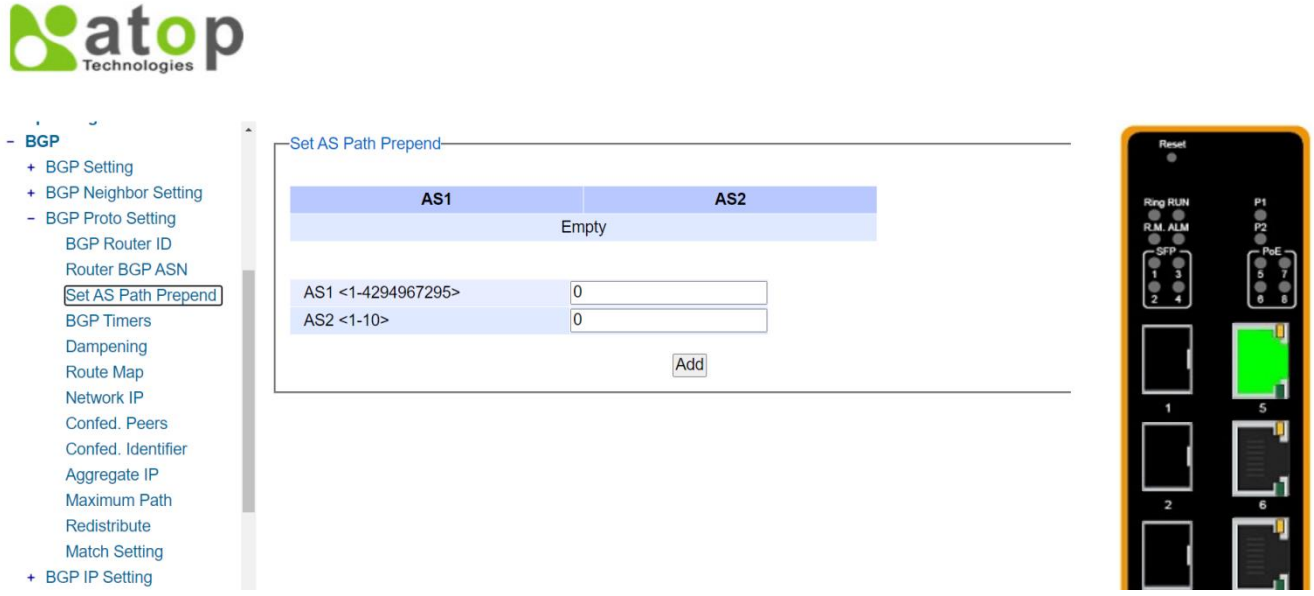


Figure 2.172 *Set AS Path Prepend* Submenu inside the *BGP Proto Setting*

2.13.3.4 BGP Timers

This sub-menu of ***BGP Proto Setting***is called ***BGP Timers***, as shown inFigure 2.173. In this option, the user canset values of the BGP keepalive timer and the holdtime timer. In this option, two fields are needed to be filled here: *Timers1*and *Timers2.* In *Timers1* field, the user can input the frequency of which the keepalive messages are sent to the neighbors, ranging from *0* to *65535*. In *Timers2* field, user can input the interval of time which the neighbor is considered dead if keepalive messages are not received, ranging from *0* to *65535*. After the new information is keyed in, click the **ADD** button to take the effect.

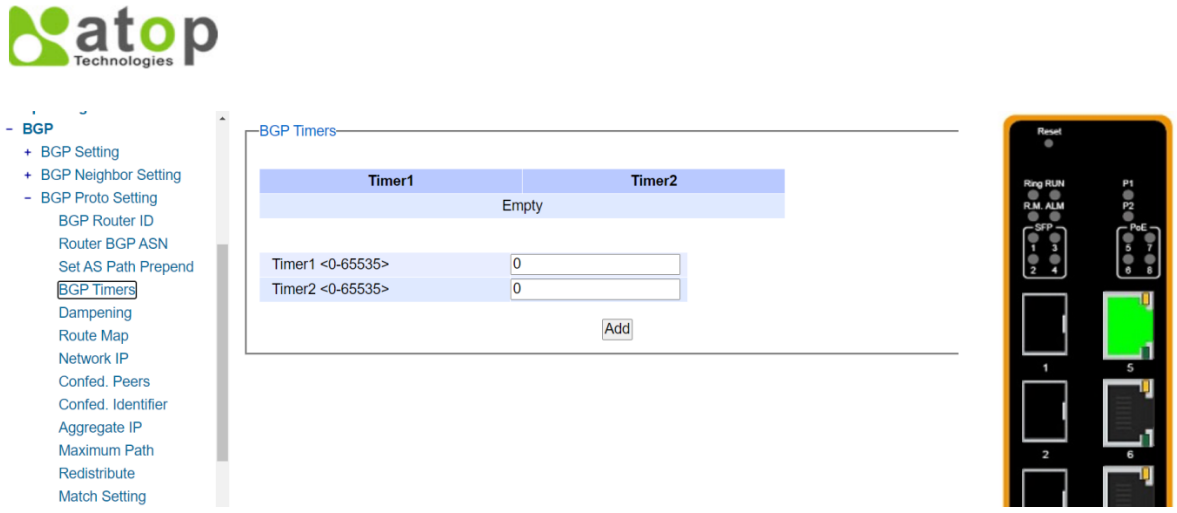


Figure 2.173*BGP Timers* Submenu inside the *BGP Proto Setting*

2.13.3.5 Dampening

This sub-menu of ***BGP Proto Setting*** is called ***Dampening***, as shown inFigure 2.174. In this option, the user can enable BGP and BGP4+ dampening and sets BGP and BGP4+ dampening parameters. BGP4+ dampening is available from the IPv6 Address Family Configuration mode. BGP dampening is available from the Router Configuration mode.

In this option, four fields are needed to be filled here: *Reachtime Half Life, Reuse Threshold, Suppress Threshold,* and *Max Suppress.* In *Reachtime Half Life* field, the user can specify the reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value. This value is ranging from 1 to 45, and the default value is set to 15 minutes. In the Reuse *Threshold* field, the user can specify the reuse limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. This value is ranging from 1 to 20000, and the default value for the reuse limit is set to 750. In the *Suppress Threshold* field, the user can specify the suppress limit value. When the penalty for a route exceeds the suppress value, the route is suppressed. Value of the suppress time is ranging from 1 to 20000 and the default value is set to 2000. In the *Max Suppress* field, the user can specify the max-suppress-time, or the maximum time that a dampened route is suppressed. This value is ranging from 1 to 255, and the default value is set to 4 times the half-life time (60 minutes). After the new information is keyed in, click the **ADD** button to take the effect.

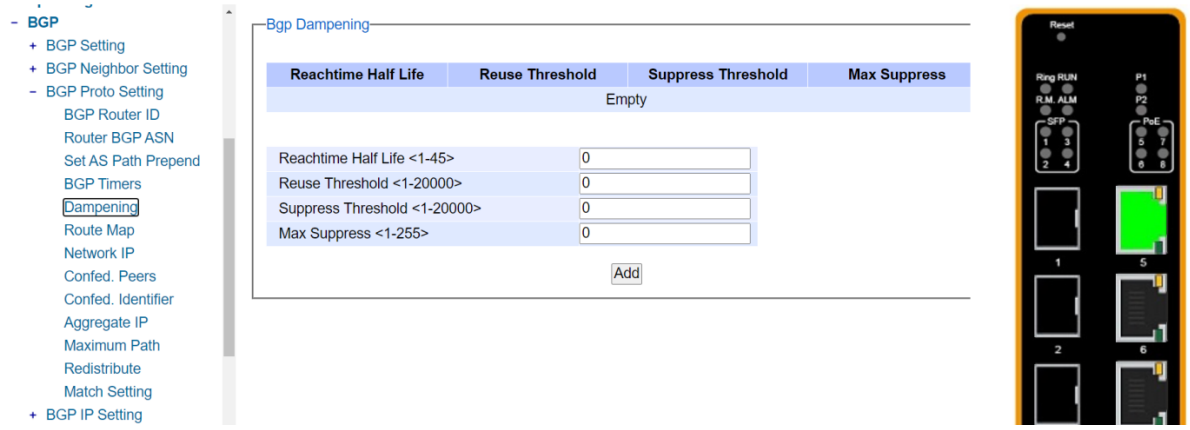


Figure 2.174 *Dampening* Submenu inside the *BGP Proto Setting*

2.13.3.6 Route Map

This sub-menu of ***BGP*** is called ***Route Map***, as shown in Figure 2.175. In this option, the user can apply a route map to incoming or outgoing routes for BGP or BGP4+. Three fields are needed to be filled and selected here: *Name, List Type,* and *Sequence Number.* In *Name* field, the user can specify name of the route-map. In *List Type* field, the user can select whether Permit or Deny. In *Sequence Number* field, the user can specify that the access list applied to incoming or outgoing advertisements. After the new information is keyed in, click the **ADD** button to take the effect.

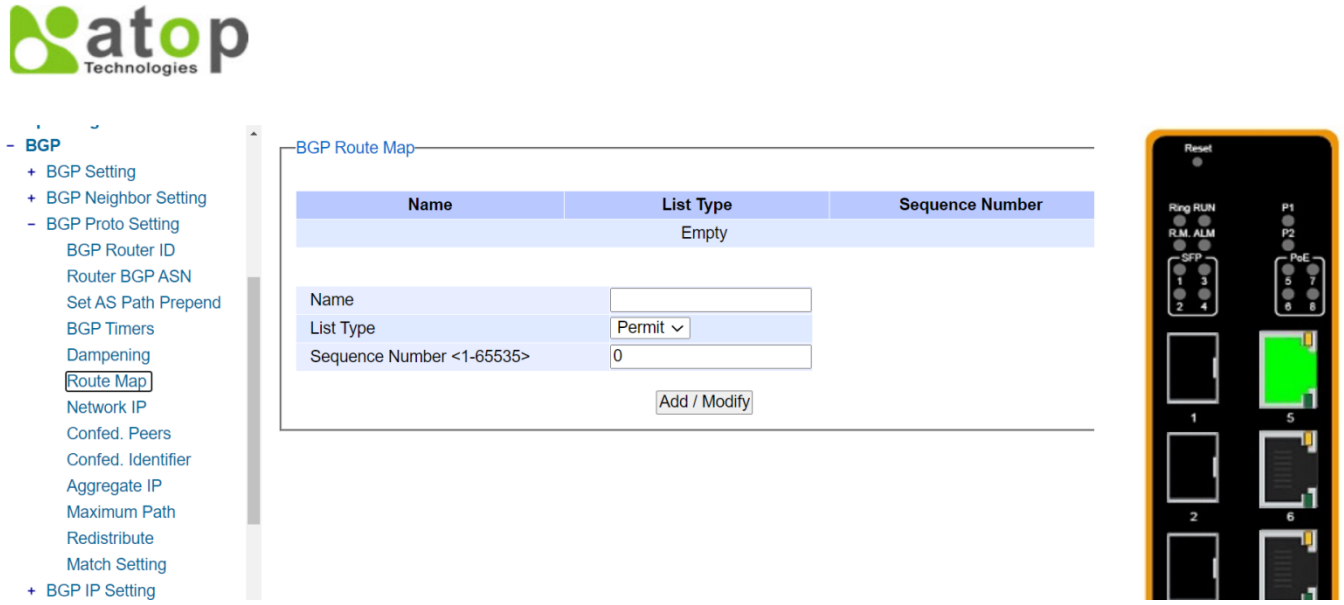


Figure 2.175Route Map Submenu Inside the BGP Proto Setting

2.13.3.7 NetworkIP

This sub-menu of ***BGP Proto Setting*** is called ***Network IP***, as shown inFigure 2.176. In this option, the user can specify particular routes to be advertised into the BGP or BGP4+ routing process. In this option, two fields are needed to be filled here: *Network IP* and *Prefix.* In *Network IP* field, user can specify an IP address of the network in dotted decimal format A.B.C.D. In the *Prefix* field, IP prefix length of the network can be specified, ranging from 4 to 36. After the new information is keyed in, click the **ADD** button to take the effect.

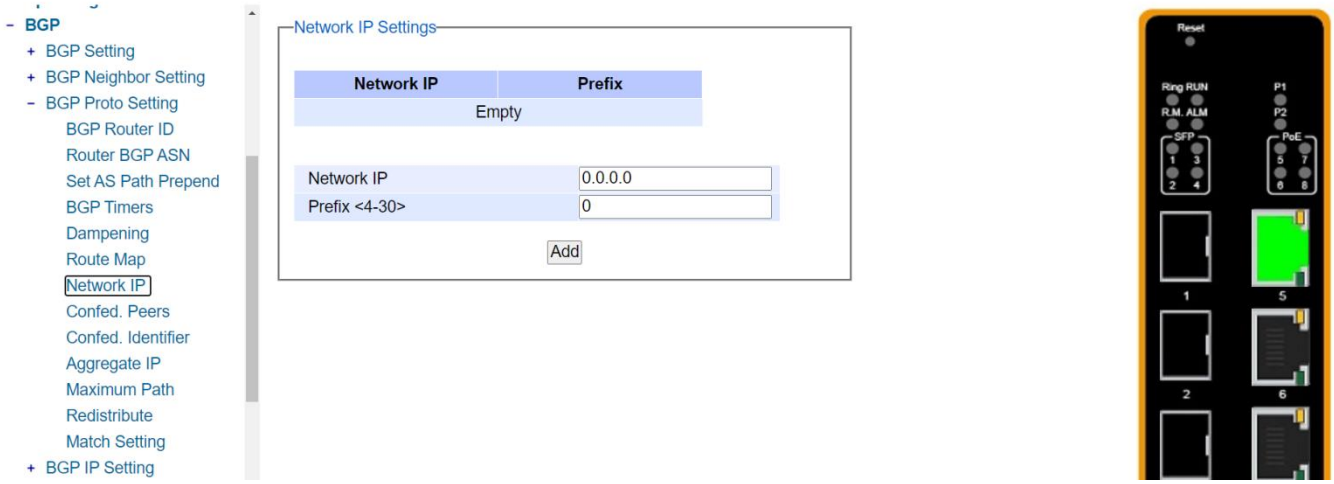


Figure 2.176 *Network IP* Submenu inside the *BGP Proto Setting*

2.13.3.8 Confed. Peers

This sub-menu of ***BGP Proto Setting*** is called ***Confed. Peers***, as shown in Figure 2.177. In this option, the user can configure the Autonomous Systems (AS) that belongs to the same confederation as the current device. In this option, only one field is needed to be filled here: *Confederation Peers.* In *Confederation Peers* field, the user can specify AS numbers of eBGP peers that are under same confederation but in a different sub-AS. The value ranges from *1 to 4294967295.* After the new information is keyed in, click the **ADD** button to take the effect.

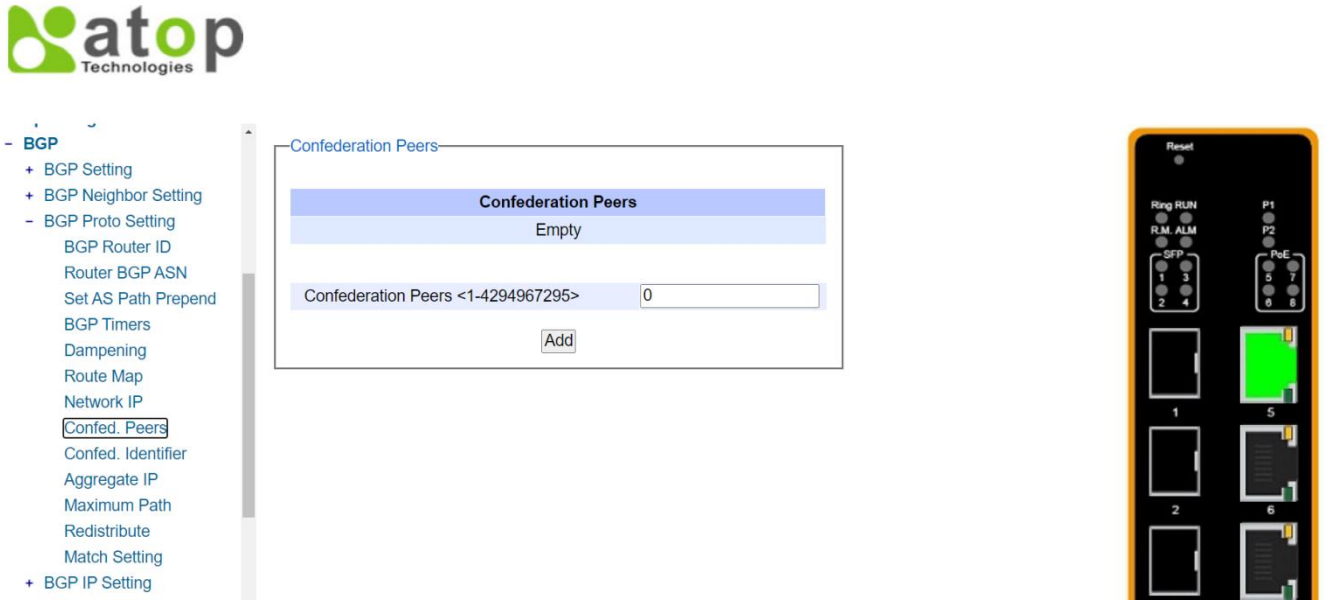


Figure 2.177 *Confed. Peers* Submenu inside the *BGP Proto Setting*

2.13.3.9 Confed. Identifier

This sub-menu of ***BGP Proto Setting*** is called ***Confed. Identifier***, as shown in Figure 2.178. In this option, the user can configure a BGP confederation identifier. In this option, only one field is needed to be filled here: C*onfederation Identifier.* In C*onfederation Identifier* field, the user can set routing domain confederation AS number, ranging from 1 to 4294967295. After the new information is keyed in, click the **ADD** button to take the effect.

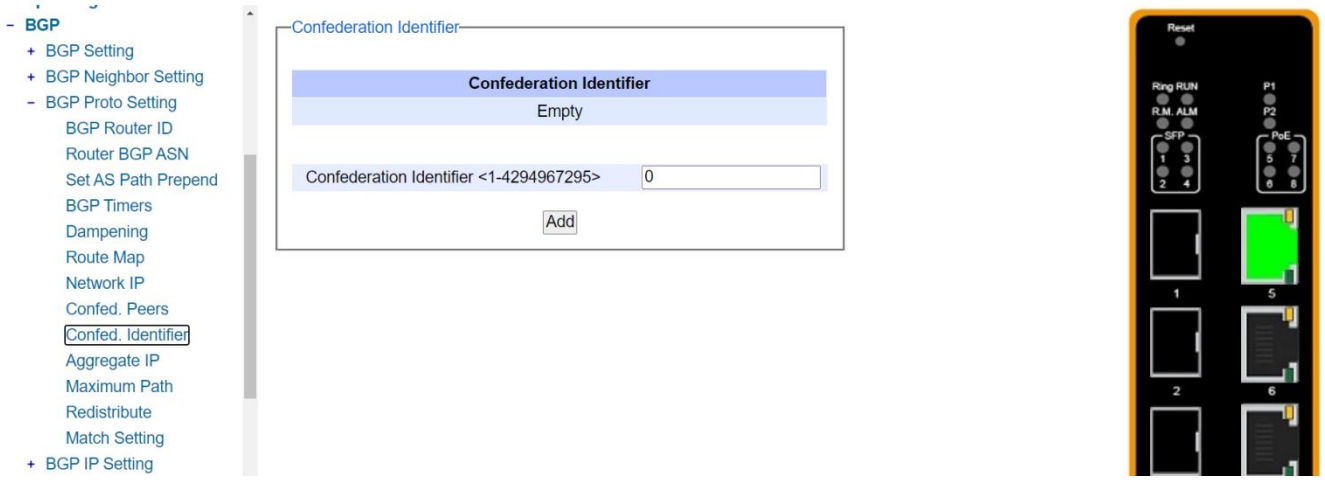


Figure 2.178 *Confed. Identifier* Submenu inside the *BGP Proto Setting*

2.13.3.10 Aggregate IP

This sub-menu of ***BGP Proto Setting*** is called ***Aggregate IP*** as shown in Figure 2.179. In this option, the user can add an aggregate route that can be advertised to BGP or BGP4+ neighbors. This command creates an aggregate entry in the BGP or BGP4+ routing table if the device learns, by any means, any routes that are within the range configured by the aggregate address/mask. In this option, three fields are needed to be filled and selected here: *Aggregate IP, Prefix,* and *List Type.* In *Aggregate IP* field, the user can specify the aggregate IPv4 address and mask. In the *Prefix* field, prefix of the aggreagate IP address can be entered here. In the *List Type* field, the user can select either Summary only or AS-Set from the drop-down options. In *Summary only* option, the user can filter more specific routes from updates. In *AS Set* option, the user can generate AS set path information. After the new information is keyed in, click the **ADD/Modify** button to take the effect.

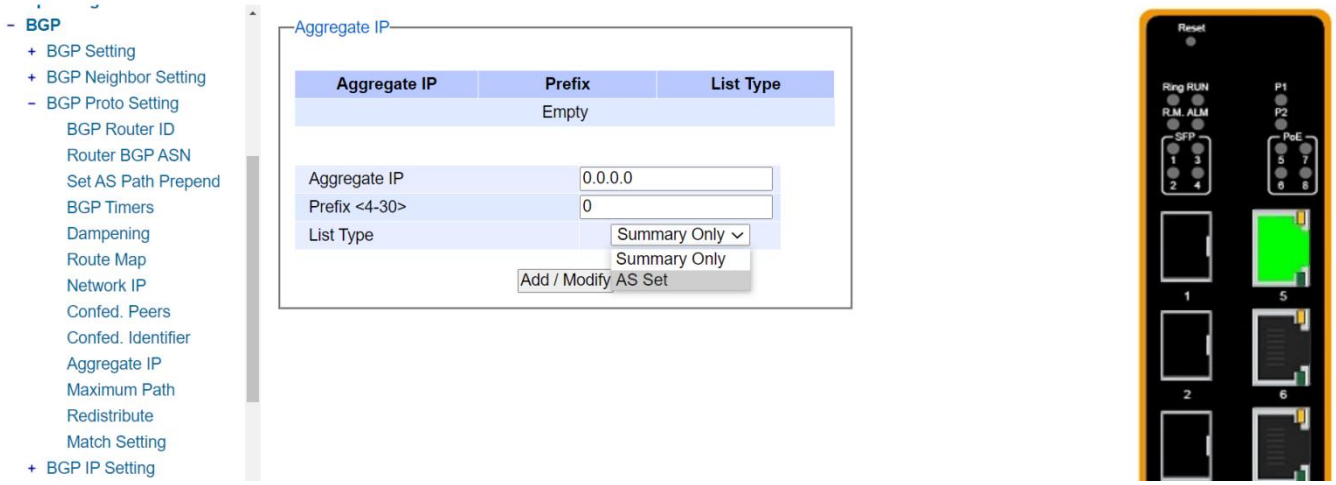


Figure 2.179 *Aggregate IP* Submenu inside the *BGP Proto Setting*

2.13.3.11 Maximum Path

This sub-menu of ***BGP Proto Setting*** is called ***Maximum Path*** as shown in Figure 2.180. In this option, the user can use this command to set the number of equal-cost multi-path (ECMP) routes for eBGP or iBGP. The user can install multiple BGP paths to the same destination to balance the load on the forwarding path. In this option, only one field is needed to be filled here: *Path Range.* In *Path Range* field, the user can specify the number of routes, 1. Note here that it supports only one route. After the new information is keyed in, click the **Update** button to take the effect.

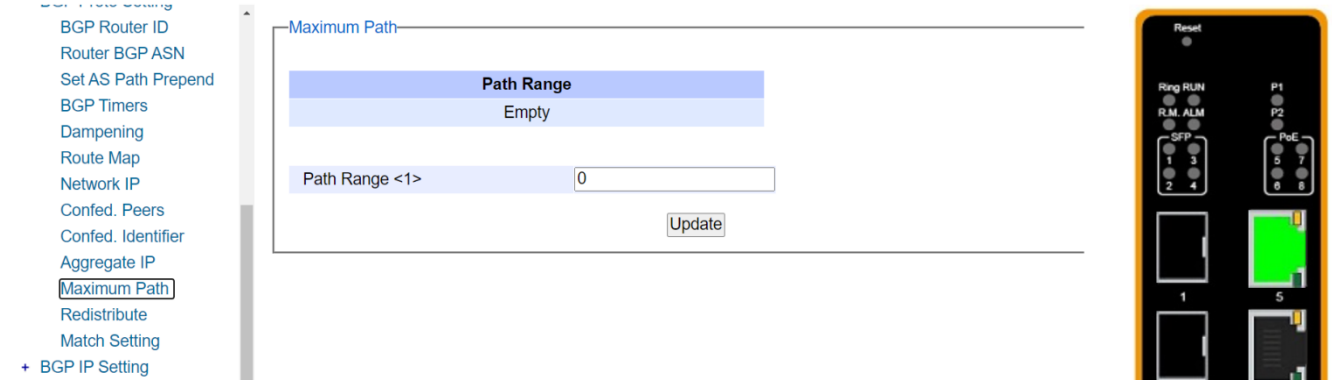


Figure 2.180 *Maximum Path* Submenu inside the *BGP Proto Setting*

2.13.3.12 Redistribute

This sub-menu of ***BGP Proto Setting*** is called ***Redistribute*** as shown inFigure 2.181. In this option, the user caninject routes from one routing process into a BGP or BGP4+ routing table. The user should configure the cluster-id in case of more than one route reflector per the BGP cluster. Usually, a cluster consists of one or more route reflectors and its clients, where each cluster is identified by the router-id of its single route reflector. Only one field is needed to be selected here: *Name*. There are five options to choose from: *Kernel, Connected, Static, Rip,and OSPF.* In *Kernel field,* theuser can specify the redistribution of connected routes for both BGP and BGP4. In *Connected* field, the user can specify the redistribution of connected routes for both BGP and BGP4+. In *Static* field, the user can specify

the redistribution of Static routes for both BGP and BGP4+. In *Rip* field, the user can specify the redistribution of RIP information for BGP or RIPng information for BGP4+. In *OSPF* field, the user can specify the redistribution of OSPF information for BGP or OSPFv3 information for BGP4+. After the new information is keyed in, click the **ADD/Modify** button to take the effect.

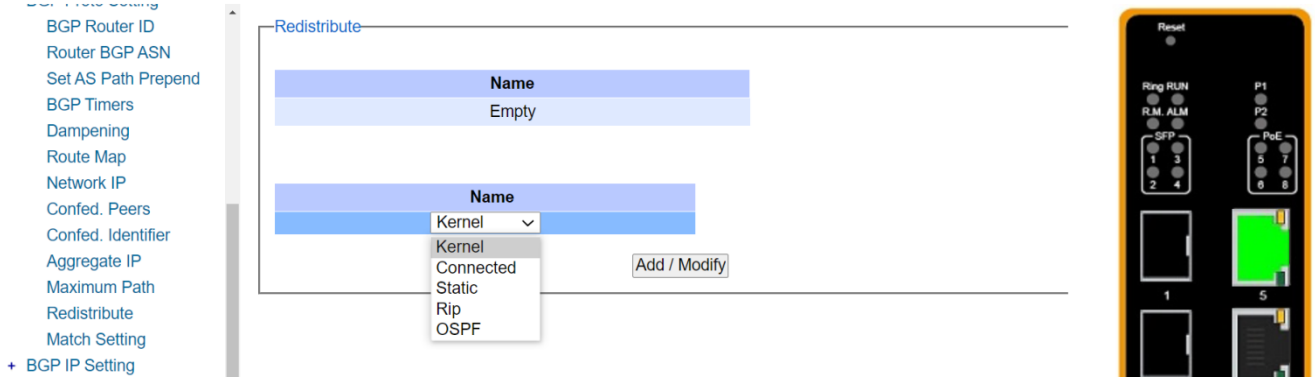


Figure 2.181 *Redistribute* Submenu inside the *BGP Proto Setting*

2.13.3.13 Match Setting

This sub-menu of ***BGP Proto Setting*** is called ***Match Setting***. There are three subsections under it: AS Path, Community Range, and Match Prefix List.

The first sub-menu of ***Match*** is ***AS Path***, as shown in Figure 2.182. In this option, the user can use this command to add an autonomous system (AS) path match clause to a route map entry. The user can specify the AS path attribute value or values to match by specifying the name of an AS path access list. To create the AS path access list, enter Global Configuration mode and use the ip as-path access-list command. In this option, only one field is needed to be filled here: *AS Path (WORD).* In *AS Path (WORD)*, the user can specify an AS path access list name. After the new information is keyed in, click the **ADD** button to take the effect.

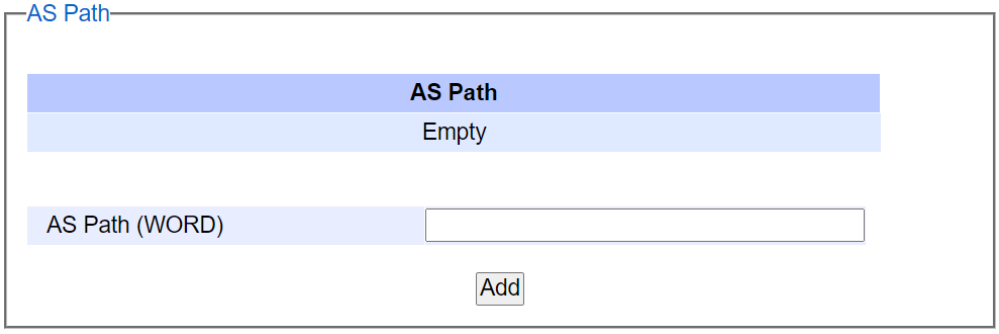


Figure 2.182 *AS Path* Submenu inside the *BGP Proto Setting -> Match Setting*

The second sub-menu of ***Match Setting*** is ***Community - > Range***, as shown in Figure 2.183. In this option, the user can add a community match clause to a route map entry by specifying the community values to match through a community list. To create the community list, go to BGP->Match-> IP Community List submenu. In this option, two fields are needed to be selected and filled here: *Mode* and *Range.* In *Mode* field, the user can select the community list number of two modes: Standard (1-99) and Expanded (100-199). In *Range* field, the user can input a number according to its mode. After the new information is keyed in, click the **ADD** button to take the effect.

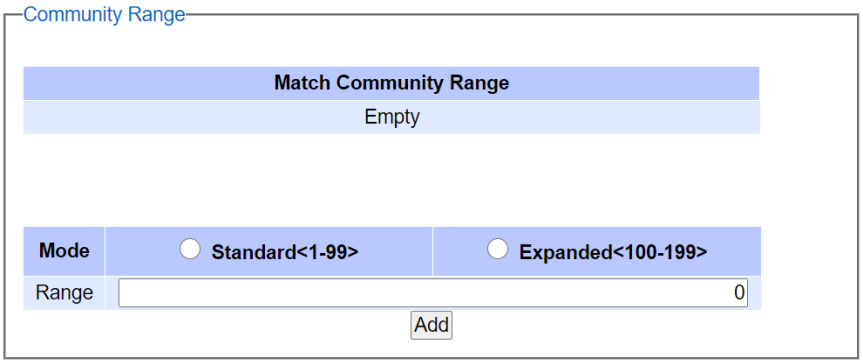


Figure 2.183 *Community Range* Submenu inside the *BGP Proto Setting* ->*Match Setting*

The third sub-menu of ***Match*** is ***Match Prefix List***, as shown inFigure 2.184. In this option, the user canadd an IP address prefix match clause to a route map entry. The prefix or prefixes can be specified to match by either one of the followings: 1) name of an access list, 2) name of a prefix list. Note here that the access list can be created by going to submenu BGP->Match-> IP Community List, and the prefix list can be created by going to submenu BGP->Match->Prefix List. In this option, only one field is needed to be filled here: *Prefix List WORD*. In *the Prefix List WORD* field, the user can use an IP prefix list to specify which prefixes to match. After the new information is keyed in, click the **ADD** button to take the effect.

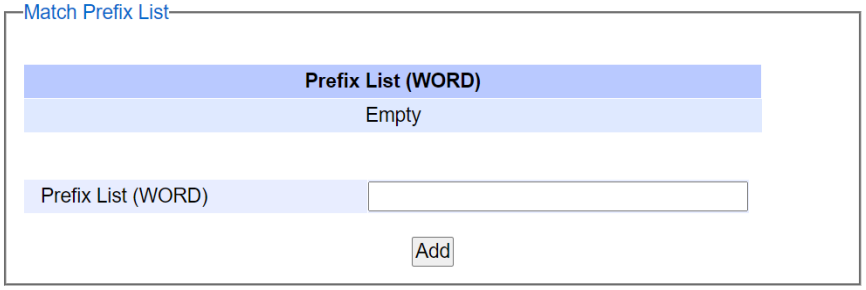


Figure 2.184 *Match Prefix List* Submenu inside the *BGP Proto Setting* ->*Match Setting*

2.13.4 BGP IP Setting

The fourth submenu under the **BGP** section is the **BGP IP Setting**. Under it, there are three submenus: IP Community List, IP Ext. Community List, and Prefix List, as shown inFigure 2.185.

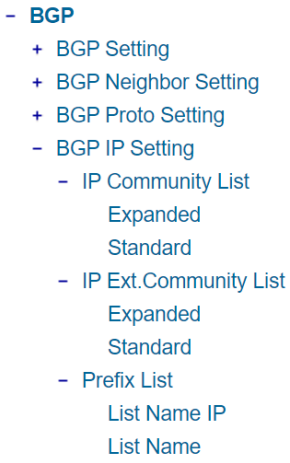


Figure 2.185Submenus inside the *BGP IP Setting*

2.13.4.1 IP Community List

This sub-menu of ***BGP IP Setting*** is called ***IP Community List***. There are two submenus under it: Expanded and Standard. The first sub-menu of ***IP Community List*** is ***Expanded***, as shown inFigure 2.186.

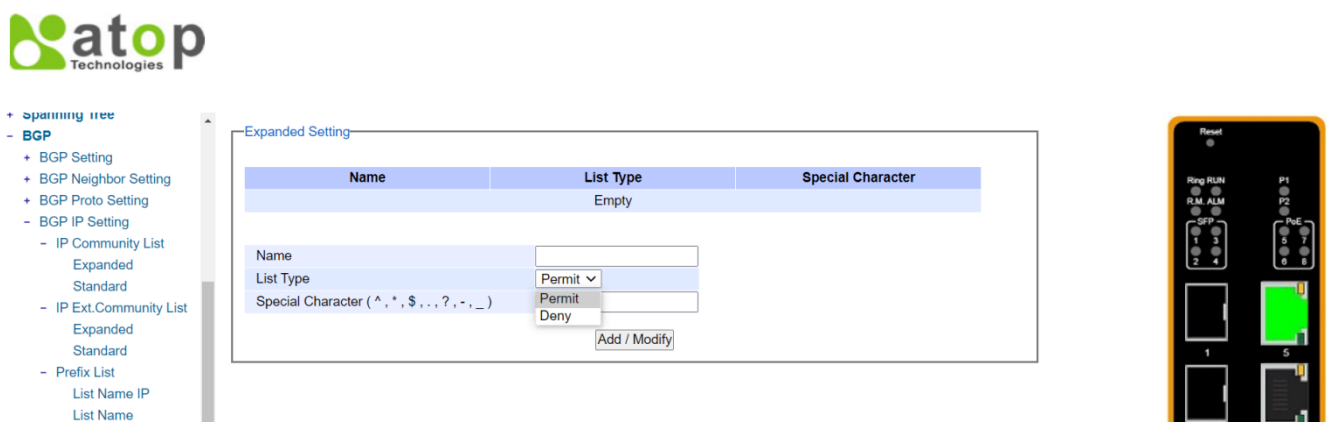


Figure 2.186*Expaned* Submenus inside the *BGP IP Setting* ->*IP Community List*

In this option, the user canadd an entry to an expanded BGP community-list filter. Three fields are needed to be filled and selected here: *Name, List Type,* and *Special Character (^, *, $, ., ?, -, _).* In *Name* field, the user can specify an expanded community list entry. In *List Type* field, the use can choose *permit* or *deny* from the dropdown menu to accept or reject the community. In *Speccial Character (^, *, $, ., ?, -, _)* field, the user can specify community attributes with regular expressions, where the details of each is shown in the table below. After the new information is keyed in, click the **Add/Modity** button to take the effect.

Table 2.42Meanings of the Special Character Field

Symbol	Meanings
^	Caret is used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign is used to match the end of the input string.
.	Period is used to match a single character (white spaces included).
*	Asterisk is used to match none or more sequences of a pattern.
?	Question mark is used to match none or one occurrence of a pattern.

Symbol	Meanings
_	Underscore is used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.
-	Hyphen Separates the end points of a range.

The second sub-menu of ***IP Community List*** is ***Standard***, as shown inFigure 2.187. In this option, the user canadd an entry to a standard BGP community-list filter. Three fields are needed to be filled and selected here: *Name, List Type,* and *Community.* In *Name* field, the user can specify a standard community list entry. In *List Type* field, the user can specify either *deny* (to reject) or *permit* (to accept). In the *Community* field, user has the following options to select: *AS:VAL, local-AS, no-advertise,* and *no-export*. *AS:VAL* specifies the valid value for the community number. This format represents the 32-bit community value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format. local-AS specifies routes not to be advertised to external BGP peers. *no-advertise* specifies routes not to be advertised to other BGP peers. *no-export* specifies routes not to be advertised outside of the autonomous system boundary. After the new information is keyed in, click the **Add/Modify** button to take the effect.

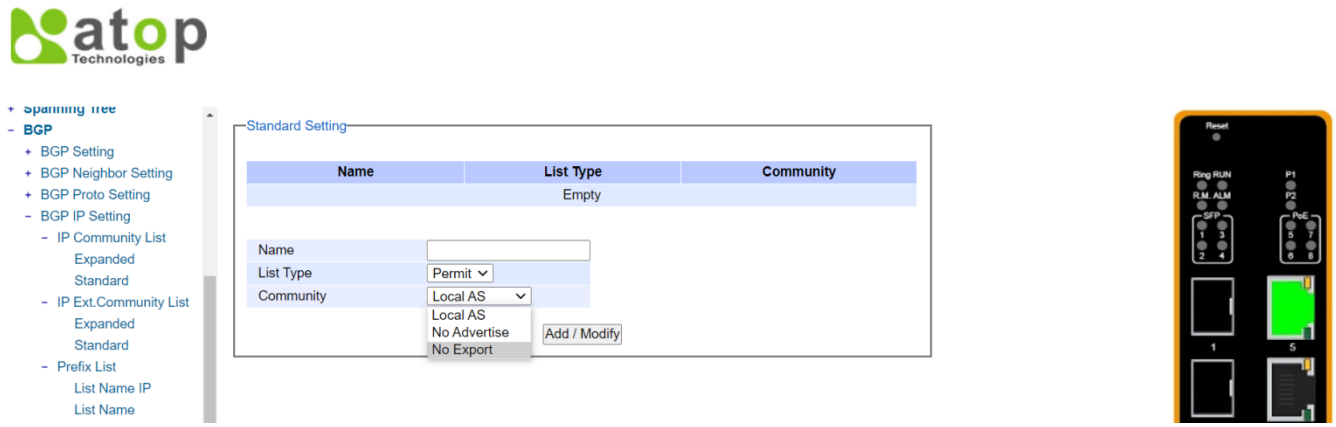


Figure 2.187Standard Submenu inside the BGP IP Setting -> IP Community List

2.13.4.2 IP Ext. Community List

This sub-menu of ***BGP IP Setting*** is called***IP Ext. Community List***. There are two submenus under it: Expanded and Standard. The first sub-menu of ***IP Ext. Community List*** is ***Expanded***, as shown inFigure 2.188.

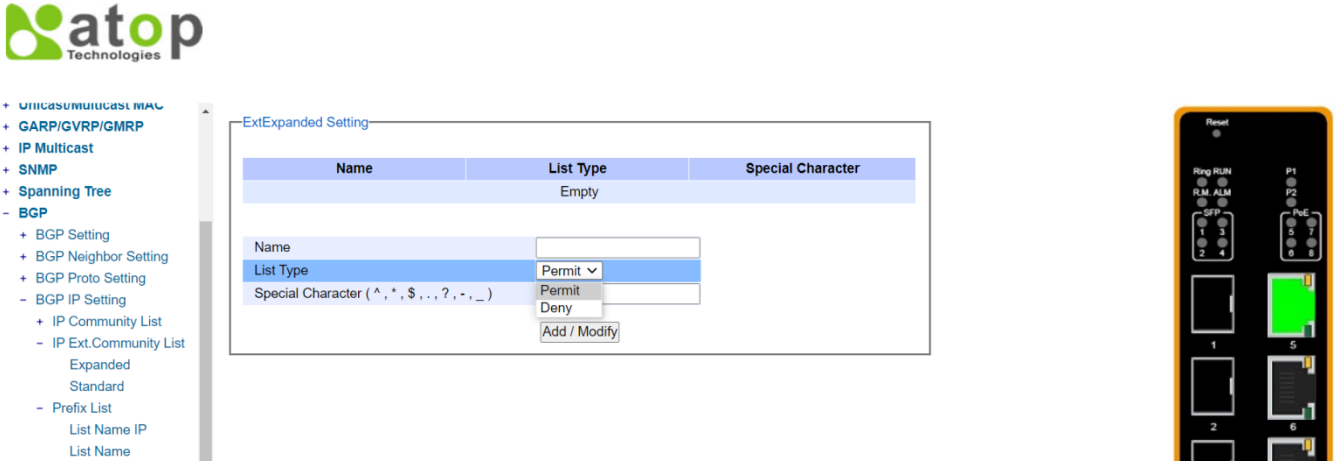


Figure 2.188*Expanded Submenu* inside the *BGP IP Setting ->IP Ext. Community List*

In this option, the user cancreate or delete an expanded extended community list. In this option, three fields are needed to be filled and selected here: *Name, List Type,* and *Special Character (^, *, $, ., ?, -, _).* In *Name* Field, the user can specify an expanded ext. community list entry. In *List Type* field, the user can choose either permit (to accept the extcommunity) or deny (to reject the extcommunity) options. In Special *Character(^, *, $, ., ?, -, _) field,* the user can specifyext. community attributes with regular expression, where the details of each is shown in the table below. After the new information is keyed in, click the **Add/Modity** button to take the effect.

Table 2.43Meanings of the Special Character Field

Symbol	Meanings
^	Caret is ssed to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match.
$	Dollar sign is used to match the end of the input string.
.	Period is used to match a single character (white spaces included).
*	Asterisk is used to match none or more sequences of a pattern.
?	Question mark is used to match none or one occurrence of a pattern.
_	Underscore is used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.
-	Hyphen Separates the end points of a range.

The second sub-menu of ***IP Ext. Community List*** is ***Standard***, as shown inFigure 2.189. In this option, the user cancreate and delete a standard extended community list. In this option, three fields are needed to be filled and selected here: *Name, List Type,* and *Community.* In *Name* field, the user can specify a standard extended community list entry. In *List Type* field, the user can select permit (accept the extended community) or deny (reject the extended community) options. In *Community* field, two options can be selected: *RT* or *SOO*. The user can choose *RT* to specify the route target of the extended community or *SOO* to specify the site of origin of the extended community. After the new information is keyed in, click the **ADD/Modify** button to take the effect.

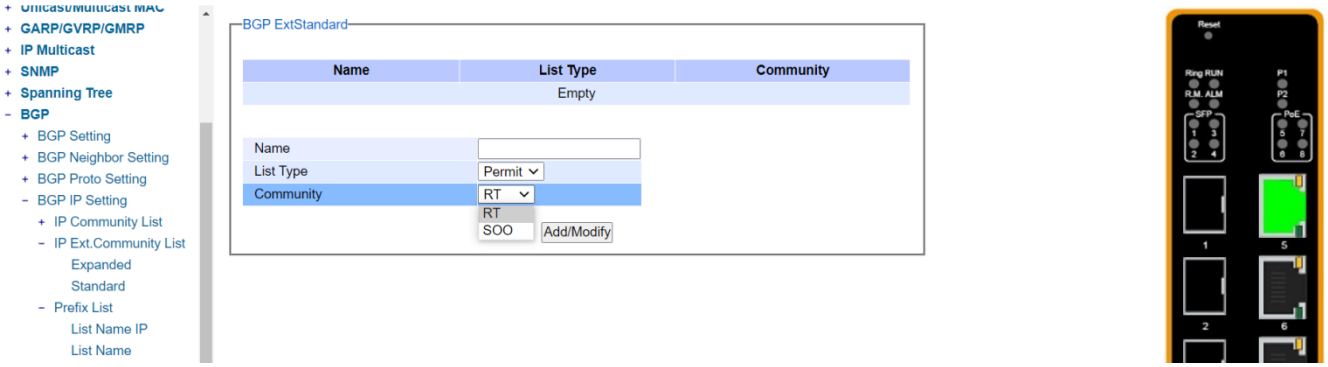


Figure 2.189 *Standard* Submenu inside the *BGP IP Setting -> IP Ext. Community List*

2.13.4.3 Prefix List

This sub-menu of ***BGP IP Setting*** is called ***Prefix List***. There are two submenus under it: List Name IP and List Name. The first sub-menu of ***Prefix List*** is ***List Name IP***, as shown inFigure 2.190. In this option, the user creates an entry for an IPv4 prefix list. In this option, five fields are needed to be filled and selected here: *Name*, *Sequence Number*, *List Type*, *IPv4 Address*, and *Prefix.* In *Name field*, the user can specify the name of a prefix list. In *Sequence Number* field, the user can specify the sequence number of the prefix list entry, which ranges from 1 to 429496725. In *List Type* field, the user can select permit or deny option from a drop-down menu to specify that the prefixes are included or excluded from the list. In *IPv4 Address* field, the user can specify an IPv4 address and a length of the network

mask in dotted decimal format A.B.C.D/M. In *Prefix* field, the user can specify prefix of an IPv4 address to be matched, ranging from 4 to 30. After the new information is keyed in, click the **ADD** button to take the effect.

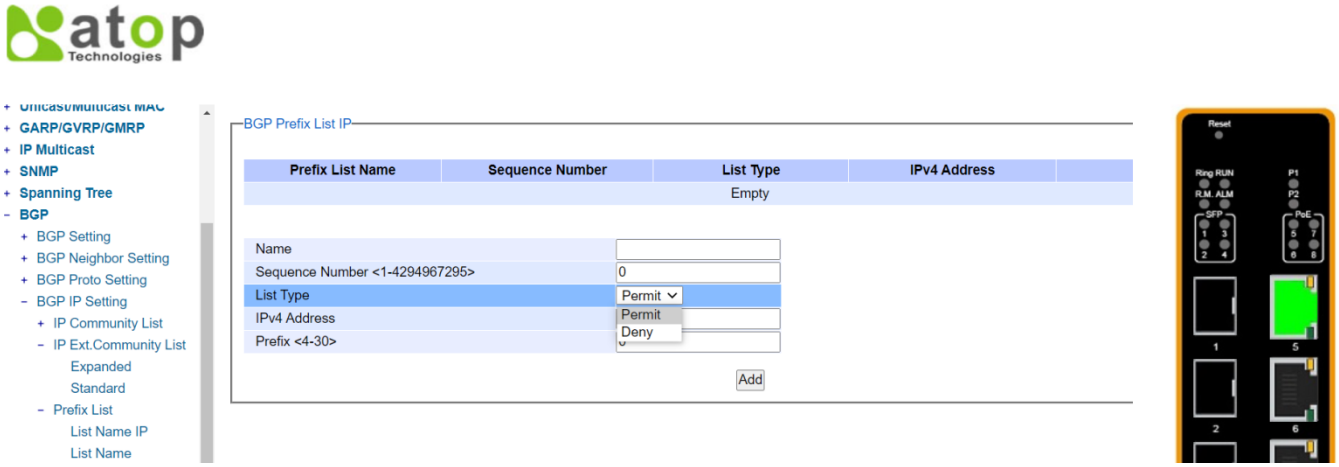


Figure 2.190 *List Name IP* Submenu inside the *BGP IP Setting -> Prefix List*

The second sub-menu of ***Prefix List*** is ***List Name***, as shown inFigure 2.191. In this web page, the user creates an entry for an IPv4 prefix list. Seven fields are needed to be filled and selected here: *Name*, *Sequence Number*, *List Type*, *IPv4 Address*, *Prefix*, *Prefix Listname*, and *Prefix Length.* In *Name field*, the user can specify the name of a prefix list. In *Sequence Number* field, the user can specify the sequence number of the prefix list entry, which ranges from 1 to 429496725. In *List Type* field, the user can select permit or deny option from a drop-down menu to specify that the prefixes are included or excluded from the list. In *IPv4 Address* field, the user can specify an IPv4 address and a length of the network mask in dotted decimal format A.B.C.D/M. In *Prefix* field, the user can specify prefix of an IPv4 address to be matched, ranging from 4 to 30. In *Prefix Listname* field, the user can specify either *ge* or *le to determine the minimum* or *maximum prefix length to be matched.* In *Prefix Length* field, the user can specify value of the prefix length to be matched, ranging from 0 to 32. After the new information is keyed in, click the **ADD** button to take the effect.

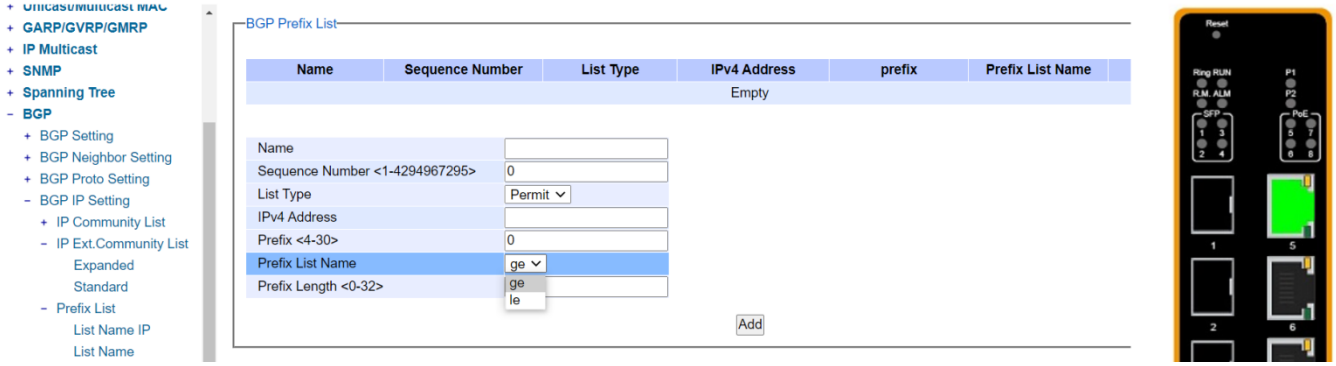


Figure 2.191 *List Name* Submenu inside the *BGP IP Setting -> Prefix List*

2.14 VLAN

A **V**irtual **L**ocal**A**rea **N**etwork (**VLAN**)is a group of devices that can be located anywhere on a network, but all devices in the group arelogically 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(seeFigure 2.192).

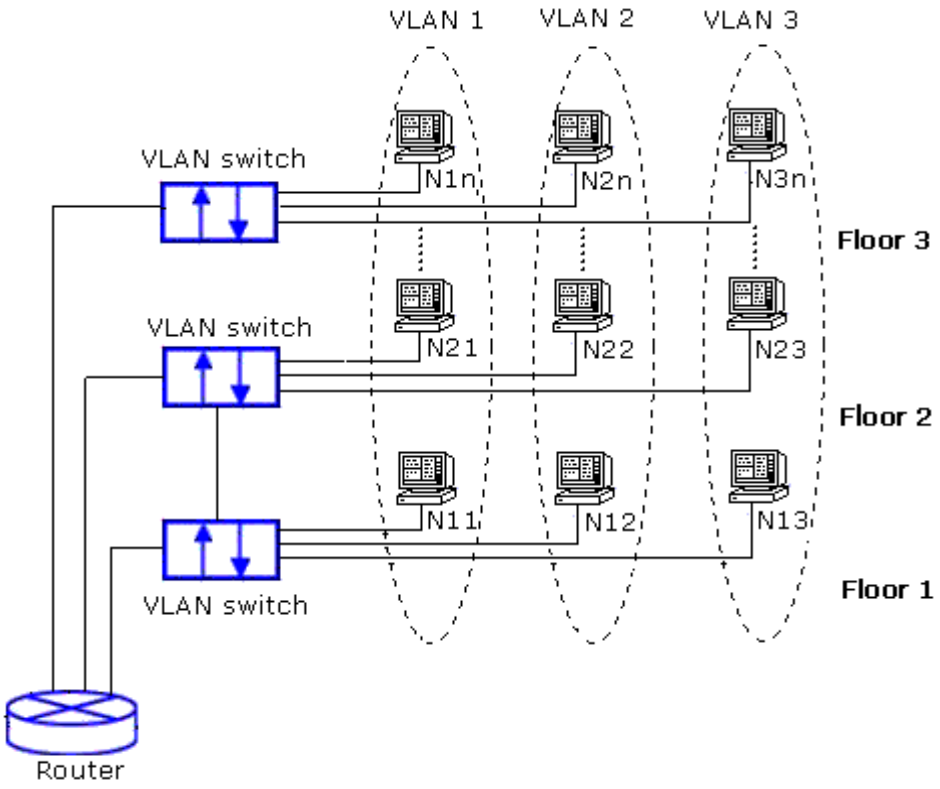


Figure 2.192Example of VLAN Configuration

Atop's managed switch RHG9XXX series provide six approaches to create VLAN as follows:

- **Tagging-based (802.1Q)VLAN**
- **Port-based VLAN**
- **MAC-based VLAN**
- **IP Subnet-Based VLAN**
- **Protocol-Based VLAN**
- **QinQ or Double Tagging-based VLAN**

Figure 2.193shows the drop-down menu under the VLAN section.

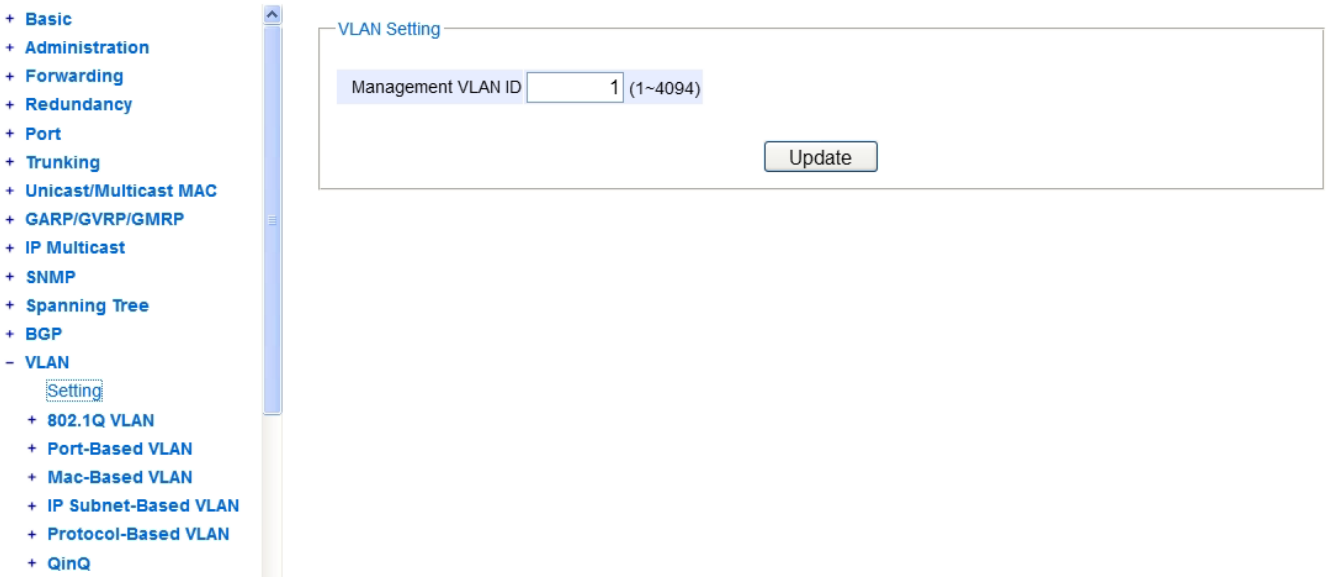


Figure 2.193 VLAN Dropdown Menu

2.14.1 VLAN Setting

The first menu under the VLAN section is the VLAN Setting. Here the management VLAN Identification number (ID)is configured based on the IEEE 802.1Q standard. The default value is VID =1. Note that the ID can be the number from 1 to 4096. If the users change the management VLAN ID to other number, please click the **Update** button to set it on the managed switch. Figure 2.194 depicts the VLAN Setting webpage. Table 2.44describes the VLAN Setting option.

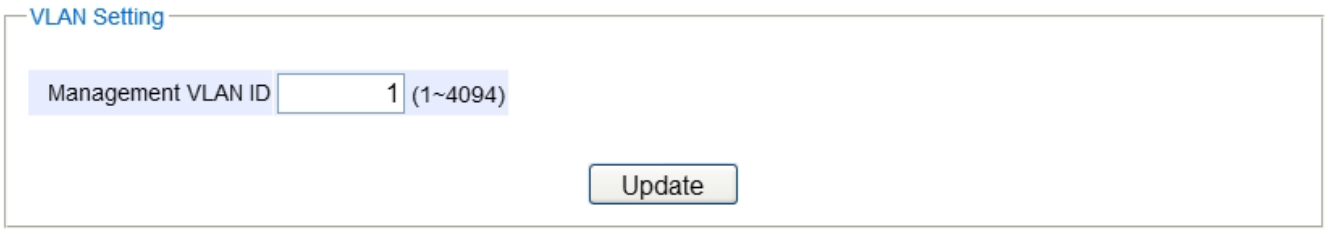


Figure 2.194 VLAN Setting Webpage

Table 2.44Description of VLAN Setting

Label	Description	FactoryDefault
Management VLAN ID	Configure the management VLAN ID that can be accessed this switch. Range from 1 to 4094.	1

2.14.2 802.1Q VLAN

Tagging-based (802.1Q)VLANis the networking standard that supports virtual LAN (VLANs)on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures for bridges and switches in handling such frames. The standard also contains provisions for a quality of service prioritization scheme commonly known as IEEE 802.1Q.

VLAN tagging frames are frames with 802.1Q (VLAN)tags that specify a valid VLAN identifier (VID).Whereas,

untagged frames are frames without tags or frames that carry 802.1p (prioritization)tags and only having prioritization information and a VID of 0. When a switch receives a tagged frame, it extracts the VID and forwards the frame to other ports in the same VLAN.

For a 802.1Q VLAN packet, it adds a tag (32-bit field)to the original packet. The tag is between the source MAC address and the EtherType/length fields of the original frame. For the tag, the first 16 bits is the Tag protocol identifier (TPID)field which set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame. This field is located at the same position as the EtherType/length field in untagged frames and is thus used to distinguish the frame from untagged frames. The next 3 bits is the Tag control information (TCI)field which refers to the IEEE 802.1p class of service and maps to the frame priority level. The next one bit is the Drop Eligible Indicator (DEI)field which may be used separately or in conjunction with PCP to indicate frames eligible to be dropped in the presence of congestion. The last 12 bits is the VLAN identifier (VID)field specifying the VLAN to which the frame belongs.

Under the 802.1Q VLAN menu, there are three submenus which are **Setting**, **PVID Setting**, and **VLAN Table** as shown in Figure 2.195.

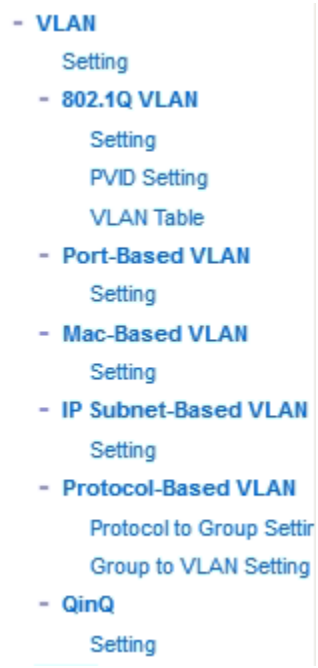


Figure 2.195 802.1Q VLAN Dropdown Menu

2.14.2.1 802.1Q VLAN Settings

Figure 2.196 shows the 802.1Q VLAN Setting webpage which allow the users to add new tagged-based VLAN to the managed switch. Please follow the following procedure to setting up the 802.1Q VLAN on the switch.

1. Go to**802.1Q VLAN,**then select**Setting**submenu.
2. Fill in appropriate Name, VID, Member Ports, and Tagged Ports as show in Figure 2.196. The description of each fields is summarized in Table 2.45. Then, click**Add/Modify**button. Note to select multiple **Member Ports** or multiple **Tagged Port**s, press and hold the **Ctrl** key while selecting multiple ports.
3. Go to **802.1Q VLAN's PVID Setting**described in the next subsection.
4. Choose the same ports,and enter PVID (which is the same as VID), see Figure 2.197.

To remove any of the VLAN from the 802.1Q VLAN setting, click the **Remove** button at the end of that particular VLAN record as shown in Figure 2.196.

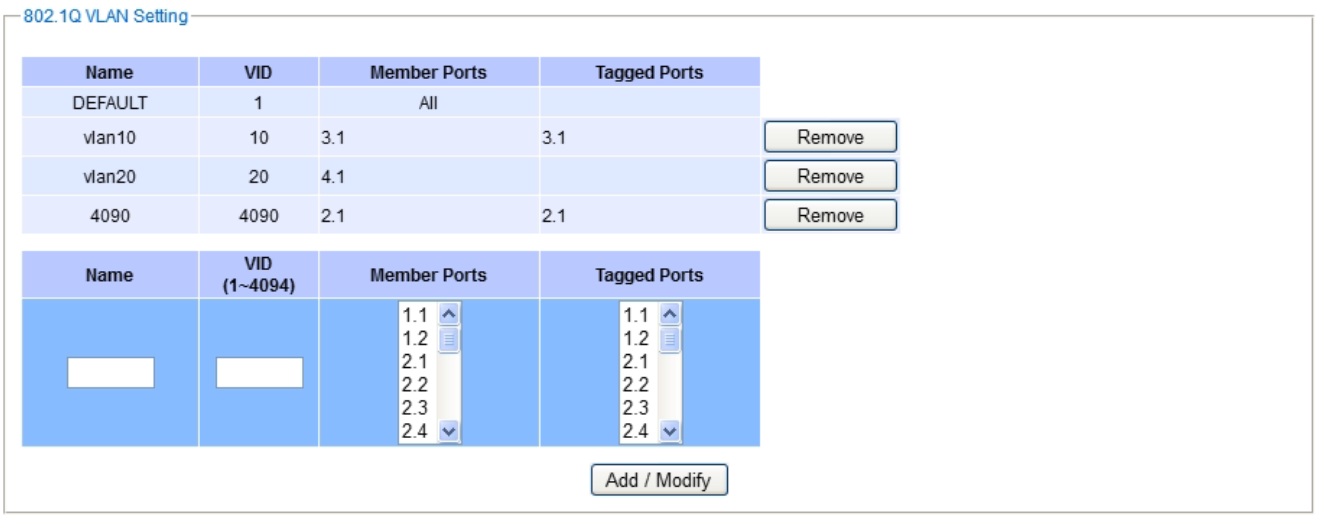


Figure 2.196 802.1Q VLAN's Setting Webpage

Table 2.45Setting Descriptions of 802.1Q VLAN Settings

Label	Description	Factory Default
Name	The VLAN ID name that can be assigned by the user.	Factory Default
VID	Configure the VLAN ID that will be added in static VLAN table in the switch.The VLAN ID is in the range 2~4094.	Dependent
Member Ports	Configure the port to this specific VID.	All Ports
Tagged Ports	Configure the port that outgoing packet is tagged or untagged. Selected:The outgoing packet is tagged from this port. Unselected:The outgoing packet is untagged from this port.	Dependent

*NOTE:Default settings only have VLAN ID on 1. To set VLAN ID to other value beside 1, users will have to assign ports to be in that VLAN group.

2.14.2.2 802.1Q VLAN PVID Settings

Each port is assigned a native VLAN number called the Port VLAN ID (PVID). When an untagged frame goes through a port, the frame is assigned to the port's PVID. That is the frame will be tagged with the configured VLAN ID defined in this subsection. Figure 2.197 shows the PVID Setting for 802.1Q VLAN where the upper table lists the current PVID assigned to each port. The users can configure the PVID by select either on or multiple ports (by clickingand holding the Ctrl key)and select the desired PVID value between 2 to 4094 from drop-down list. Please click Updatebutton to allow the configuration to take effect on the switch. Table 2.46 summarizes the PVID Setting's descriptions.

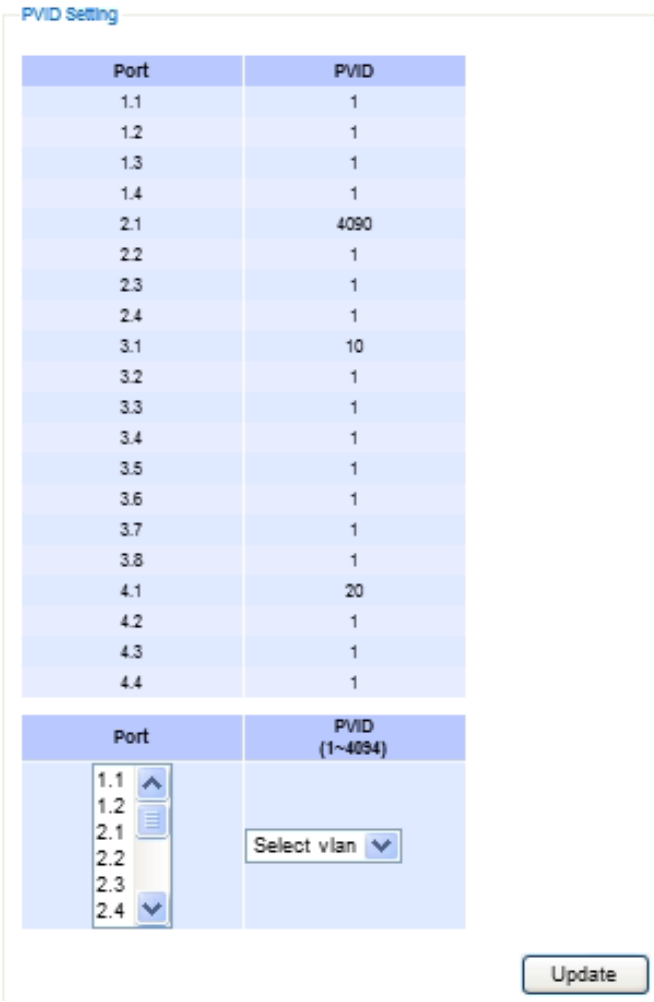


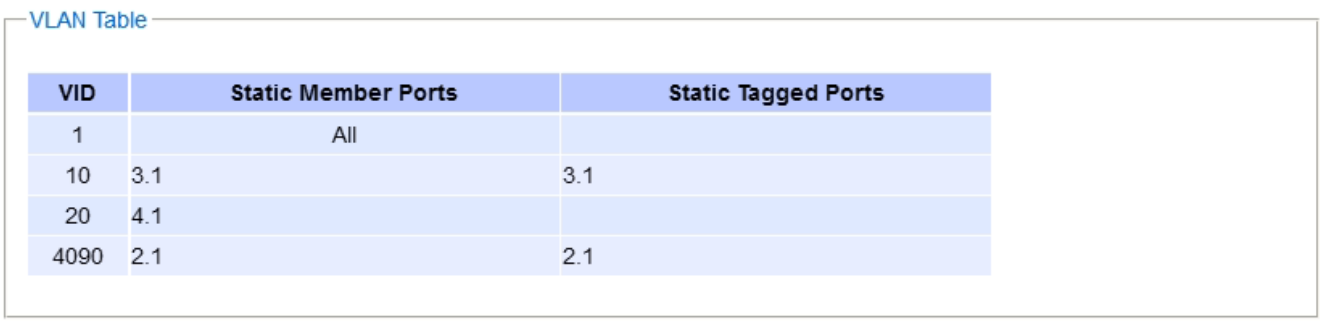
Figure 2.197 802.1Q VLAN PVID Setting Webpage

Table 2.46 Setting Descriptions of 802.1Q VLAN PVID

Label	Description	Factory Default
Port	Select specific port(s) to set the PVID value	-
PVID	Configure the default 802.1Q VID tag assigned to specific Port.The VLAN ID is in the range 1~4094.	1

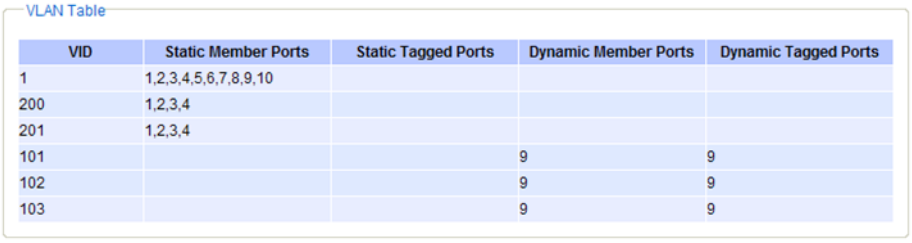
2.14.2.3 802.1Q VLAN Table

This webpage shown in Figure 2.198 displays the 802.1Q VLAN table which lists all the VLANs that are automatically and manually added/modified to the managed switch. Figure 2.199 illustrates examples of the static and dynamic VLAN information of each VID. Table 2.47 summarizes the descriptions of VLAN Table.


VLAN Table

VID	Static Member Ports	Static Tagged Ports
1	All	
10	3.1	3.1
20	4.1	
4090	2.1	2.1

Figure 2.198 802.1Q VLAN Table Webpage


VLAN Table

VID	Static Member Ports	Static Tagged Ports	Dynamic Member Ports	Dynamic Tagged Ports
1	1,2,3,4,5,6,7,8,9,10			
200	1,2,3,4			
201	1,2,3,4			
101			9	9
102			9	9
103			9	9

Figure 2.199 Example of 802.1Q VLAN Table

Table 2.47 Descriptions of 802.1Q VLAN Table

Label	Description	Factory Default
VID	Indicate the VLAN ID number	Dependent
Static Member Ports	Indicate the member ports to this VID. This entry is created by user.	All ports
Static Tagged Ports	Indicate the ports that outgoing packet is tagged or untagged. **Displayed**:The outgoing packet is tagged from this port. **Non-displayed**:The outgoing packet is untagged from this port. This entry is created by user.	Dependent
Dynamic Member Ports	Indicate the member ports to this VID. This entry is created by GVRP(discussed in Section 2.9.3).	Dependent
Dynamic Tagged Ports	Indicate the member ports that outgoing packet is tagged or untagged. **Displayed**: The outgoing packet is tagged from this port. **Non-displayed**: The outgoing packet is untagged from this port. This entry is created by GVRP(discussed in Section 2.9.3).	Dependent

2.14.3 Port-Based VLAN

Port-Based VLAN(or Static VLAN equivalent)assignments are created by assigning ports to a VLAN. If a device is connected to a certain port, the device will be assigned a VLAN to that specific port. If a user changes the connected port, a new port-VLAN assignment must be reconfigured for this new connection. To setup port-based VLAN, please follow the following steps:

1. Click on **Port-Based VLAN setting**pageas shown in Figure 2.200.
2. Select specific ports to be included in certain group by checking the corresponding box under the Member ports on particular row of port-based VLANs'Group ID. Note that if the users check the box under the Group ID column, all of the Member Ports will belong to that VLAN'sGroup ID.
3. Click on the **Update** button to allow the setting to take effect on the managed switch.

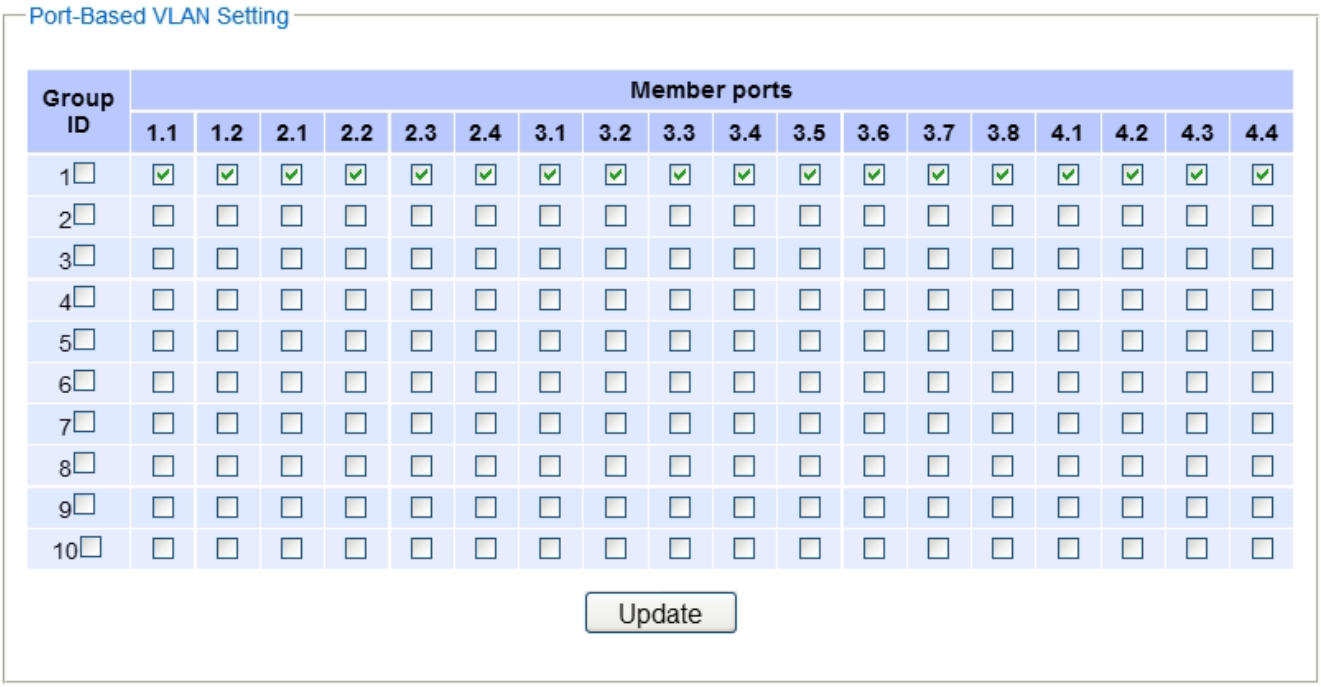


Figure 2.200 Port-based VLAN Setting Webpage

2.14.4 MAC-Based VLAN

The managed switch also supports the ability to assign a VLAN ID (VID)to an untagged packet based on the source MAC address. This can be set in this sub-menu as shown in Figure 2.201. There are maximum 512 entries in the MAC-based VLAN table (Source MAC address + VLAN ID)in the lower part of this webpage. If the users enter a duplicated MAC address into the MAC-based VLAN table, the old VLAN ID will be overwritten by the new VLAN ID. The VLAN ID range is between 1 to 4096. If the source MAC address of a packet is matched with any entry inside the MAC-based VLAN table here, the mapped VLAN ID will be added to the packet.

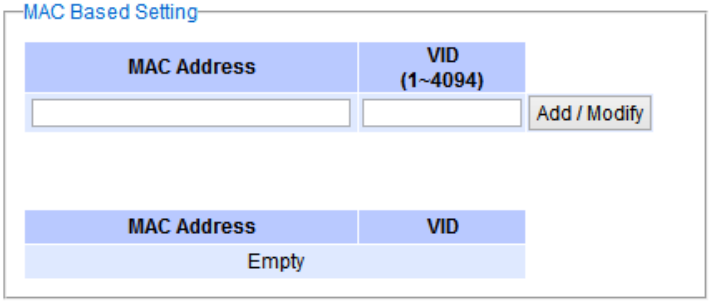


Figure 2.201 MAC-Based VLAN Setting Webpage

2.14.5 IP Subnet-Based VLAN

This sub-menu allows the user to assign a VLAN ID to an untagged packet based on the source IP address and the prefix length which is called IP subnet-based VLAN. Figure 2.202 shows the webpage where the users can enter the IP address, prefix length and VLAN ID (VID)for creating a VLAN based on its IP subnet. The list of existing IP subnet-based VLAN is shown in the lower part of the webpage. This feature support maximum of 64 sets (IP address +Prefix length + VLAN ID). The VLAN ID (VID)range is between 1 to 4096. This VLAN setup feature supports both IPv4 and IPv6. If a duplicated pair of IP address and prefix length is entered into the table, there will be an error message. The prefix length of IPv4 is 0 to 32 while the prefix length of IPv6 is 0 to 64.

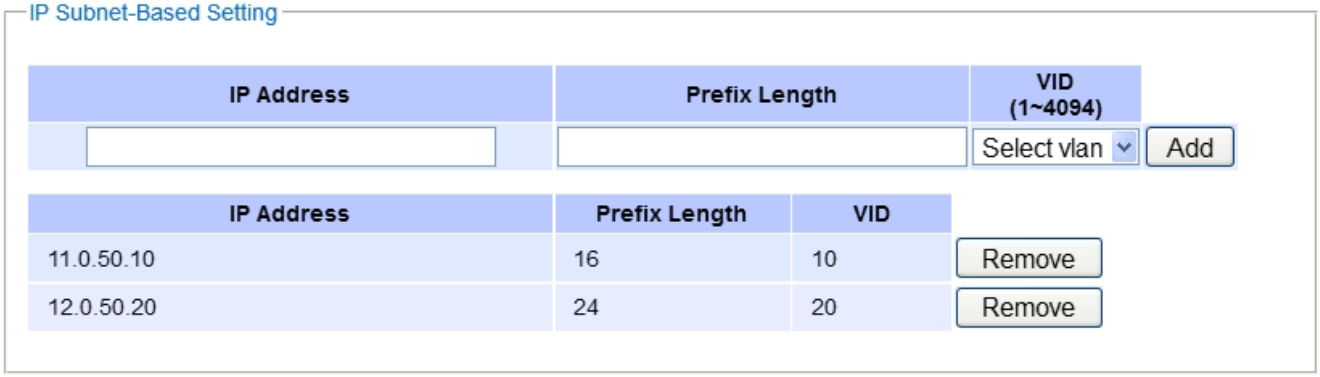


Figure 2.202 IP Subnet-Based VLAN Setting Webpage

2.14.6 Protocol-Based VLAN

For the protocol-based VLAN, the switch supports 3 Ethernet packet frame types: Ethernet II, 802.3 LLC, and 802.3 SNAP. It uses the EtherType field (Protocol IDin these frames to assign a VLAN ID for each untagged packet. There are two submenus for **Protocol-Based VLAN**: **Protocol to Group Setting** and **Group to VLAN Setting**.

2.14.6.1 Protocol to Group Settings

The users can add or modify the Group ID in this menu option, as shown inFigure 2.203 . Here, the maximum of 16 rules are supported. “Protocol Group Setting”is used to define the protocol rule and assign a unique ID (Group ID).The value of **Group ID** is between 1 to 2147483646. The **Frame Type** can be **Ethernet**, **SNAP**, or **LLC**. The “**Value**”field in the webpage is the EtherType (Protocol ID).

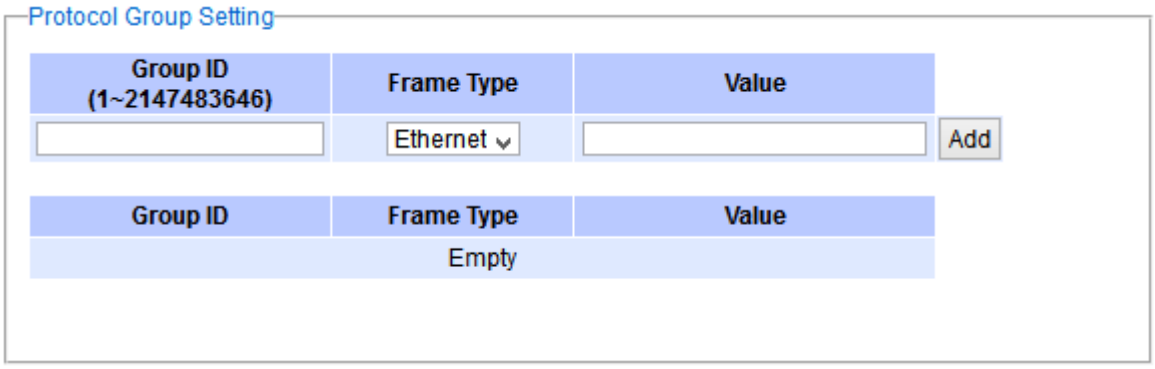


Figure 2.203 Protocol to Group Setting Webpage

2.14.6.2 Group to VLAN Settings

The users can add or modify **Group ID** and for each port or multiple ports in this menu option, as shown inFigure 2.204. “Group to VLAN Setting”is used to map the **Group ID**to a VLAN ID (**VID**). This will map the FrameType and EtherType to a VLAN ID.

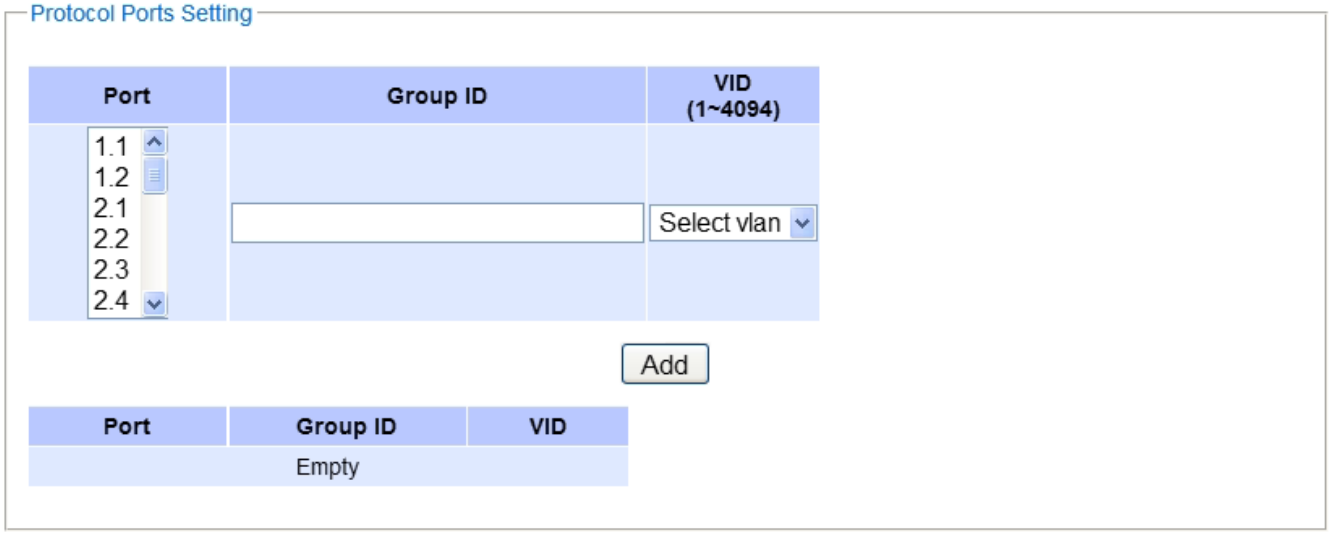


Figure 2.204 Group to VLAN Setting Webpage

2.14.7 QinQ

Originally the 802.1Q standard VLAN only allowed one VLAN tag appended in a packet. But the QinQ feature in this subsection allows two VLAN tags to be appended in a packet. The main purpose of the QinQ is for service providers to place additional VLAN tag as an external network identification and to keep the original customer's VLAN tag if existed.

To understand the operation of QinQ VLAN setting, we will use an example of a network where there are two buildings called Building 1 and Building 2 that has two departments called Department A and Department B of the same company on both buildings. Department A want use the VLAN2 (TPID =0x8100)for inside communication and Department B also want to use the VLAN2 (TPID =0x8100)for inside communication but they do not want to communicate with each other.

The network administrators can enable the QinQ VLAN feature or double tagging VLAN function in the company managed switches. If Building 1 has the following switches: A1(for Department A), B1 (for Department B), H1 (for Backbone network)and Building 2 has the following switches: A2 (for Department A), B2 (for Department B), and H2 (for Backbone network)then all of the switches can be configured as shown in Figure 2.205.

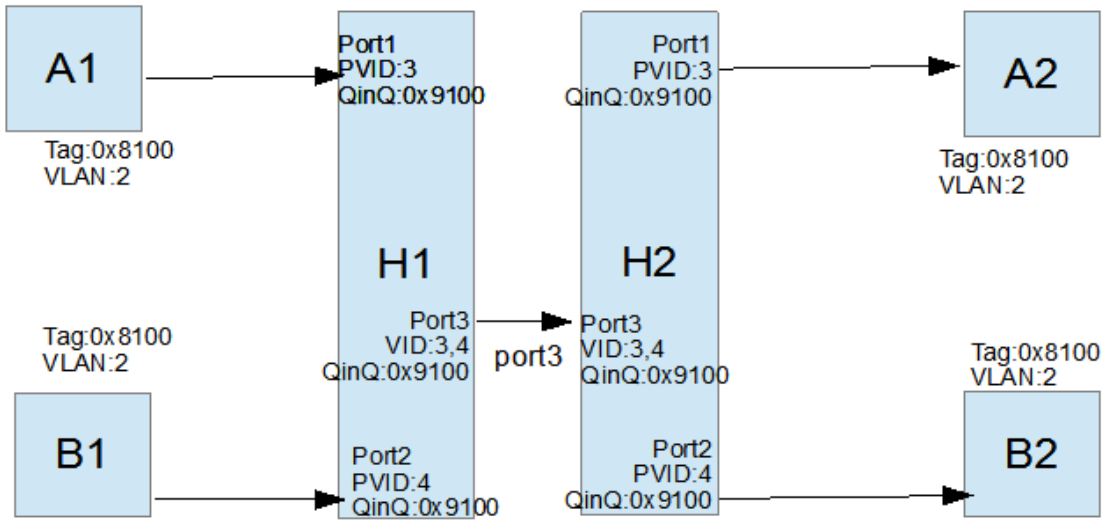


Figure 2.205 Example of QinQ Deployment

The operation of the network in Figure 2.205 based on QinQ VLAN setting rule can be described as follows.

1. Switch A1 and Switch B1 send some packets with VLAN tag (TPID=0x8100, VLAN ID=2)to H1.
2. The Switch H1 treats these received packets with VLAN tag (TPID=0x8100)as untagged packets because the receiving ports' QinQ TPID =0x9100. These packets will be inserted the second VLAN tags (TPID=0x9100, VLAN ID =PVID).
3. The Switch H1 will switch these packets to Port3 (VLAN ID=3 or 4 depending on the incoming port number from A1 or B1).
4. The Switch H2 receives these packets and switches them by the VLAN rule. The packets with VLAN ID 3 will be sent to Port 1 and the packets with VLAN ID 4 will be sent to Port 2.
5. Before Switch H2 sends these packets out from Port 1 or Port 2, the VLAN tags (TPID=0x9100, VLAN ID=3 or 4)will be removed from these packets.

Figure 2.206 shows the QinQ Setting webpage where the QinQ function can be enabled for each port on the managed switch. When checking the corresponding enabled box behind each port, the TPID field will become active. The default TPID is set to 0x8100 which means that the QinQ feature is disable. To enable the QinQ for a port, the users need to set the TPID value. In general, it should be set to 0x9100 which must be different from the original tag's 0x8100as described in Section 錯誤! 未知的選項引數。. The TPID value should be between 0x0000 to 0xFFFF. When setting a trunk port with QinQ, it is not allowed each physical port with different QinQ setting. This means that the QinQ enabled fields and TPID fields of all physical ports in a trunk port must be the same.

The QinQ setting rule is summarized as follows:

- For ingress ports and egress ports, they use the TPID field to decide whether a packet is being with a VLAN tag or not.
  - A packet is untagged (without VLAN tag)if its TPID field is not the same as the TPID that we set for the port in the QinQ configuration.
  - A packet is tagged (with VLAN tag)if its TPID field is the same as the TPID that we set for the port in the QinQ configuration.
- Either tagged packet or untagged packet are processed by the general VLAN rule to tag a packet, untag a packet, or keep the same packet, and do the switching.
- When a packet is tagged with a VLAN tag. The tag's TPID is from the input port's QinQ setting and the tag's VLAN ID is from the input port's PVID setting.

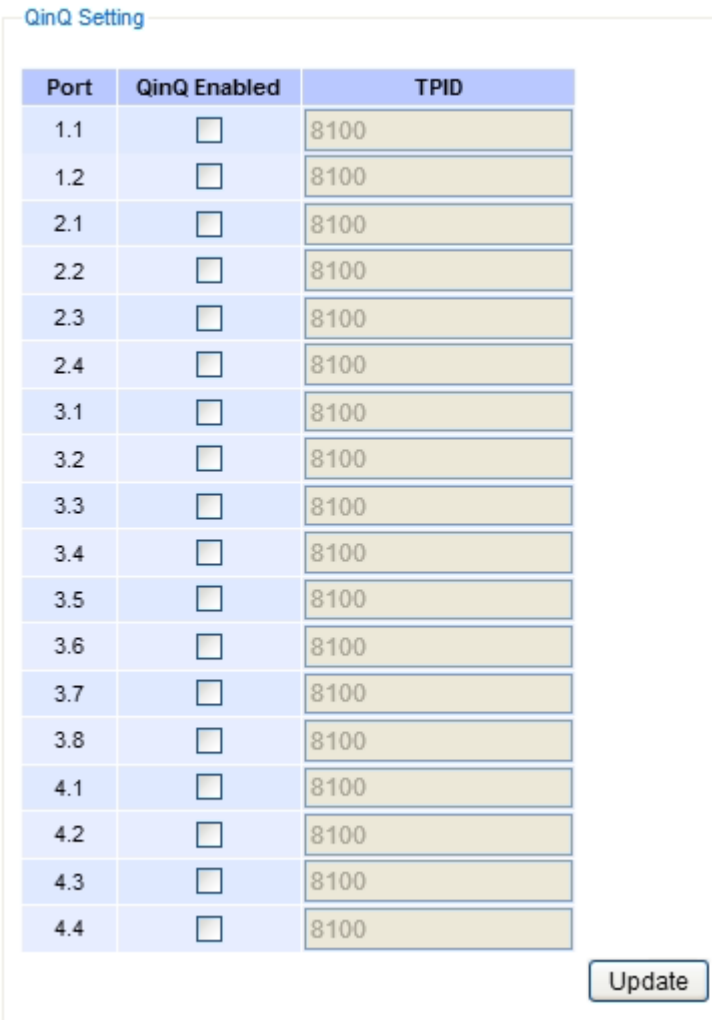


Figure 2.206 QinQ Setting Webpage

After finish setting the QinQ feature for any of the port, please click the **Update** button to allow the setting take effect on the managed switch.

2.15 VRRP

Virtual Router Redundancy Protocol (VRRP) (RFC 3768) enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts. The VRRP routing platforms share the IP address corresponding to the default route configured on the hosts. At any moment, one of the VRRP routing platforms is the master (active) and the others are backups. An Example of VRRP configuration is depicted in Figure 2.207. If the master router fails, one of the backup routers will become the new master router.The master router provides a virtual default routing platform and enables traffic on the LAN to be routed without relying on a signle routing platform. Using VRRP, a backup router can take over a failed default (master) router within a few seconds. This is performedautomatically with the minimum required VRRP traffic and without any interaction with the hosts.

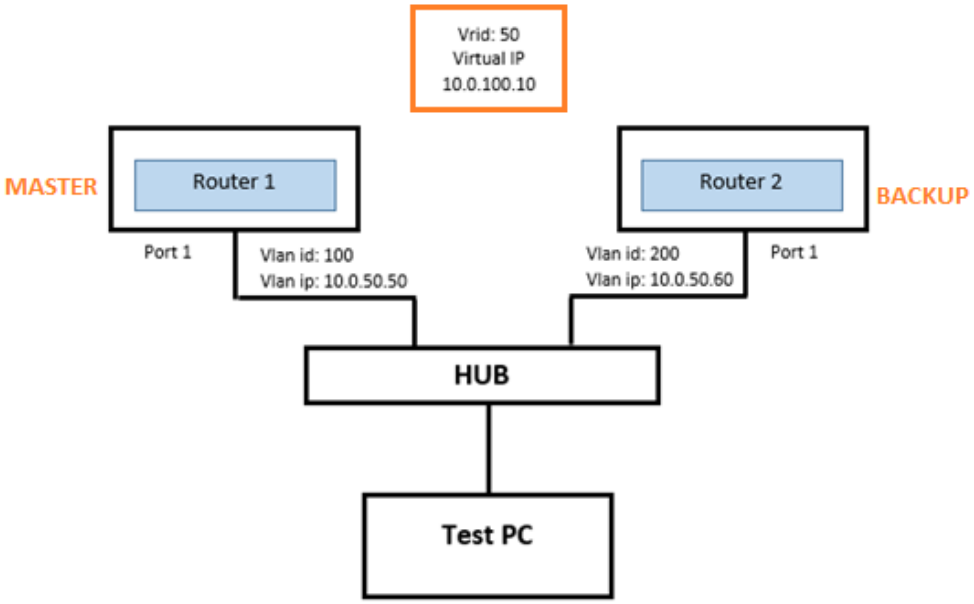


Figure 2.207 Overview of the VRRP

Figure 2.208shows the dropdown menu for VRRP section on the RHG96XX L3 managed switch. The VRRP menu consists of the following options: VRRP, Setting, and Restart.These menus will allow the user to check the status of VRRP whether itis enabled or disabled, to configure the VRRP Virtual Router IDs and Virtual Interfaces, and to restart the VRRP.

Figure 2.208VRRP Dropdown Menu

2.15.1 VRRP

The VRRP main page as shown in displays the current status of VRRP under the **Running Status** box. If the VRRP is enabled and running, this page will allow the user to disable/stop the VRRP by clicking on **Disable** button. If the VRRP is disabled/not running, this page will allow the user to enable/run the VRRP by clicking on **Enable** button.

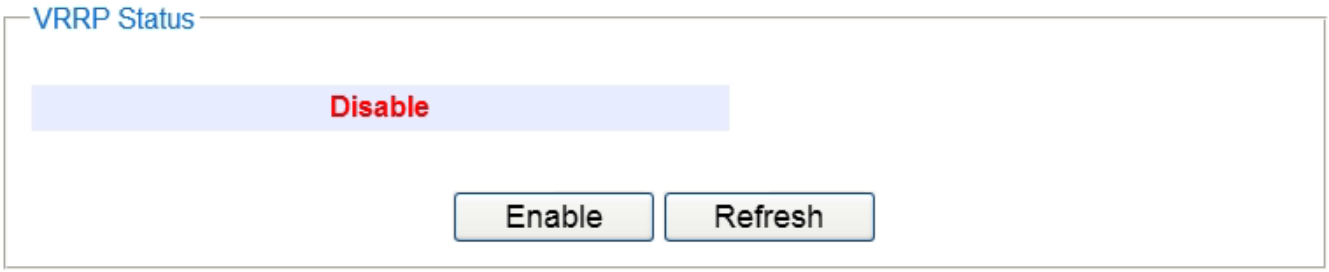


Figure 2.209 VRRP Running Status

2.15.2 Setting

In this VRRP's**Setting**web page, the user can configure the VRRP by adding new **Virtual Router**, adding new **VRRP Virtual interface** and modifying any **Current VRRP Settings**. Figure 2.210showsthe three boxes on the **Setting** web page.

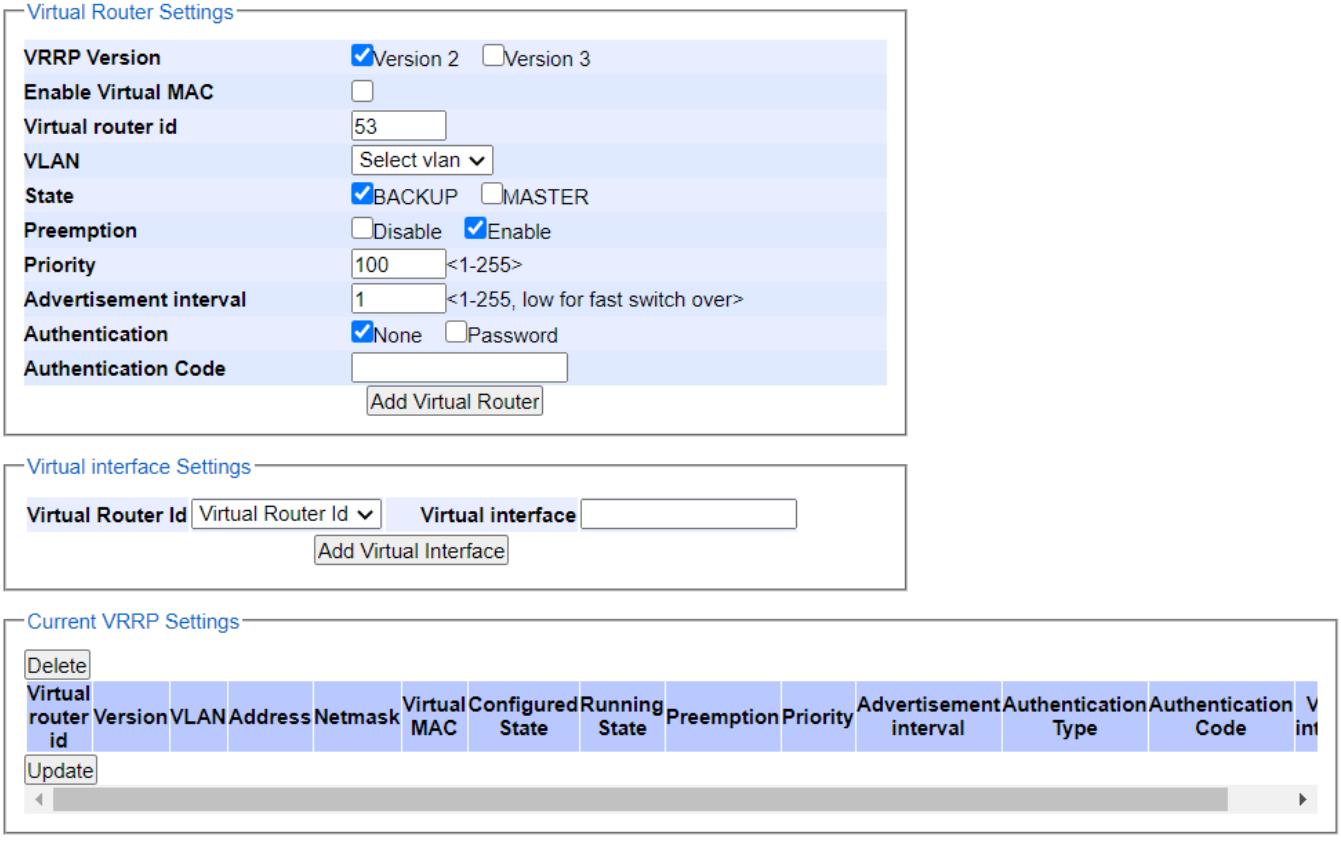


Figure 2.210Setting in VRRPMenu

To add the virtual router, first the user needs to configure a VLAN with an IP interface. You can select either VRRP Version 2 or Vertion 3 from the check boxes in the first option. Then the user has an option to select the **Enable Virtual MAC** checkbox and can proceed to enter the **Virtual router id** (VRID). Note that the VRID is an 8-bit number which can be from 1 to 255. Then, exisiting **VLAN** ID can be selected from the dropdown list on the next option and can be the number in between 1 to 4096. Next the user can assign the **State** of the virtual router whether it is a **Master** or a **Backup** by choosing from the check boxes. Next, the **Preemption** option can be selected as either **Disable** or **Enable**. This option allows a backup router to preempt a master router. Next the **Priority** is another 8-bit number indicate the priority value of the configured virtual router. The higher values represent the higher priority. VRRP routers configured as backup router must use priority values between 1 to 254. The default priority value for VRRP routers backing up a virtual router is 150. The priority value 255 is the highest priority. The priority value of

0means that the master router does not want to participate. Next the **Advertisement interval** is the time inverval in seconds and the default value is 10 second. It is also 8-bit number which means the interval can be between 1 to 255 seconds. Finally, the last two options are the **Authentication Type** and **Authentication Code**. The VRRP's **Authentication Type** can be either **None** or **Password** which can be selected from the check boxes. The**PasswordAuthentication Type** means that the VRRP will use 8 characters of plain text as **Authentication Code**. Thus, the user must enter the **Authentication Code** option as a string of 8 bytes. If the string is shorter than 8 bytes, the remaining space must be cleared to zero. When no user preferences are specified, the default values of the above options will be used. After entering all the required parameters, please click on the **Add Virtual Router** button.

The next step is to add a **Virtual Interface** to the **Virtual Router ID**. The user can select the desired **Virtual Router ID** from the dropdown list and then enter the IP address in the field behind the **Virtual Interface** as shown in the **VRRP Virtual Interface** box in Figure 2.211. Note that the **Virtual Router ID** can be created as described in the previous paragraph. Then, clicking on the **Add Virtual Interface** button to finish the setting.

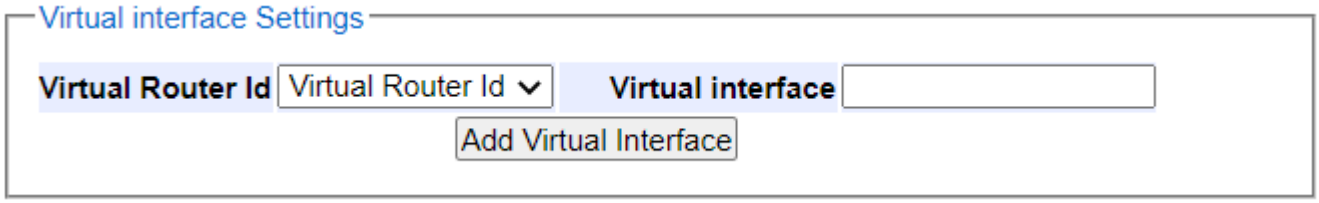


Figure 2.211 VRRP Virtual Interface Box under VRRP's Setting

The last box at the bottom of the VRRP's **Setting** web page is the **current VRRP Settings** as shown inFigure 2.212 and Figure 2.213. Inside the box, it is a table listing all existing virtual router id configured in the RHG96XX. Each entry comprises the following columns: **Virtual router id**, **VLAN**, **Address**, **Netmask**, **Configured State**, **Running State**, **Preemption**, **Priority**, **Advertisement interval**, **Authentication Type**, **Authentication Code**, and **Virtual Interface**.

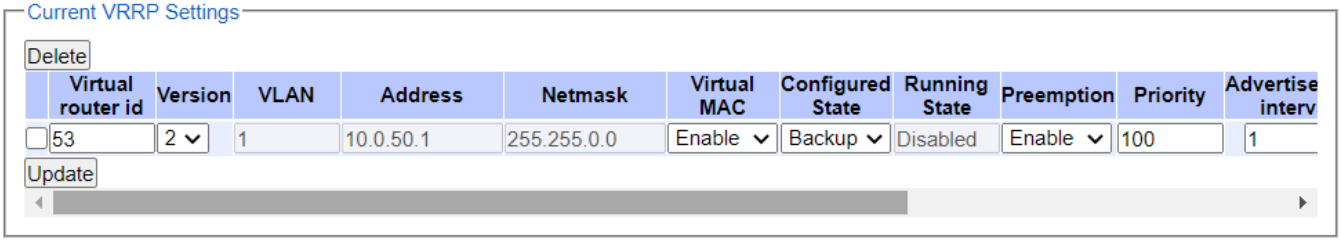


Figure 2.212 Setting in VRRP Menu after Adding Virtual Router ID (Front part)

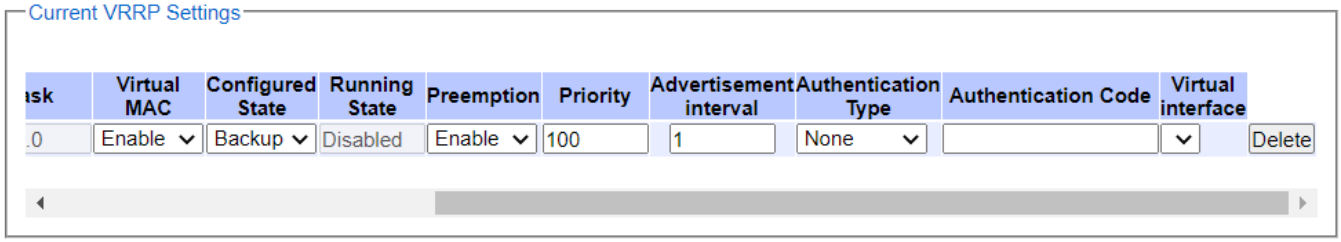


Figure 2.213 Setting in VRRP Menu after Adding Virtual Router ID (Ending part)

To update or delete an existed entry, the checkboxin the front (before virtual router ID) must be selected first, before clicking on the **Update** button on the front of the entry or **Delete** button on the back of the entry. The user canperform the following instructions to update or delete some values in the existing entry.

- The **Priority** or the **Advertisement interval** can be modified by keying in the new values and clickingon the "**Update**" button on the bottom front.
- The **Configured state** and the **Preemption** can be modified by selecting value from the drop-down menu and clicking on the"**Update**" button.

- The **Authentication type** can be modified by selecting the value from the drop-down menu while the value ofthe **authentication code**can be modified by entering in a new string of 8 charactersand clicking on the "**Update**" button.
- The **Virtual Interface** can be deleted by selecting the IP Address and clicking on the "**Delete**" button on the very right end of the entry.
- The **VRRP Virtual Router ID** can be deleted by selecting Virtual Router ID entry and clicking on the"**Delete**" button.
- The **VLAN**ID can only be modified to anew value if a new VLAN is already created.

2.15.3 Restart

VRRP needs to be restarted for any change in VRRP configuration to take effect.Figure 2.214 displays the **Restart** button in **VRRP Restart** web page.Clicking on the**Restart** button to restart VRRP.

Figure 2.214 Restart in VRRP Menu

2.16 DHCP Server

The user can set up a DHCP (Dynamic Host Configuration Protocol) server inside the RHG96XX industrial L3 managed switch. Multiple VLANs (Virtual Local Area Networks) can be configured as depicted in Figure 2.215. For each VLAN, the DHCP server's setting can support two DNS (Domain Name Server) servers, two Gateways (routers) and two NetBIOS servers. Inside each VLAN, the user can configure multiple dynamic IP address ranges and a static IP address for a specific MAC address.

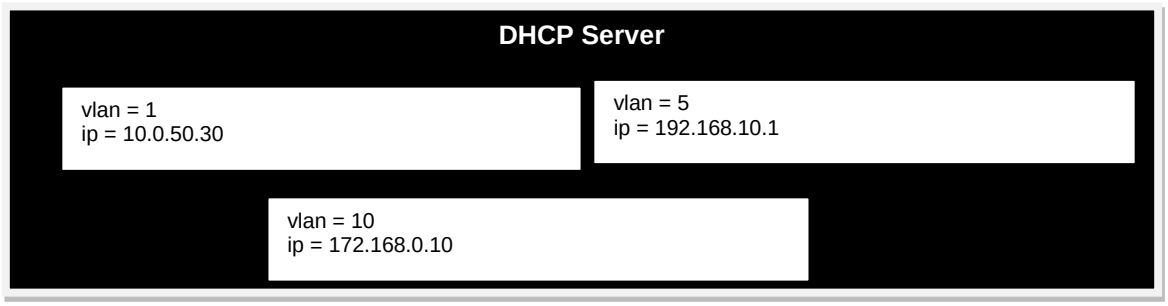


Figure 2.215Multiple VLANs for a DHCP Server

Figure 2.216shows the dropdown menu for **DHCP Server**section on the managed switch, which consists of **Setting**, **Clients**, and **Restart** submenus.

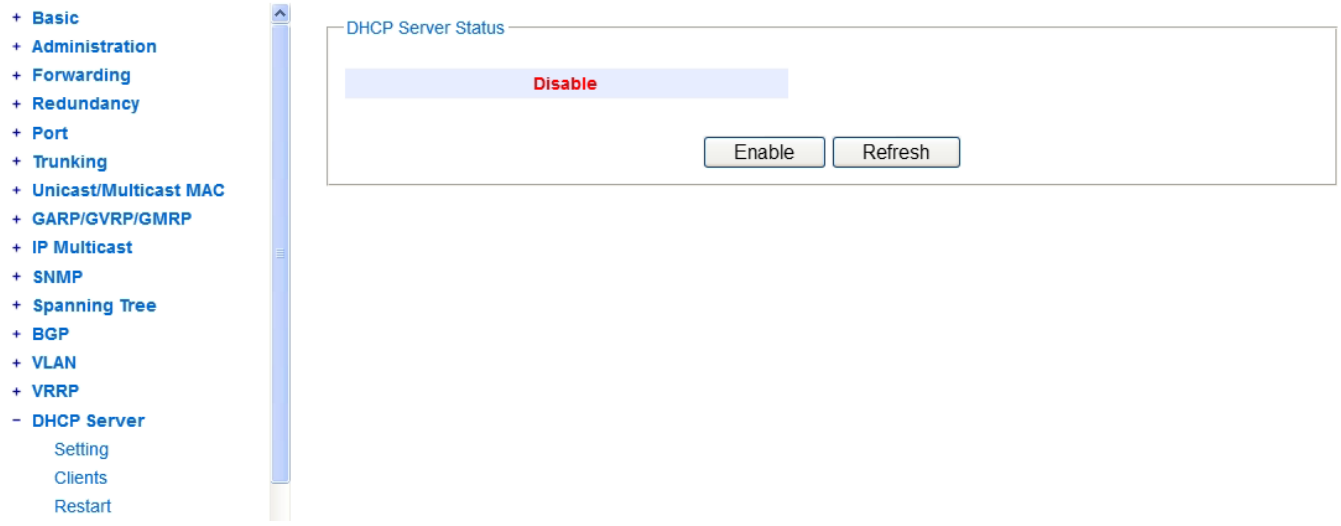


Figure 2.216DHCP Server Dropdown Menu

Figure 2.217shows the **DHCP Server**'s current status. If the DHCP server is enabled and running, the user can disable/stop the DHCP server by clicking on the **Disable** button below the **Running Status** box. Otherwise, if the DHCP server is disabled/not running, user can enable/run the DHCP server by clicking on the **Enable** button below the **Running Status** box. Note that the DHCP Server need to be configured in the next subsection before the user can enable the DHCP Server here.

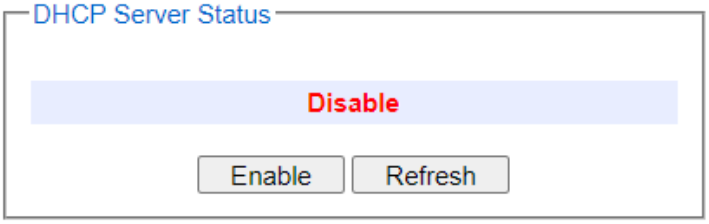


Figure 2.217Status of theDHCP Server

2.16.1 Setting

In **Setting** dropdown submenu, the DHCP server inside the RHG96XX can be configured. As described earlier, each **VLAN** can configured with **Lease Time**, two **Domain NameServers**, two **Gateways**, and two **Netbios Servers** as shown in Figure 2.218. Note that the **Lease Time** is the duration of time that the IP address which is assigned to a client will be expired.

2.16.1.1 Adding VLAN

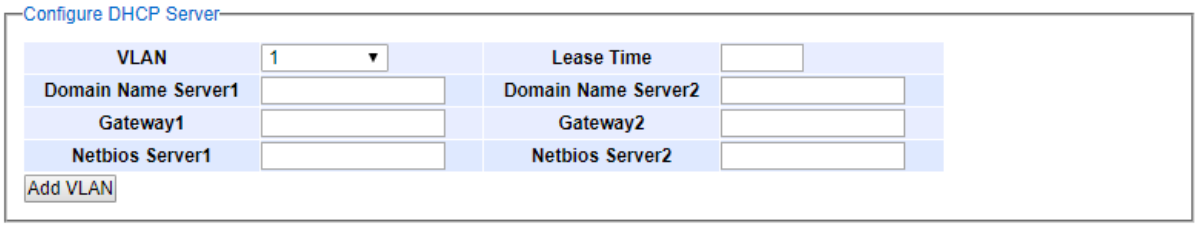


Figure 2.218DHCP Server's Setting Submenu

Multiple **VLAN IDs**can be added to the **DHCP Server**. This will enable any client joining a specific **VLAN** to obtain an IP address from the **DHCP Server** inside the RHG96XX. Only VLANs that are already configured withIP interfacescan be added to the **DHCP server**. First, the user should select the **VLAN** ID from the dropdown list. The available option for **Lease Time** are: 1 Hour, 12 Hours, 1 Day, 7 Days, 15 Days, 30 Days, 45 Days, 90 Days, 120 Days. Then, the user should enter all the fields inside the **Configure DHCP Server** box. When no IP addresses are specified for **Domain Name Servers**, **Gateways**, and **Netbios Servers**,the default values which are set to 0.0.0.0 will be used. The default value of **Lease Time**is 3,200seconds. Finally, clicking on the **Add VLAN** button will add a **VLAN** to the **DHCP server**.

The user can configure either dynamic or static IP address assignment by DHCP Server for each VLAN. These can be done under the **Add Dynamic IP** or **Add Static IP** boxes as shown in Figure 2.219 and Figure 2.220, respectively.

2.16.1.2 Adding Dynamic IP Address Ranges

To add dynamic IP address, the user need to select a specific **VLAN** ID from the dropdown list inside the **Add Dynamic IP** box as shown inFigure 2.219. Then, the user must enter a starting IPv4 address in the **Dynamic IP Start** field and enter an ending IPv4 address in the **Dynamic IP End** field.Finally, clicking on the **Add Dynamic IP** button to update the data.

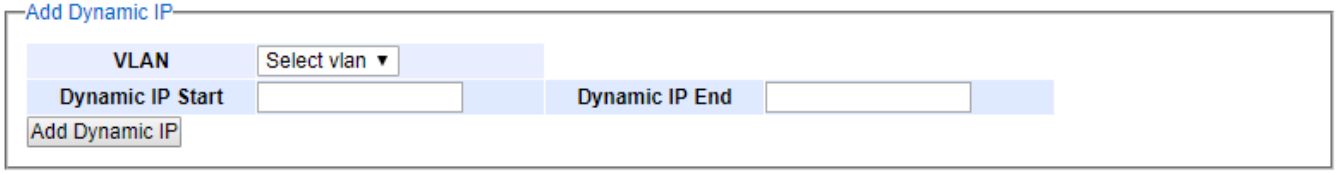


Figure 2.219 Add Dynamic IP Address in DHCP Server's Setting Submenu

2.16.1.3 Adding Static IP Address

The user can add a static IP address for a client (host)that joins a VLAN under the DHCP Server. To add a new static IP address, first the user must select a **VLAN** ID from the dropdown list inside the **Add Static IP** box as shown in Figure 2.220. Then, the desired **Static IP** address, the**Host Name**, and the**MAC Address** of the host must be entered. Note that the **Host Name** must be entered without spaces in between. Finally, clicking on the **Add Static IP** button to update the entry into the DHCP Server.

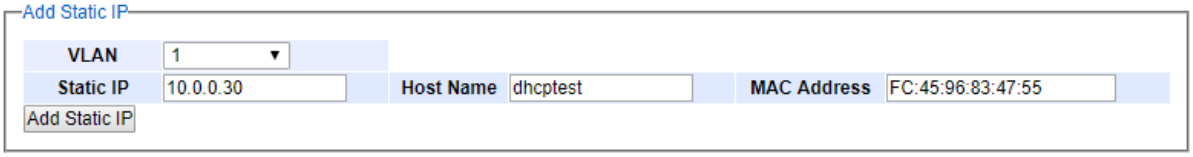


Figure 2.220Add Static IP Address in DHCP Server's Setting Submenu

2.16.1.4 Modification of DHCP Server Configuration

To updating or deleting DHCP Server Configuration of a VLAN, the user can modify an entry in the list of **VLAN** inside the **Current DHCP Settings** box as shown in Figure 2.221. An entry must be selected by clicking on the checkbox in front of it. Then, the user can follow one of the instructions listed below to update or delete some values in the existing entry.

10.0.50.35 10.0.50.45

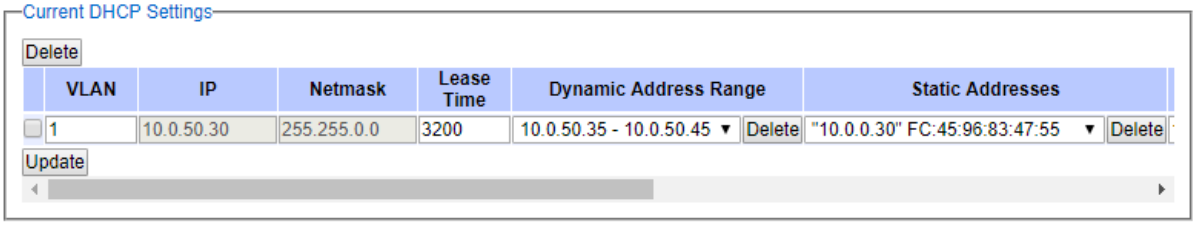


Figure 2.221Modify DHCP Server Configuration in DHCP Server's Setting Submenu

- Domain Name Servers and/or Gateways and/orNetbios Servers can be modified by keying in Domain Name Server (Domain Name Server 1 and/or Domain Name Server2),and/orGateway (Gateway1 and/or Gateway2),and/or Netbios (Netbios1 and/or Netbios2).Then, clickan "**Update**" button.
- Dynamic IP address range can be deleted. However,one of the**DynamicAddressRanges** must be selectedfrom the dropdown list first. Then, clicking on the "**Delete**" button to remove that yynamic IP address range.
- Static IP address can be deleted.Once again,one of the**Static Addresses** must be selectedfrom the dropdown list first. Then, clicking on the"**Delete**" button to remove that static IP address.
- A VLAN configuration in the DHCP Server can be deleted. However,one of VLAN entries must be selected first. To remove that VLAN configuration, then clicking on the "**Delete**" button.
- A VLAN can be modified into a new VLAN only if thatnew VLAN is already created.

2.16.2 Clients

In **Clients** dropdown submenu, the **DHCPServer's Client details** are displayed for each VLAN in a table format as shown in Figure 2.222. The columns in the table are **VLAN**, **Client Name**or host name, IP **Address**, **MAC**address, **Lease Start**, and **Lease End**. Note that all configured static IP addresses will always be listed in the table even though they are not assigned to any clients. However, the dynamic IP addresses which were already assigned to clients will be shown in the list.

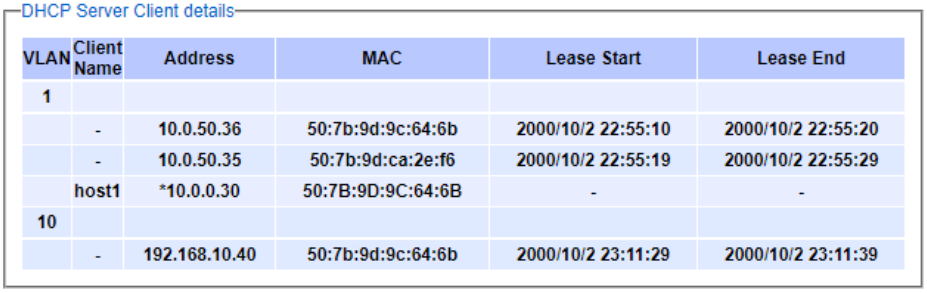


Figure 2.222Client Menu in DHCP Server's Dropdown Menu

2.16.3 Restart

For the DHCP Server's configuration to take effect after any modification, the user needs to restart the DHCP server inside the RHG96XX. Click **Restart** buttonin **DHCP Restart** box under **Restart** dropdown submenu to restart the DHCP Server.

Figure 2.223Restart Menu in DHCP Server's Dropdown Menu

2.17 Security

Three security features are providedin RHG96XX series:

- **Port Security(Static)**
- **802.1X**
- **IP Source Guard**
- **ARP Spoof Prevention**
- **DHCP Snooping**
- **Access Control List (ACL)**
- **Dynamic ARP Insepction**

Figure 2.224 shows the dropdown menu for security section on the managed switch.

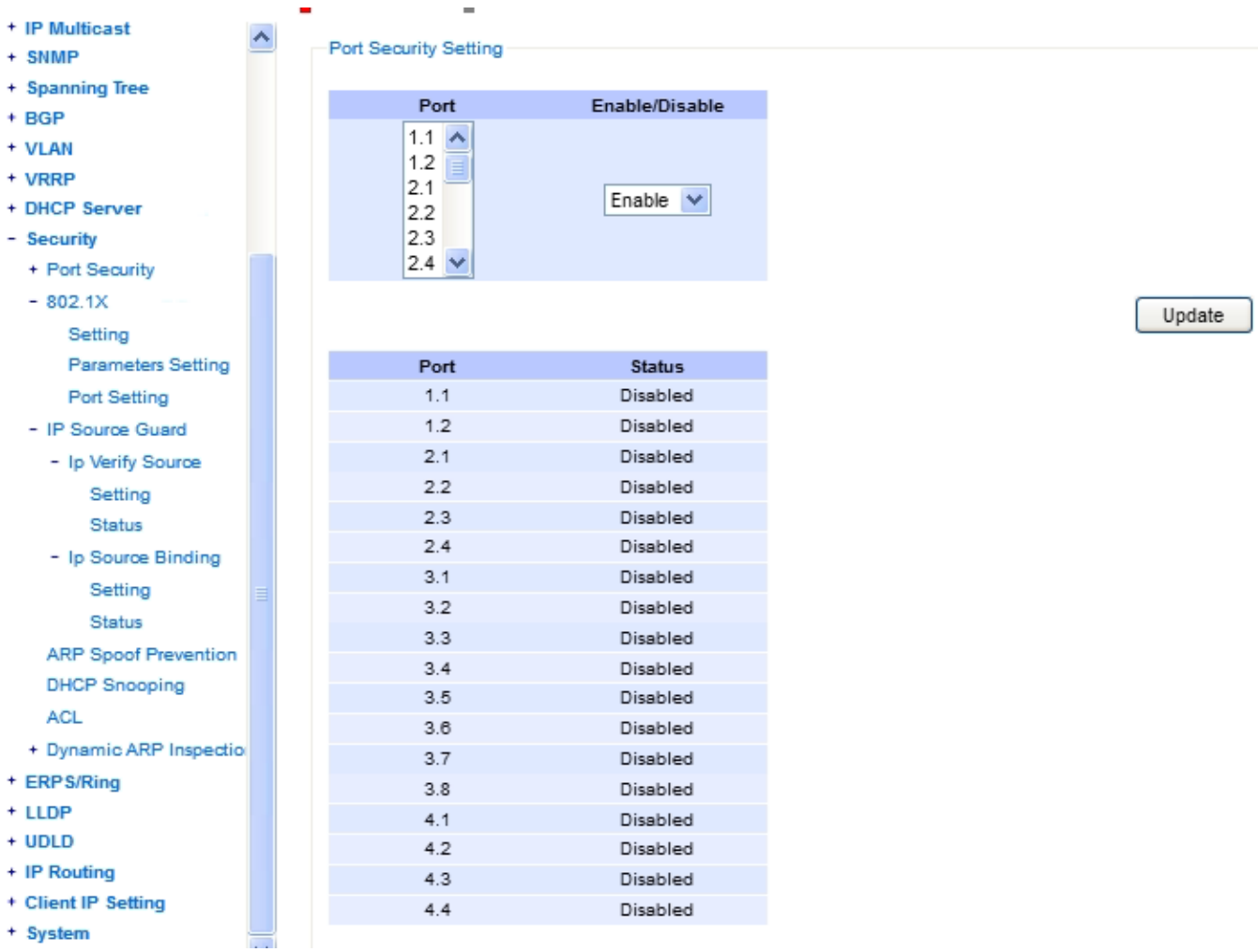


Figure 2.224 Security Dropdown Menu

2.17.1 Port Security

Port Securityor static port security subsection allows the users to control security on each port of the managed switch and create a table of MAC addresses allowed to access the switch. The **Port Security** menu is subdivided into two sub-menus which are **Setting** and **White-List MAC**.

2.17.1.1 Port Security Settings

Figure 2.225 displays the Port Security Setting webpage where the users can enable or disable static security on one or multiple ports. To enable or disable multiple ports at the same time please hold the**Ctrl** key and select multiple ports under the **Port** list and choose **Enable** or **Disable** and then click **Update** button. The lower part of the Port Security Setting webpage shows the current status of security setting for each port on the managed switch.

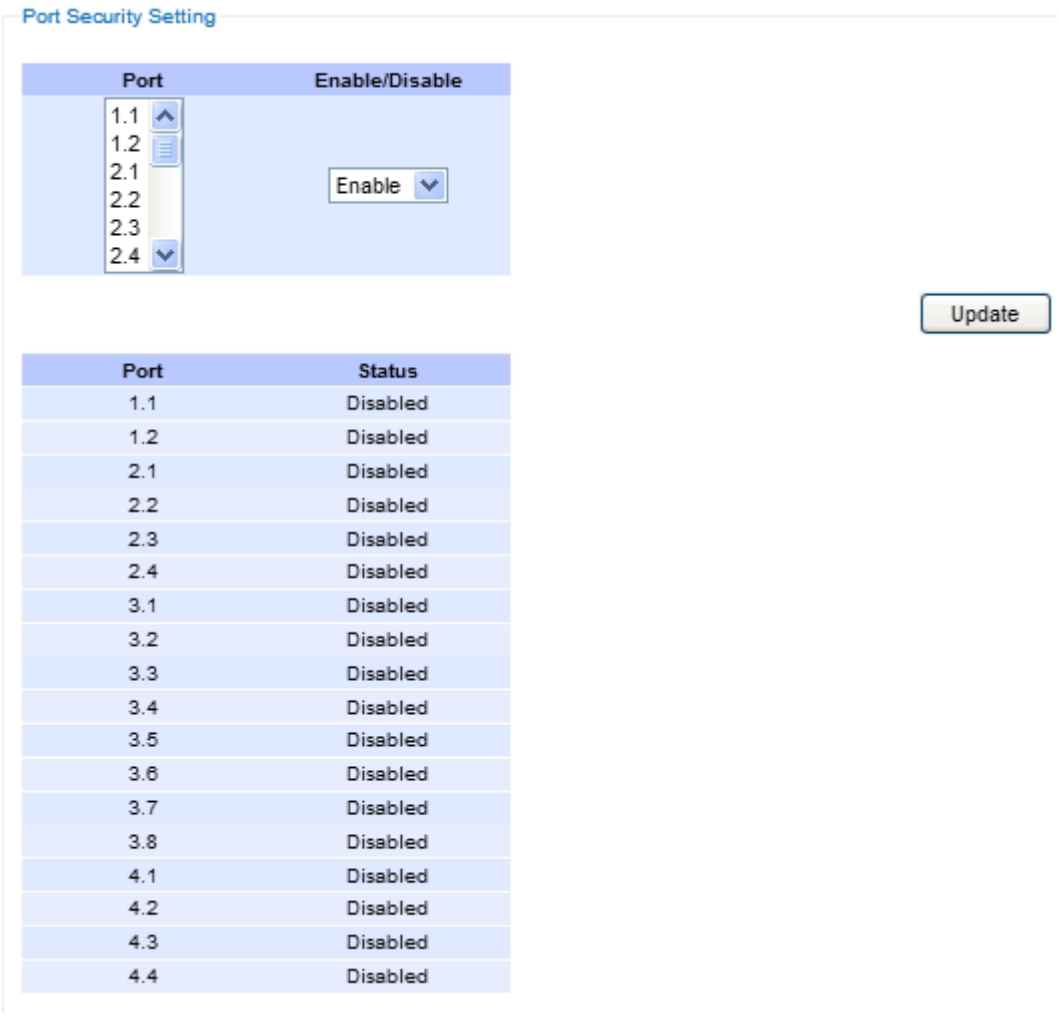


Figure 2.225 Port Security Setting Webpage

2.17.1.2 Port Security White- List MAC

The White-List MAC webpage is depicted in Figure 2.226. The users can create a list of MAC address that will be allowed to access the managed switch. The users will need to specify the VLAN ID (VID)and port number for each particular MAC address added to this list. After entering all required fields, please click on the **Add** button to add the new MAC address into the white list. Please remember that the same MAC address cannot be assigned to two different ports. This will cause an error message. Note that if there are existing MAC address on the list and the users would like to remove them, please click on the **Remove** button at the end of each record. Image below summarizes the descriptions of the fields in White-List MAC webpage.

Figure 2.226 White-List MAC Webpage

Table 2.48Description of Fields in White-List MAC Webpage

Label	Description
MAC Address	Type the suitable MAC address
Ports	Choose the desired ports
Remove	Option to remove the corresponding MAC address
Add	Click to add a MAC address
VLAN	Specify the corresponding VLAN address to MAC address

2.17.2 802.1X

802.1Xis an IEEE standard for port-based Network-Access Control. It provides an authentication mechanism to devices that wantto attach to a LAN or WLAN. This protocol restricts unauthorized clients from connecting to a LAN through ports that are opened to the Internet. The authentication basically involves three parties(seeFigure 2.227): a supplicant, an authenticator, and an authentication server.

- Supplicant:A client device that requests access to the LAN.
- Authentication Server:This server performs the actual authentication. We utilize RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice)as the authentication server.
- Authenticator:The Authenticator is a network device (I.e. the RHG9XXX Industrial Managed Switch)that acts as a proxy between the supplicant and the authentication server. It passes around information, verifies information with the server, and relays responses to the supplicant.

The authenticator acts like a security guard to a protected network. The supplicant is not allowed accessingto the protected side of thenetwork through the authenticatoruntil the supplicant's identity has been validated and authorized. With 802.1X authentication, a supplicant and an authenticator exchange **EAP**(**E**xtensible **A**uthentication **P**rotocol, an authentication framework widely used by IEEE). Then the authenticator forwards this information to the authentication server for verification. If the authentication server confirms the request, the supplicant (client device)will be allowed to access resources located on the protected side of the network.

RADIUS: The RADIUS is a networking protocol that provides authentication, authorization and accounting (AAA)management for devices to connect and use a network service. Figure 2.227 shows a diagram of RADIUS authentication sequence.

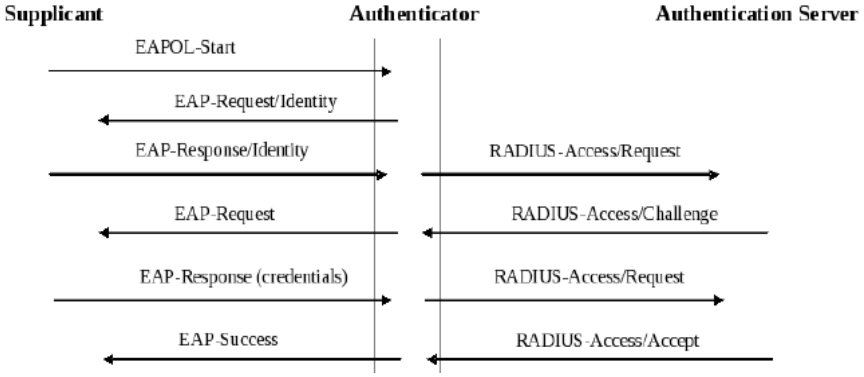


Figure 2.227RADIUS Authentication Sequence

The **802.1X** option under the Security section is subdivided into three sub-menus which are: **Setting**, **Parameters Setting**, and **Port Setting**.

2.17.2.1 802.1X Settings

The 802.1X security mechanism can be enabled in this webpage as shown in Figure 2.228. When the users check the Enabled box, the rest of the option fields will become active. The users then have to enter all the required fields to configure the 802.1X Setting which are the IP address of RADIUS server, the RADIUS server's port number,

RADIUS server's accounting port number, NAS identifier, and shared key. Summary of 802.1X Setting options are given in Table 2.49. After changing all the required fields, please click on the **Update** button.

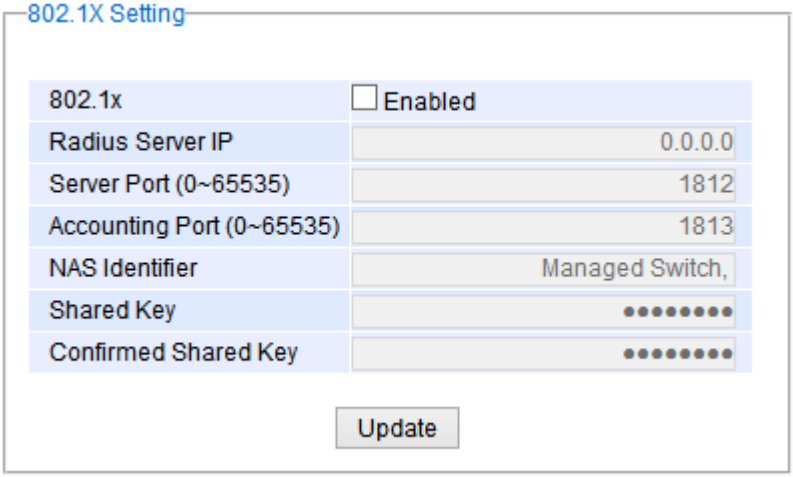


Figure 2.228 802.1X Setting Webpage

Table 2.49Descriptions of 802.1X Setting

Label	Description	Factory Default
802.1x	Choose whether to Enable 802.1X for all ports or not	Disabled
Radius Server IP	Set RADIUS server IP address	0.0.0.0
Server Port	Set RADIUS server port number. The range is 0 ~ 65535.	1812
Accounting Port	Set the accounting port number of the RADIUS server. The range is 0 ~ 65535.	1813
NAS Identifier	Specify the identifier string for 802.1X Network Access Server (NAS). Max.Of30 characters.	Managed Switch
Shared Key	A shared key between the managed switch and the RADIUS Server. Both ends must be configured to use the same key. Max. Of 30 characters.	NULL
ConfirmShared Key	Re-type the shared key string.	Dependent

2.17.2.2 802.1X Parameters Settings

There are a number of 802.1X parameters that the users might want to fine tune. This can be done on this webpage as shown in Figure 2.229. These parameters are related to the authentication periods or timeout durations and maximum number of authentication requests. Table 2.50 summarizes the descriptions of these parameters and their default setting. Please clicking on the Update button after the users changed any of the parameters.

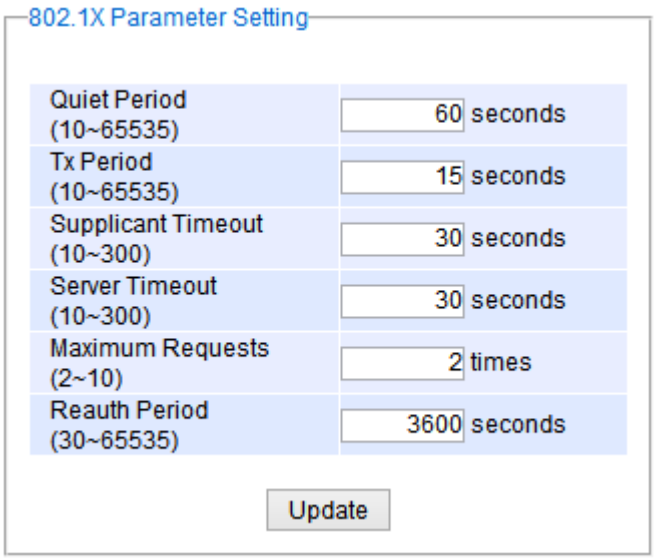


Figure 2.229 802.1X's Parameters Setting Webpage

Table 2.50Descriptions of 802.1X Parameters

Label	Description	Factory Default
Quiet Period	Waiting time between requests when the authorization has failed. Range from 10 to 65535 seconds.	60
Tx Period	Waiting time for the supplicant's EAP response packet before retransmitting another EAP request packet. Range from 10 to 65535 seconds.	15
Supplicant Timeout	Waiting time for the supplicant to response to the authentication server's EAP packet. Range from 10 to 300 seconds.	30
Server Timeout	Waiting time for the authentication server to response to the supplicant's EAP packet. Range from 10 to 300 seconds.	30
Maximum Requests	Maximum number of the retransmissionsthat the authentication serversends EAP request to the supplicant before the authentication session times out.Range from 2 to 10 seconds.	2
Reauth Period	Time between periodic re-authentication of the supplicant. Range from 30 to 65535 seconds.	3600

2.17.2.3 802.1x Port Setting

The user can individually configure 802.1x security mechanism on each port of the RHG9XXX managed switch as shown in Figure 2.114. Each port can be set for any of the four authorization modeswhich are Force Authorization, Force Unauthorization, IEEE 802.1X Standard Authorization, and no authorization (N/A)as described in Table 2.48. The lower part of the webpage is a table display the current status of authorization mode and state of each port on the managed switch. To enable the 802.1X security on any of the port(s), click one of the port or press **Ctrl** key and click multiple ports on the list and choose the Authorization **Mode** from the pulldown list and click the **Update** button.To check the latest status of the 802.1X port setting, please click on the **Refresh** button.

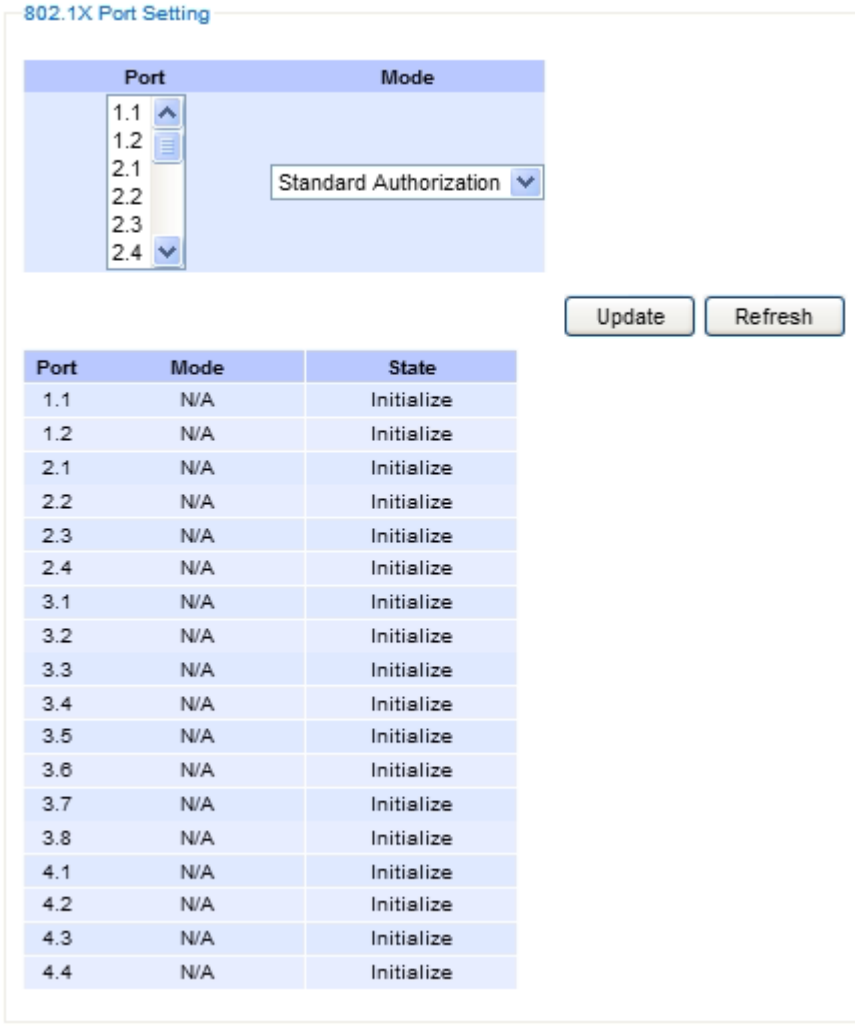


Figure 2.230802.1x Port Setting Webpage

Table 2.51Descriptions of 802.1X Port Setting

Label	Description	Factory Default
Port	Set specific ports to be configured.	Option
Mode	Choices: **Force Unauthorized:**Specify forced unauthorized **Force Authorized**: Specify forced authorized **Standard Authorization**: Specify authorization based on IEEE 802.1X **N/A**:Specify disable authorization	N/A

2.17.3 IP Source Guard

IP Source Guard is another security feature in RHG96XX managed switch that provides source IP address filtering on a Layer 2 port. This is to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. This security feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports. Figure 2.231 shows the IP Source Guard's submenus.

Figure 2.231 IP Source Guard Drop-down Menu

2.17.3.1 IP Verify Source' Setting

The IP Verify Source is a dynamic IP Source Guard that creates a Layer-2 packet filtering on each port of the RHG96XX. The filter types can be IP or IP-MAC. For IP filter type, RHG96XX will check only the Source IP address of the packets. For IP-MAC filter type, RHG96XX will consider both Source IP address and Source MAC address of the packets. Figure 2.232 shows the IP Verify Source Setting webpage. To enable IP Verify Source filtering on a port, check the corresponding Enable box and choose a Filter-type from the dropdown list. After finish configuring, click on the Update button to active the filtering. After a filter was activated, all incoming packets to a configured port will be dropped. Only the packets that conform to specific Source and MAC addresses will be allowed to pass.

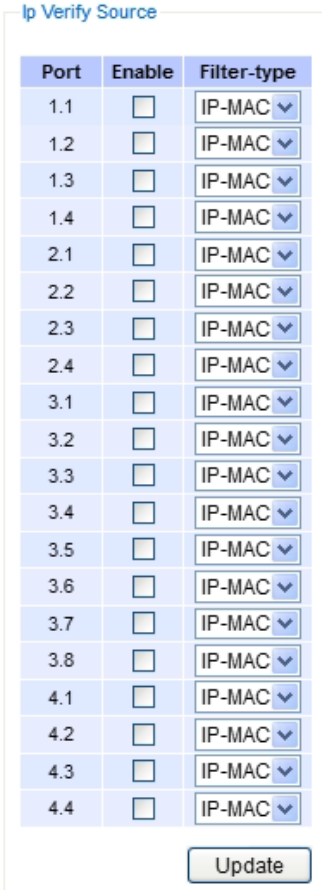


Figure 2.232 IP Verify Source's Setting Webpage

2.17.3.2 IP Verify Source's Status

The user can check the status of IP Verify Source guard setting on each port in this webpage as shown in Figure 2.233. For each entry in the status table, there will be port number, Filter-type, Filter-mode, IP Address, and MAC Address. Note that if the DHCP snooping function was not enable or no traffic on the port, you will see the notification "inactive-no-snooping" message in each entry.

Ip Verify Source - Status

Port	Filter-type	Filter-mode	IP Address	MAC Address
1.1		inactive-no-snooping		
1.2		inactive-no-snooping		
1.3		inactive-no-snooping		
1.4		inactive-no-snooping		
2.1		inactive-no-snooping		
2.2		inactive-no-snooping		
2.3		inactive-no-snooping		
2.4		inactive-no-snooping		
3.1		inactive-no-snooping		
3.2		inactive-no-snooping		
3.3		inactive-no-snooping		
3.4		inactive-no-snooping		
3.5		inactive-no-snooping		
3.6		inactive-no-snooping		
3.7		inactive-no-snooping		
3.8		inactive-no-snooping		
4.1		inactive-no-snooping		
4.2		inactive-no-snooping		
4.3		inactive-no-snooping		
4.4		inactive-no-snooping		

Figure 2.233 IP Verify Source's Status Webpage

2.17.3.3 IP Source Binding' s Setting

The IP Source Binding is a static IP Source Guard that creates a Layer-2 packet filtering on each port of the RHG96XX. This packet filter will require specific Source IP Address and Source MAC Address to be entered for each port. To enable IP Source Binding filtering on a port or multiple port, the user must enter the Source MAC Address and the Source IP Address in the corresponding textboxes as shown in Figure 2.234. Then, check the boxes for all required ports. Then, click Add button to add the filtering entry for IP Source Binding. An entry of IP Source Binding filtering will be listed in the table in the lower part of the webpage.

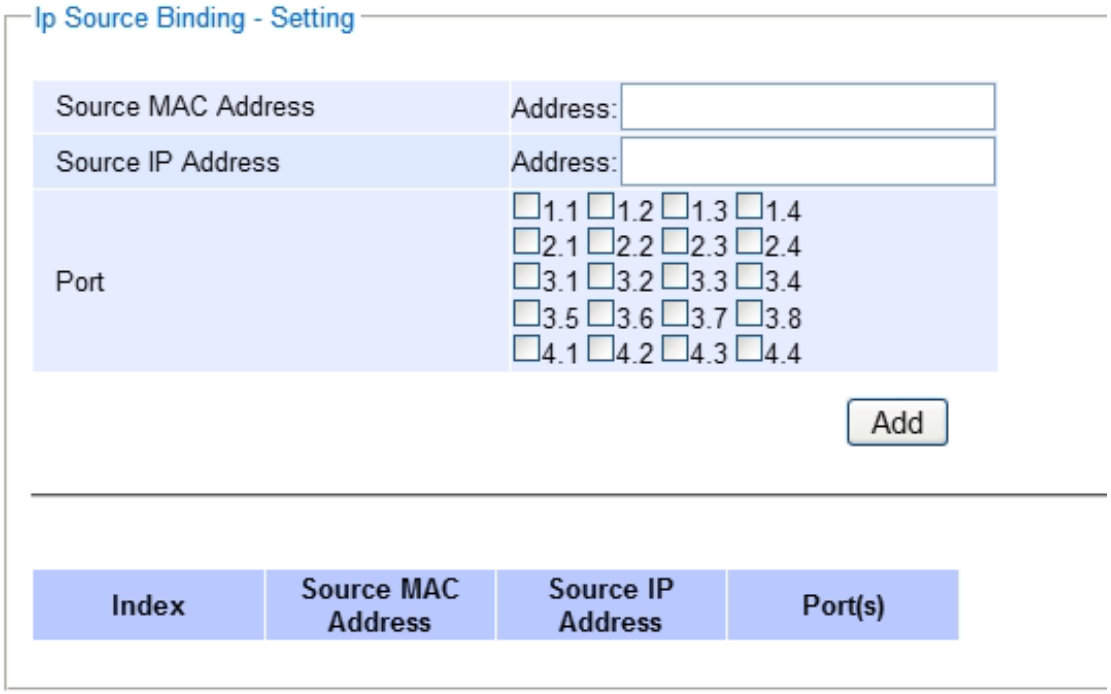


Figure 2.234 IP Source Binding's Setting Webpage

2.17.3.4 IP Source Binding's Status

The user can check the status of IP Source Binding guard setting based on MAC Address and IP address pairs in this webpage as shown in Figure 2.235. For each entry in the status table, there will be MAC Address, IP Address, Lease (seconds), Type of Filtering, and list of Ports.

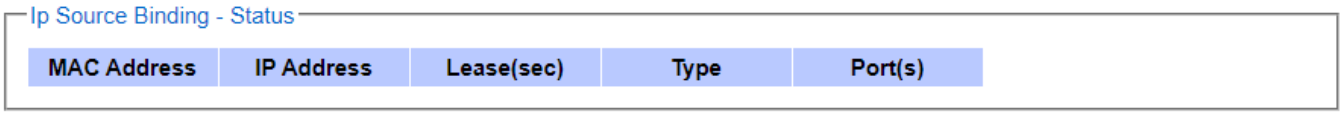


Figure 2.235 IP Source Binding's Status Webpage

2.17.4 ARP Spoof Prevention

ARP (Address Resolution Protocol) Spoof Prevention is a security mechanism supported by Atop's RHG96XX series to prevent ARP spoof attacks. The ARP spoof attack is a kind of network security attacks that a malicious host or node sends a falsify ARP messages over a local area network. This type of attack is also called ARP spoofing, ARP cache poisoning, or ARP poison routing. Typically, the attacker would like other hosts/nodes in the network to link or map the malicious Ethernet MAC address to a legitimate IP address of a victim host/node. To enable this security mechanism, check the Enabled box for ARP Spoof Prevention option as shown in Figure 2.236 and then click **Update** button.

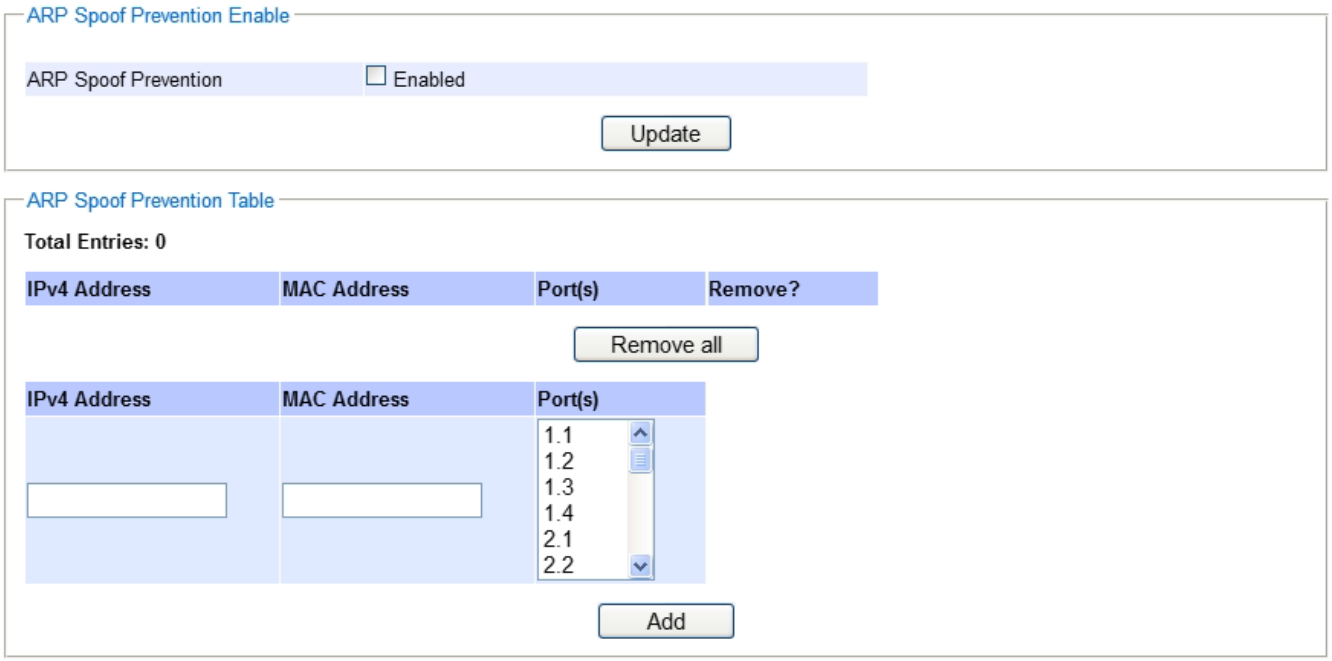


Figure 2.236 ARP Spoof Prevention Webpage

When ARP Spoof Prevention is enabled on RHG96XX series, the ARP spoof prevention table must also be set with prevention entries. Each entry consists of IPv4 Address, MAC Address, and Port number(s). The IP Address and the MAC address in each entry belong to a legitimate or valid host/node that the administrator assigned or approved and the administrator of RHG96XX want to protect that host/node from being spoofed. The port number can be one or group or all of the ports on RHG96XX that will be accepting incoming ARP packets from the network. If there are incoming ARP packets to RHG96XX and both IP address and MAC address of the ARP packets match one of the entries in the table, the ARP packets will be accepted by the RHG96XX system. If the sender's IP address of an ARP packet matches the IP address in one of the entries in the table but the sender's MAC address of the ARP packet does not match, the RHG96XX will drop the ARP packet on its port. Note that RHG96XX will bypass or accept other ARP packets whose sender IP is not in the ARP Spoof Prevention Table.

To fill in a prevention entry, scroll down to the ARP Spoof Prevention Table part in Figure 2.236. Then, enter an IP address in the first textbox under IPv4 Address column and a MAC address in the second textbox under the MAC Address column. Then select one or multiple port number from the list of the ports under the Port(s) column. Note that if you did not select any port from the list, the default setting will be all ports. Then, click **Add** button to insert the entry into the table. Finally, make sure that the Enabled box behind the ARP Spoof Prevention is checked and click **Update** button inside the ARP Spoof Prevention Enable part. The new entry should be updated on the table and activate the security mechanism. To remove one of the entries from the table, please click on the **Remove** button for the corresponding entry in the table. To remove all of the entries from the table, please click on the **Remove all** button under the ARP Spoof Prevention Table.

2.17.5 DHCP 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 RHG96XX provide DHCP Snooping feature. When this feature is enabled on specific port(s) of RHG96XX managed switch, the RHG96XX 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, check the Enabled box behind the DHCP Snooping option under the DHCP Snooping webpage as shown in Figure 2.237. By default, all interfaces of RHG96XX are untrusted for DHCP Snooping. To configure specific port(s) as trusted port(s), simply check the box under the Trust column for that particular Port(s). Finally, click the **Update** button at the bottom of the webpage to activate the DHCP Snooping on the selected port(s). Note that the table inside the DHCP Data box will show information of the IP-to-MAC mapping, the Request Port and Lease Time of DHCP. To obtain the latest information on the bindings table, click on the **Refresh** button.

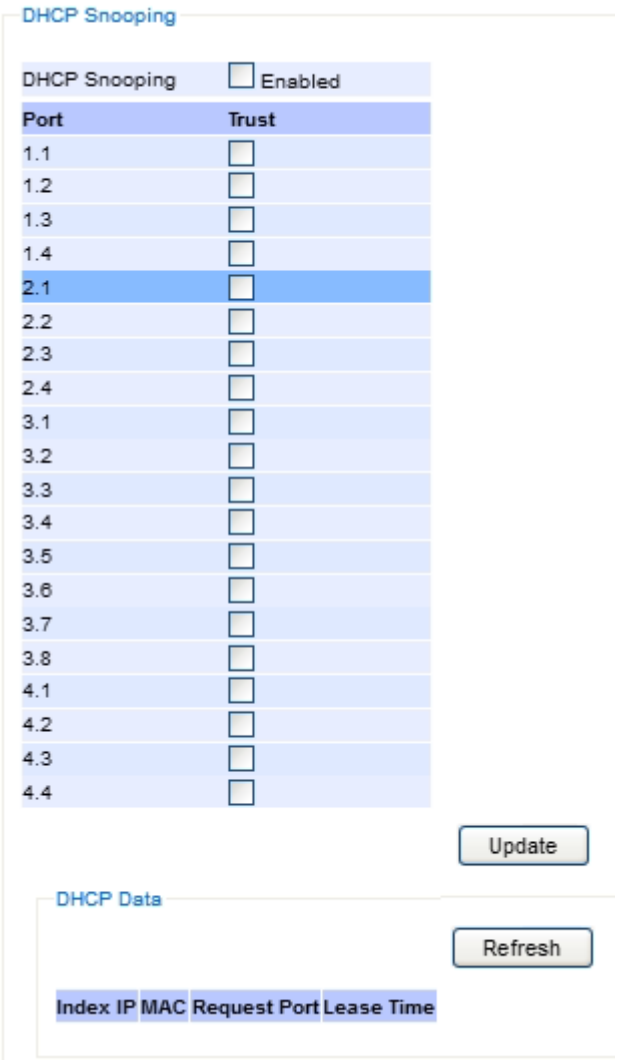


Figure 2.237 DHCP Snooping Webpage

2.17.6 ACL (Access Control List)

Access Control List (ACL)is the mechanism for network access control.Theusers configure the switch's filtering rules for accepting or rejecting some packets. Two types of filters are deployed in the RHG96XX series:

1) by MAC layer, and
2) by IP layer.

The numbers of matching rules can be at most 128.However, the main important rules that are mostly exercise are follows.Rules for filtering by MAC layer includes MAC address, VLAN ID or Ether type. Whereas, rules for filtering by IP layer includes IP protocol, IP address, TCP/UDP port or Type of Service (TOS) for IPv4 or Traffic Class for IPv6.When filtering is enabled, the matching rulesare used to check whether the receiving packet ismatched. If it is match, the packet will be rejected; otherwise it will be accepted. Note here that the matching rules later will be referred to as the entries of ACL.

The ACL webpage is depicted inFigure 2.238. To differentiate between each ACL entry, **Index** number from 1 to 128 is used. The ACL entry that has higher priority will be checked first before the lower priority. The **Name** field is for setting name of this rule. Type of filtering whether MAC layer ("**Mac Base**")and IP layer ("**IPv4 Base**" or "**IPv6 Base**")can be set in the **Filter** field.Note that when change from Mac Base to IP Base the required parameters for ACL setting will be changed accordingly.

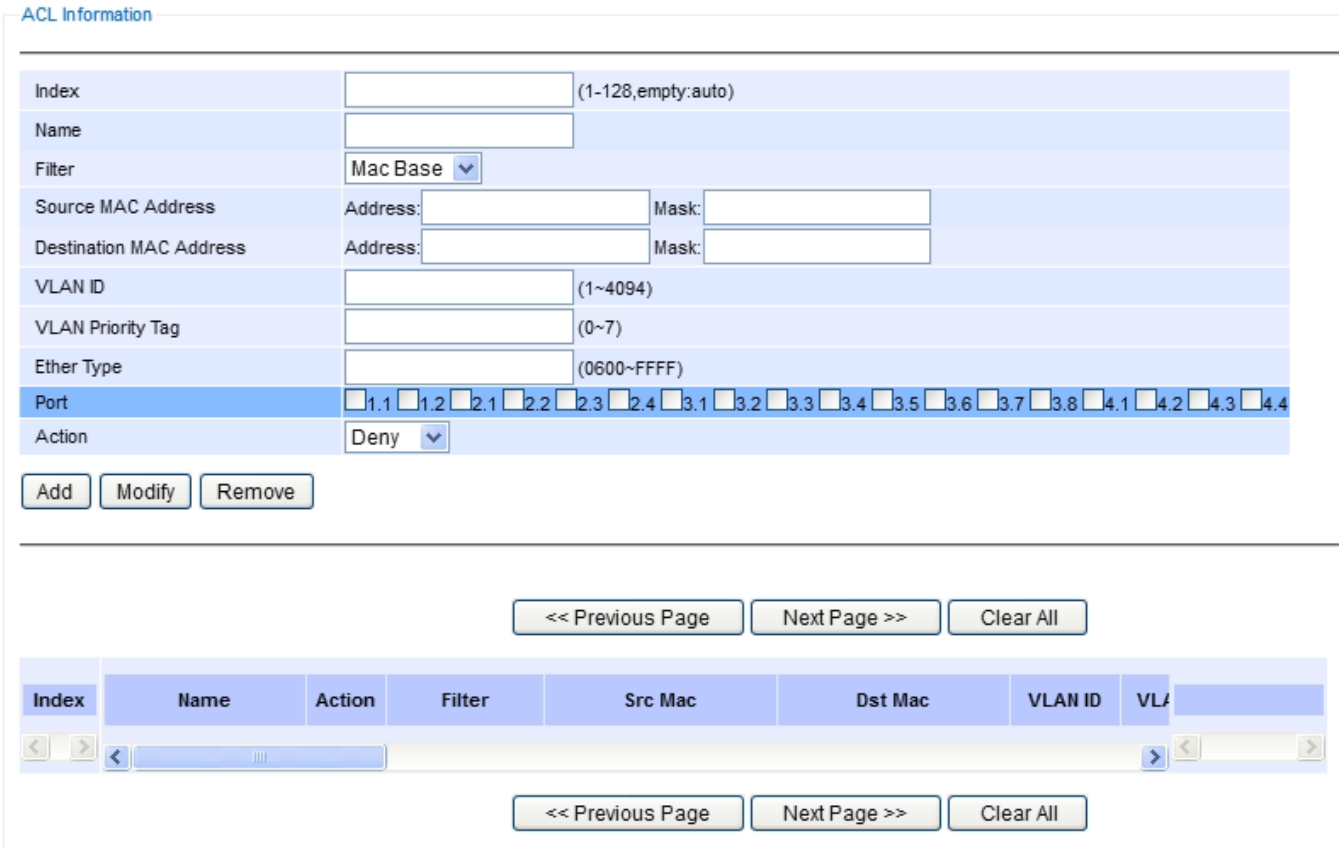


Figure 2.238 Security Access Control List Information Webpage(MAC Based Filtering)

The main ACL entries for filtering by MAC layer (also called L2 filtering) as shown in Figure 2.238 include MAC address, VLAN ID, VLAN Priority Tag and Ether Type. Table 2.52describes definition of each in details. Here note that if any field is empty, that ACL entry will be ignored.

Table 2.52 Descriptions of Main ACL Entries for L2 Filtering in ACL Webpage

ACL Entry	Definition	Range
Source or Destination MAC Addresses	MAC address are the fields of the Ethernet frame header. The Mask item is a bit mask for comparing range.	For every non-zero bit in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of 255.255.255.255 and all of bits in the IP Address are compared.
VLAN ID	The VLAN ID field of 802.1Q VLAN tag in the Ethernet frame header. If the trunk ports are created, they will also be shown on the port list. If you want to select a trunk port, please make sure that there are no ACL entry using the physical ports which are belonging this trunk port.	The item value is between 1~4094.

ACL Entry	Definition	Range
VLAN Priority Tag	The Priority field of 802.1Q VLAN tag in the Ethernet frame header.	The item value is between 0~7.
Ether Type	The Ethernet type field in the Ethernet frame header. The followings are examples. The value 0x8000 is an IPv4 packet. The value 0x86DD is an IPv6 packet. The value 0x8100 is an 802.1Q packet.	The item value is between 0x0600~0xFFFF.

For IP Layer, there are two types of filtering:

1) IPv4 Base, and
2) IPv6 Base.

The main ACL entries for filtering by IP layer (also called L3 filtering)as shown in Figure 2.239 and Figure 2.240 for IPv4 and IPv6 include IP Protocol, Source IP Address, Destination IP address, TCP/UDP Source Port, TCP/UDP Destination Port and TOS (Type of Service for IPv4) or Traffic Class (for IPv6).Table 2.53 describes definition of each in details. Once again, note that if any field is empty, that ACL entry will be ignored.

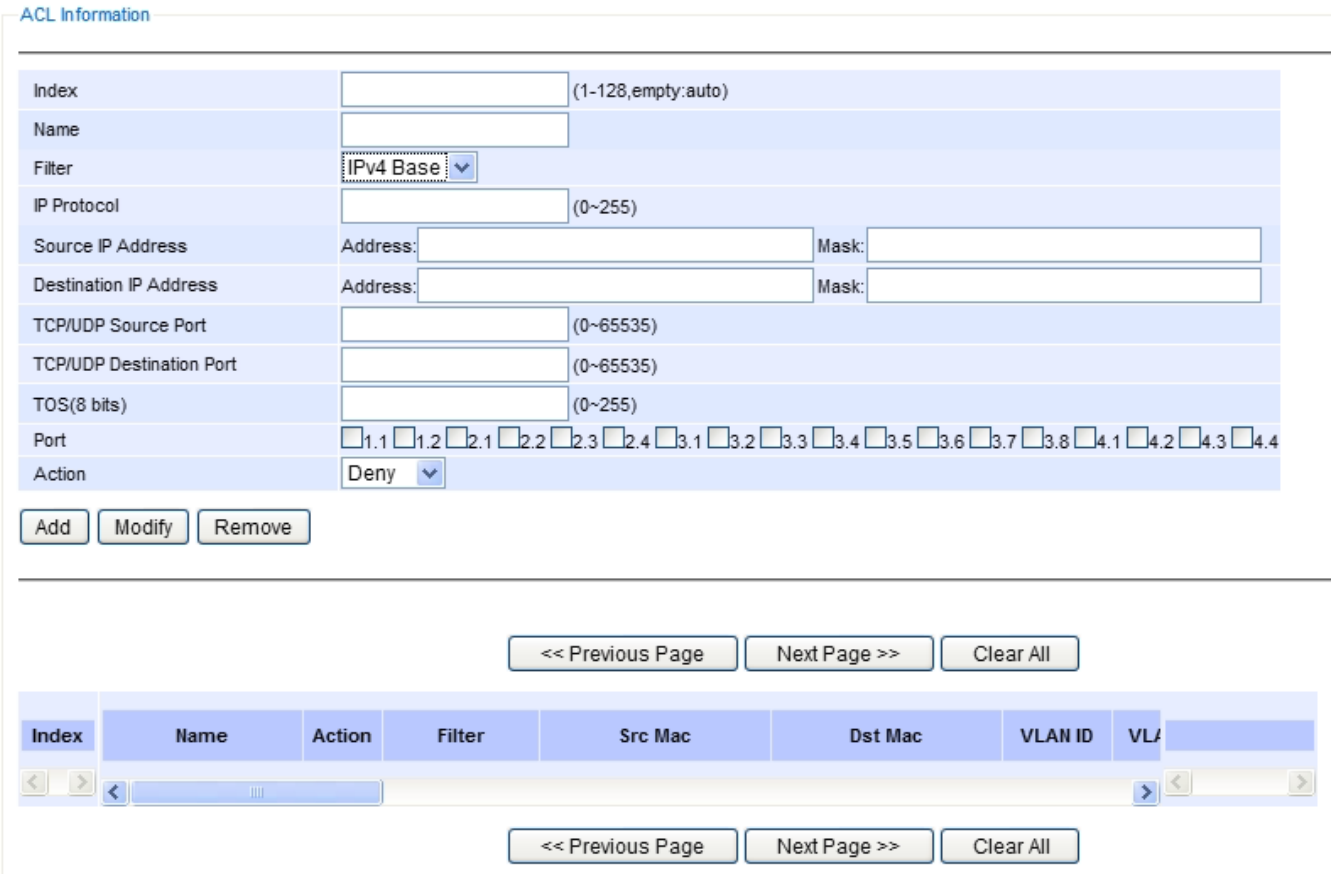


Figure 2.239 Security Access Control List Information Webpage (for IPv4 Based Filtering)

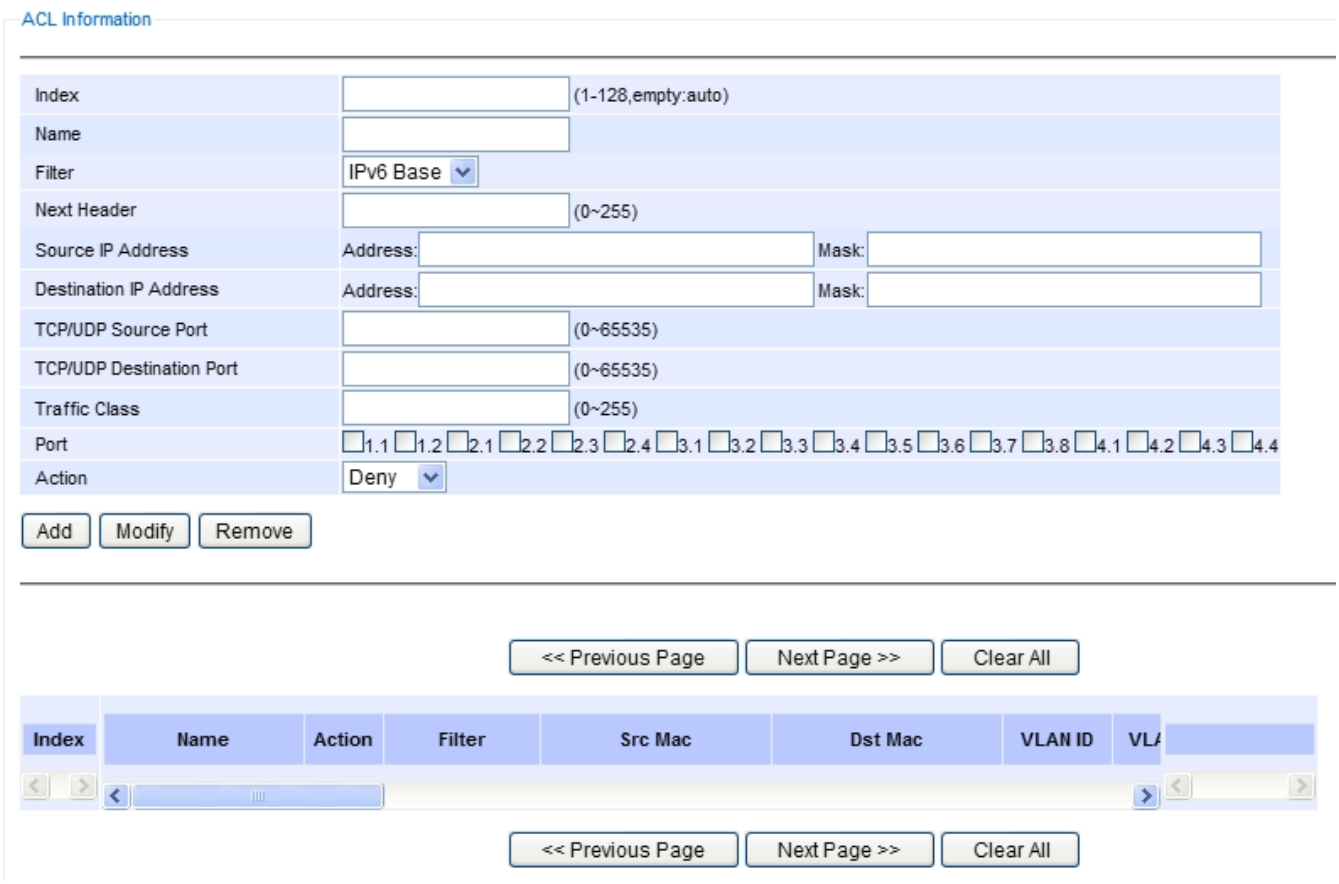


Figure 2.240 Security Access Control List Information Webpage (for IPv6 Based Filtering)

Table 2.53 Description of Main ACL Entries for L3 Filtering in ACL Webpage

ACL Entry	Definition	Range
IP Protocol	The Protocol field of the IPv4 packet header. The followings are examples.The value 1 is for an ICMP packet.The value 6 is for the TCP packet.The value 17 is for the UDP packet.	The item value is between 0~255
Next Header	The Protocol field of the IPv6 packet header. The followings are examples. The value 58 is for an ICMP packet. The value 6 is for the TCP packet. The value 17 is for the UDP packet.	The item value is between 0~255
Source or Destination IP Addresses	IP Addresses are the fields of the IPv4 or IPv6 header. The Mask item is a bit mask for comparing range.	IPv4: For every non-zero bits in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of 255:255:255:255 and all of bits in the IP Address are compared IPv6: For every non-zero bits in the Mask, its relative bit in the IP address will be compared. If the Mask is 0.0.0.0.0.0, then this condition is always accepted. If the Mask is empty, it is considered equal to the Mask of

ACL Entry	Definition	Range
		FF:FF:FF:FF:FF:FF and all of bits in the IP Address are compared
TCP/UDP Source Port /TCP/UDP Destination Port	The fields of TCP/UDP frame header. It is used to filter the application services. For example, the TCP Destination Port 21 is for the FTP service, the TCP Destination Port 23 is for the Telnet service and the TCP Destination Port 80 is for the HTTP service. To select which ports will follow the filter rule and what action to take, check the checkbox corresponding to that port and select choice of "Deny"or "Permit"in the action field. If this ACL entry is match, rejecting packet if 'Deny' is selected, and accepting packet if 'Permit'is selected.	The item value is between 0~65535.
TOS (Type of Service)	A Differentiated Service Code Point (DSCP)field in an IPv4 header.It is used for providing Quality of Service (QoS).	The item value is between 0~255.
Traffic Class	The Traffic Class field indicates class or priority of IPv6 packet. It helps switch to handle the traffic based on priority of the packet. If congestion occurs on switch, then packets with least priority will be discarded.	The item value is between 0~255.

Table 2.54 Summary of Label, Description, and Factory Default for Both ACL Filtering Method

LABEL	DESCRIPTION	FACTORY DEFAULT
Index	Priority (1-128)	NONE
Name	Max length 32	NONE
Filter	Mac Base/IPv4 Base/IPv6 Base	Mac Base
Source MAC Address and Mask	A:B:C:D:E:F.is the MAC address. Mask is for bit mask checking.0.0.0.0.0.0 is for accepting all. Empty is as FF:FF:FF:FF:FF:FF.	NONE
Destination MAC Address and Mask	A:B:C:D:E:F.is the MAC address.Mask is for bit mask checking.0.0.0.0.0.0 is for accepting all.Empty is as FF:FF:FF:FF:FF:FF.	NONE
VLAN ID	1-4094	NONE
VLAN Priority Tag	0 ~ 7	NONE
Ether Type	0x0600-0xFFFF	NONE
IP Protocol	0-255	NONE
Next Header	0-255	NONE
Source IP Address	A.B.C.D is the IP address. Mask is for bit mask checking.0.0.0.0 is for accepting all. Empty is as 255.255.255.255.	NONE
Destination IP Address	A.B.C.D is the IP address. Mask is for bit mask checking.0.0.0.0 is for accepting all.Empty is as 255.255.255.255.	NONE
TCP/UDP Source Port	0-65535	NONE
TCP/UDP Destination Port	0-65535	NONE
TOS	0-255	NONE
Traffic Class	0-255	NONE
Port	1,2,3,4,5,6,7,8	NONE

LABEL	DESCRIPTION	FACTORY DEFAULT
Action	Deny/Permit	NONE

The users can **Add**, **Modify**, or **Remove** each ACL entry based on the Index number as shown in Figure 2.238,Figure 2.239 and Figure 2.240. The lower part of the ACL Information webpage is the list of all ACL entries.The user can browse through the list by using the **Previous Page** and **Next Page** buttonsTo remove all of the ACL entries from the list, click on the **Clear All** button.

2.17.7 Dynamic ARP Inspection with DHCP

Dynamic ARP Inspection (DAI) is another security feature provided by RHG96XX managed switch to prevent a class of man-in-the-middle attacks. This type of attacks occurs when a malicious node intercepts packets intended for other nodes by poisoning the ARP caches of its unsuspecting neighbors. To create the attack, the malicious node sends ARP requests or responses mapping another node's IP address to its own MAC address.

To prevent this kind of attack, RHG96XX managed switch ensures that only valid ARP requests and responses are forwarded. Invalid and malicious ARP packets will be dropped by the switch. DAI relies mainly on DHCP snooping mechanism that listens to DHCP message exchanges. Then, DAI creates a bindings database of valid tuples of MAC address and IP address. DAI is related to the function of ARP Spoof Prevention described in Section 2.17.4. DAI will drop all ARP packets if the IP-to-MAC binding is not present in the DHCP snooping bindings database. However, if some static IP address is needed to pass through the switch, the user should add this static IP-to-MAC binding in the ARP Spoof Prevention webpage in Section 2.17.4. This static mapping is useful when nodes configure static IP address, DHCP snooping cannot be run, or other switches in the network do not run dynamic.

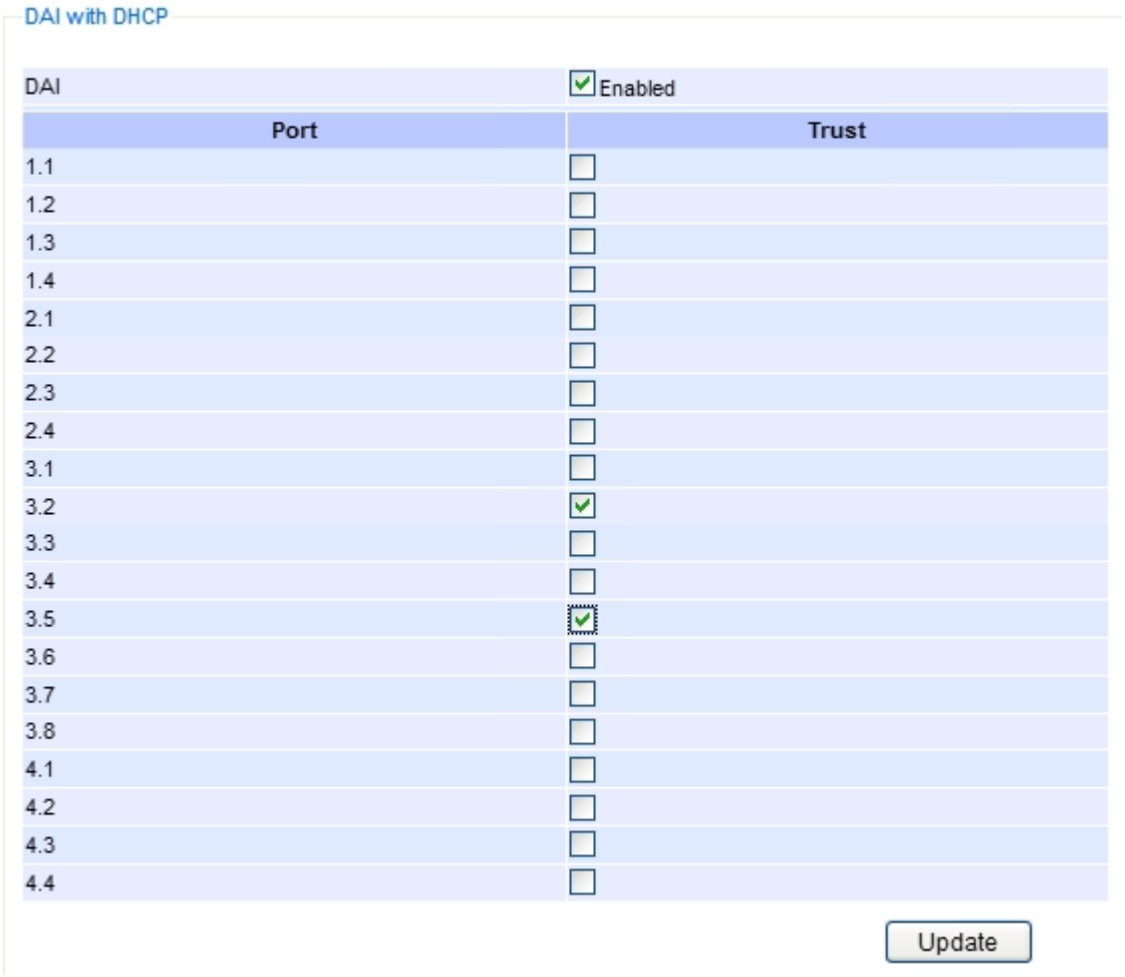


Figure 2.241 Dynamic ARP Inspection (DAI) with DHCP Webpage

To enable DAI, check the Enabled box for DAI option inside the DAI with DHCP box as shown in Figure 2.241. Then, check the box under the Trust column for corresponding Port number to configure that port number as trusted port. Then click **Update** button. The table inside the DHCP Data box will show information of the IP-to-MAC mapping, the Request Port and Lease Time of DHCP. To obtain the latest information on the bindings table, click on the **Refresh** button. Note that if the DHCP Snooping was not enabled before enabling the dynamic ARP inspection with DHCP, the user will encounter the message shown in Figure 4.2.

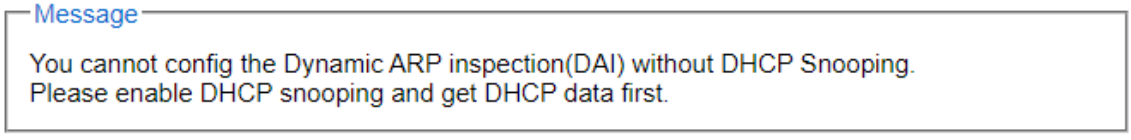


Figure 2.242Error Message for Dynamic ARP Inspection when DHCP Snooping was disabled

2.18 ERPS Ring

Ethernet **R**ing **P**rotection **S**witching (**ERPS**)is a protocol for Ethernet layer network rings. The protocol specifies the protection mechanismforsub-50ms delay time. The ring topology provides multipoint connectivity economically by reducing the number of links. 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 2.243 depicts an example of ring topology forming by four Atop's managed switch EH7520 series.

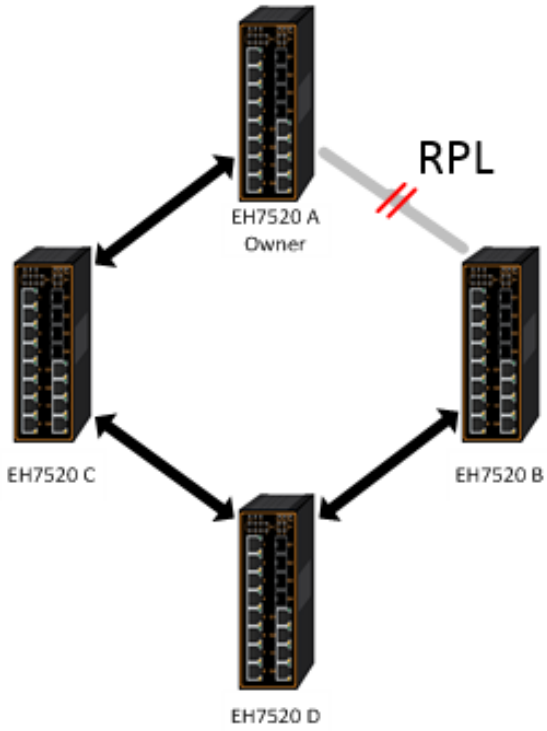


Figure 2.243An Example of Ring Topology (Example made on EH7520)

Figure 2.243 shows that each Ethernet Ring Node is connected to its adjacent Ethernet Ring Nodes participating in the same Ethernet Ring using two independent links (i.e. two ways).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 Owner Node. Thus, loops can be avoided by this mechanism. In case an Ethernet ring failure occurs, one designated Ethernet Ring Node called 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.

Atop's RHG9XXX series industrial managed switches provide a number of Ethernet ring protocol. The **ERPS/Ring** section is subdivided into six menus as shown in Figure 2.244, which are: **ERPS Setting**, **iA-Ring Setting**, **C-Ring Setting**, **U-Ring Setting**, **Compatible-Chain Setting,** and **MRP**.

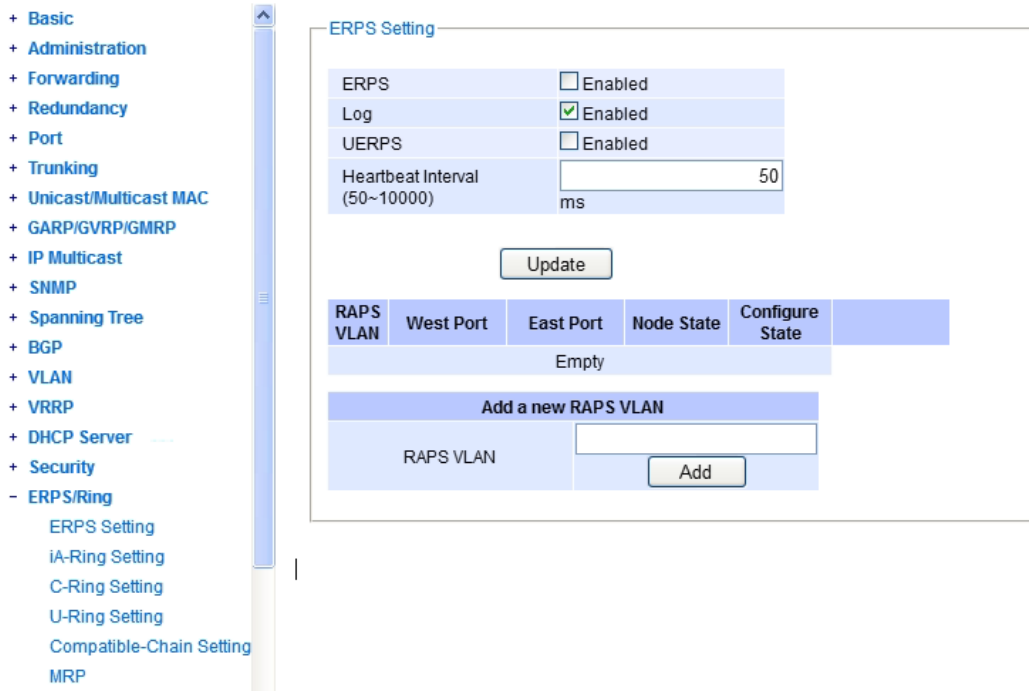


Figure 2.244 ERPS/Ring Drowdown Menu

2.18.1 ESRP Setting

ERPS Setting webpage is shown inFigure 2.245. Note that the users should disable the **DIP Switch Control** in Section 2.3.12 first in order to set up ERPS parameters. To set up ERPS on the current managed switch, please follow the following steps:

1. Enable the ERPS by checking on the **ERPS**'s **Enabled** checkbox.
2. If the users would like to keep the log, please also check the **Log**'s **Enabled** checkbox.
3. Optionally, if the users want the switch to periodically check the status of the neighboring switches on the ring topology using heartbeat packets then the user can check the **UERPS**'s **Enabled** checkbox. Note that when this feature is enabled, the recovery time of the ring topology may be longer.
4. Optionally, the users can fine tune the heartbeat interval by changing the default value 50 milli-seconds to the desired value.
5. Click on the **Update** button.
6. Skip down to **Add a new RAPS VLAN** section at the bottom of the webpage. Enter the desired **RAPS VLAN** ID in the field and click the **Add** button. The VLAN ID can be the value between 1 to 4094. Table 2.55 summarizes the fields in ERPS Setting webpage.

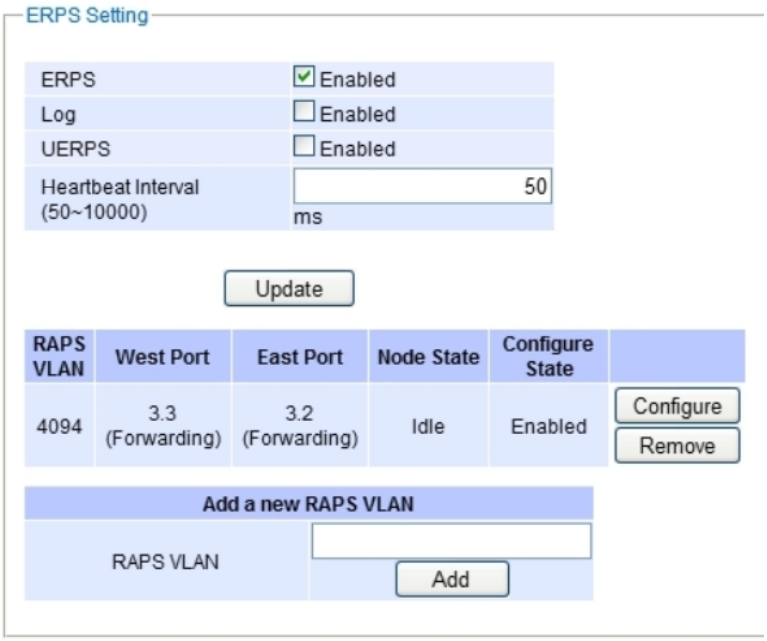


Figure 2.245ERPS Setting Webpage

Table 2.55Descriptions of ERPSSetting

Label	Description	Factory Default
ERPS	Choose whether to enable ERPS or not	Disabled
Log	Choose to enable log	Enabled
UERPS	Choose whether to enable UERPS. When UERPS is enabled, ring ports periodically sent a "heartbeat"packet to peer ring ports in order to determine whether the link path (etc. wireless bridge)is failure or alive. If peer ring port cannot receive "heartbeat"packets over 3 packets, the ring port will enter protection state. Note:This function affects the recovery time to more than 20 ms.	Disabled
Heartbeat Interval	Set the Heartbeat Interval.Range from 50 to 10000 milliseconds.	50 ms
RAPS VLAN	Create the ring by specifying the R-APS VLAN ID of the ring. VLAN ID ranges from 1 to 4094.	4090

7. Click the **Configure** button on the right side of the webpage that corresponding to the RAPS VLAN that was entered in previous step. A new webpage will be displayed for the users to config additional parameters**for ERPS RAPS VLAN Setting** as shown in Figure 2.246.
8. Configure the RAPS VLAN's **Status**, **West Port**, **East Port**, **RPL Owner**, **RPL Port**, **WTR Timer**, **Holdoff Timer**, **Guard Timer**, **MEL**, and **Propagate TC**. Detail description of these parameters are summarized in Table 2.56. Then, click **Update** button to finish the setting up of new RAPS VLAN.

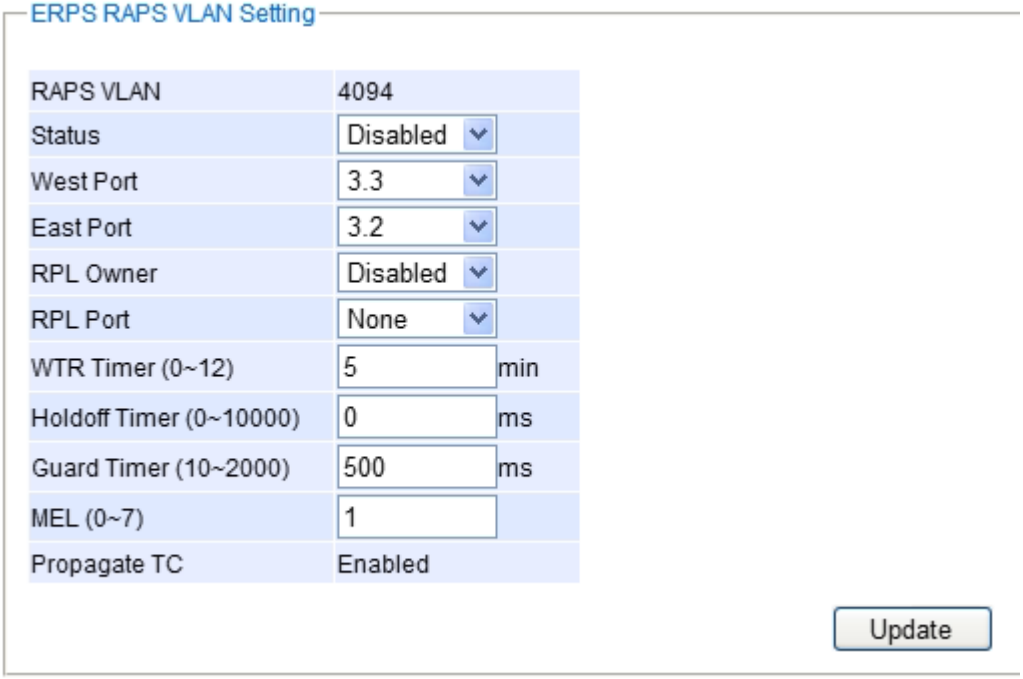


Figure 2.246ERPS RAPS VLAN Setting Webpage

Table 2.56Description of ERPS VLAN Setting

Label	Description	Factory Default
ERPS VLAN	Indicate current RAPS VLAN IDto be configured	4090
Status	Choose to enable ERPS with this particular VLAN	Disabled
West Port	Choose the *West Por*t of the RPL	Port1
East Port	Choose the *East Por*t of the RPL	Port2
RPL Owner	Choose to enable Owner Function	Disabled
RPL Port	Select the *Owner Port*which is either West Port or East Port or None.	None
WTR Timer	Set the wait-to-restore (WTR) time of the ring in minutes. Lower value has lower protection time. Range of the WTR Timer is from 0 to 12 minutes.	5
Holdoff Timer	Set the holdoff time of the ring. Range of the Holdoff Timer is from 0 to 10000 milliseconds.	0
Guard Timer	Set the guard time of the ring. Range of the Guard Timer is from 0 to 2000 milliseconds.	500
MEL	Set the maintenance entity group level (MEL)of the ring. Range of MEL is from 0 to 7.	1
Propagate TC	Indicate the topology change propagation of the ring ability.	Enabled

2.18.1.1 Example of ERPS Settings

To allow the users to understand the setting up of ERPS on the RHG9XXX industrial managed switches, this subsection provides an example of ERPS setup with four Atop's managed switches as shown in Figure 2.247.Assuming that the ring network has RHG9XXX A, RHG9XXX B, RHG9XXX C, and RHG9XXX D. There is an RPL between RHG9XXX A and RHG9XXX B. Note that the figure is based on the EH7520 model but it is applicable to any of RHG9XXX models.

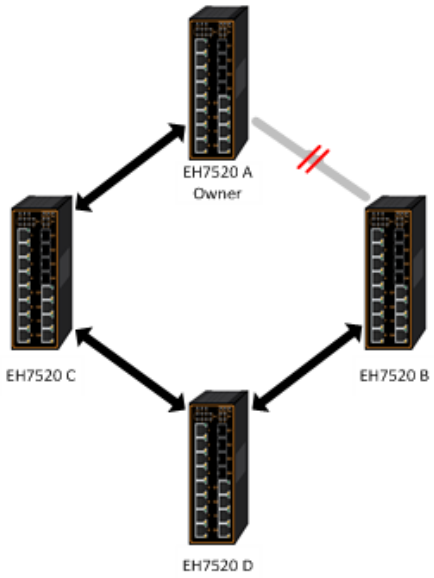


Figure 2.247Example of Ring Topology for ERPS Setup (Example made on EH7520)

For each switch, please follow the procedure outline in previous section. First, enabling the ERPS and then add the RAPS VLAN =8. On each managed switch, the users can configure ARPS VLAN Setting according to Table 2.57.

Table 2.57Setting Configuration for Switch A, B, C and D

EHX7XXX	**A**	**B**	**C**	**D**
RAPS VLAN	8	8	8	8
ERPS RAPS	Enabled	Enabled	Enabled	Enabled
West Port	1	1	1	1
East Port	2	2	2	2
RPL Owner	Enabled	Disabled	Disabled	Disabled
RPL Port	West	None	None	None

2.18.1.2 UERPS Settings (Optional)

The following procedure outlines the **UERPS**Setting under the **ERPS Setting**. You can follow them as an exercise.

1. Prepare two managed switches (Switch A and Switch B). We will use Port 7 and Port 8 on both switches for redundancy.
2. Connect Switch A and Switch B to the network or PC so that you can access them. For simplicity, the users can use Port 1 for Web configuration on both switches.
3. Open Device Management Utility(described in Chapter 5) and change the IP address of Switch B or both switchessuch thatthe IP addresses will not be conflicting.
4. Open Switch A and B's WebUI and setup ERPS settings like the following. Enable ERPS, Log, and UERPS accordingly as shown in Figure 2.248. Then, press **Update**button for the changes to take effect.

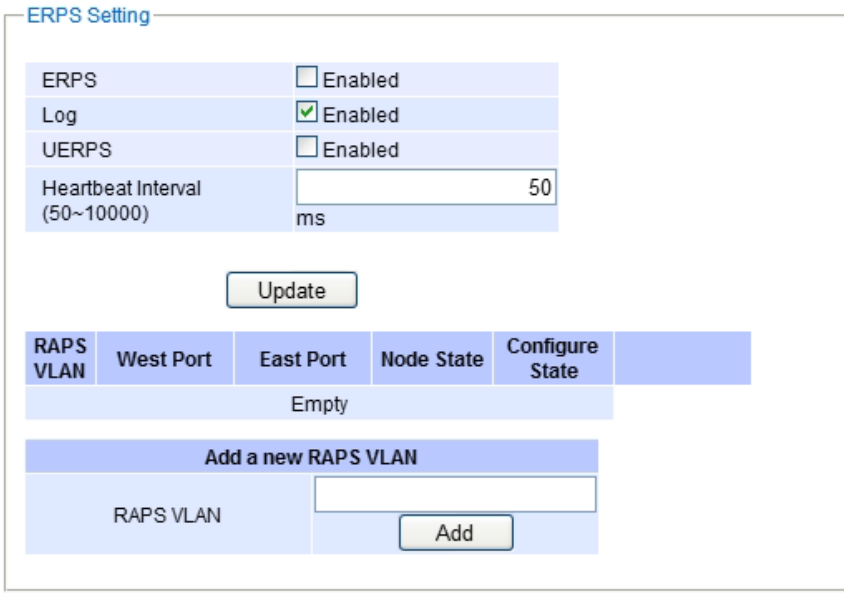


Figure 2.248Example of Switch A's ERPS settings

5. On Switch A, Click **Configure**button on RAPS VLAN and inputsettings as shown in Figure 2.249.

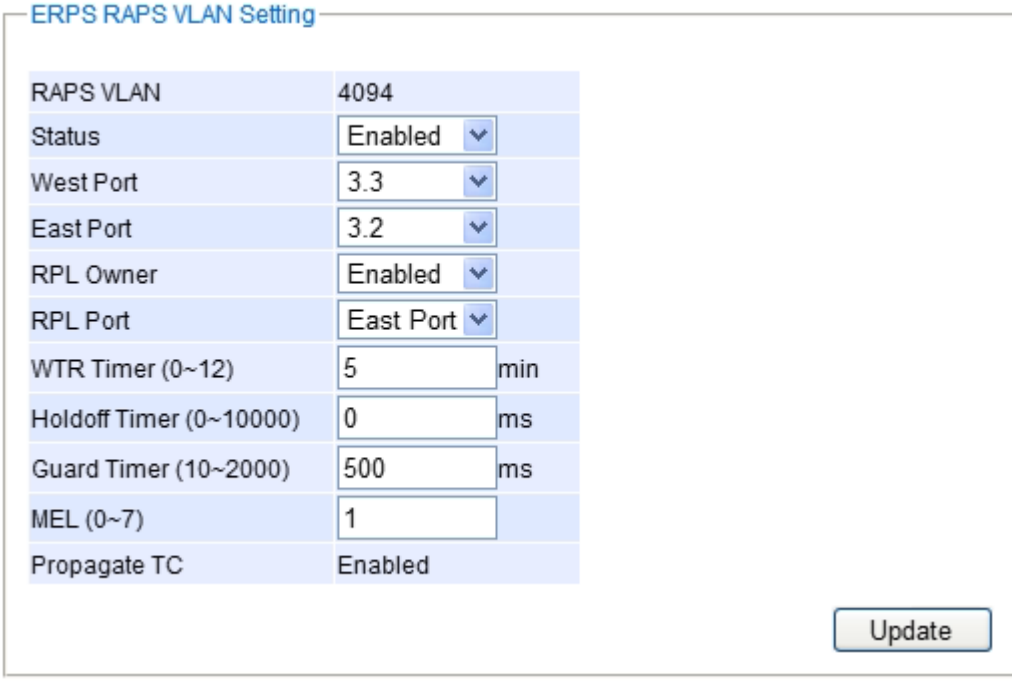


Figure 2.249Example of SwitchA's RAPS VLAN Settings

6. Open Switch B's WebUI and input settings for ERPS as shown in Figure 2.250.

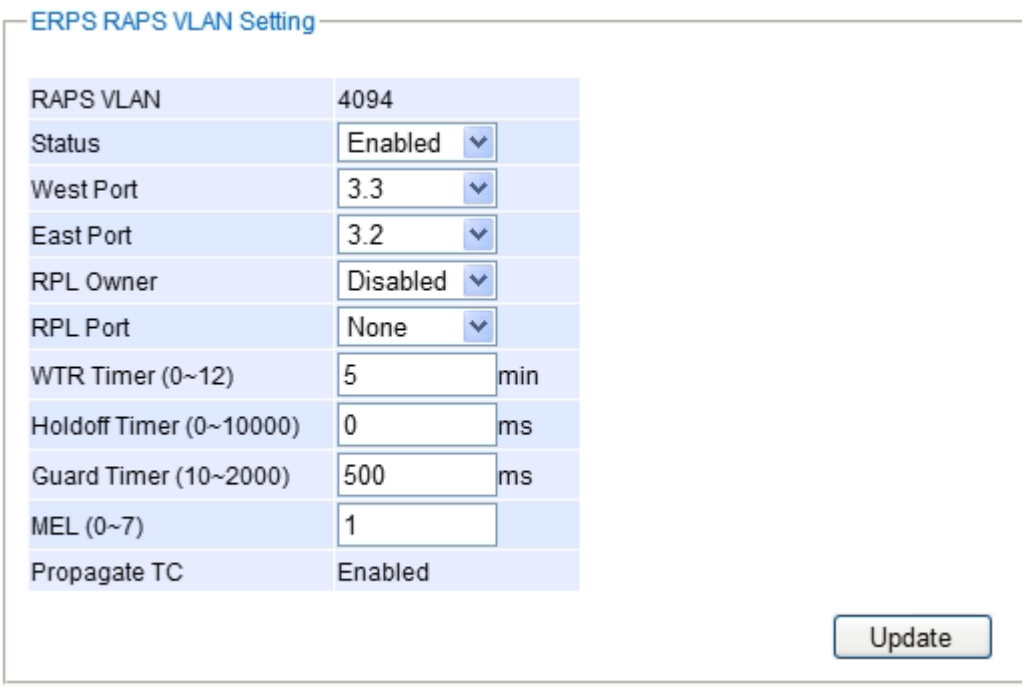


Figure 2.250Example of Switch B's RAPS VLAN Setting

7. Connect Switch A's Port 7 to Switch B's Port 8, andconnect Switch A's Port 8 to Switch B's Port 7 (like cross-over)for the redundancy port.
8. If everything is setup properly, you will find Switch A having the following ERPS state as shown in Figure 2.251.Also,it will automatically block Port 8 to prevent a network loop.

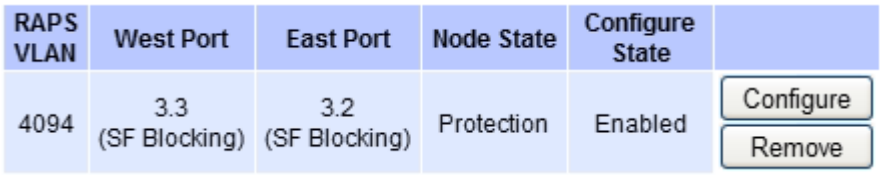


Figure 2.251Switch A's ERPS state

9. From here on, the users can add another bridgebetween the two managed switches.

2.18.2 iA-Ring Settings

The Atop's managed switch is designed to be compatible with iA-Ring protocol for providing better network reliability and faster recovery time for redundant ring topologies. It is in the same category as R Rings, but with its own protocol.It has been a successful development that reduces recovery time to less than 20 ms. iA-Ring can be used for any single ring, which is shown in thediagram below (Figure 2.252).

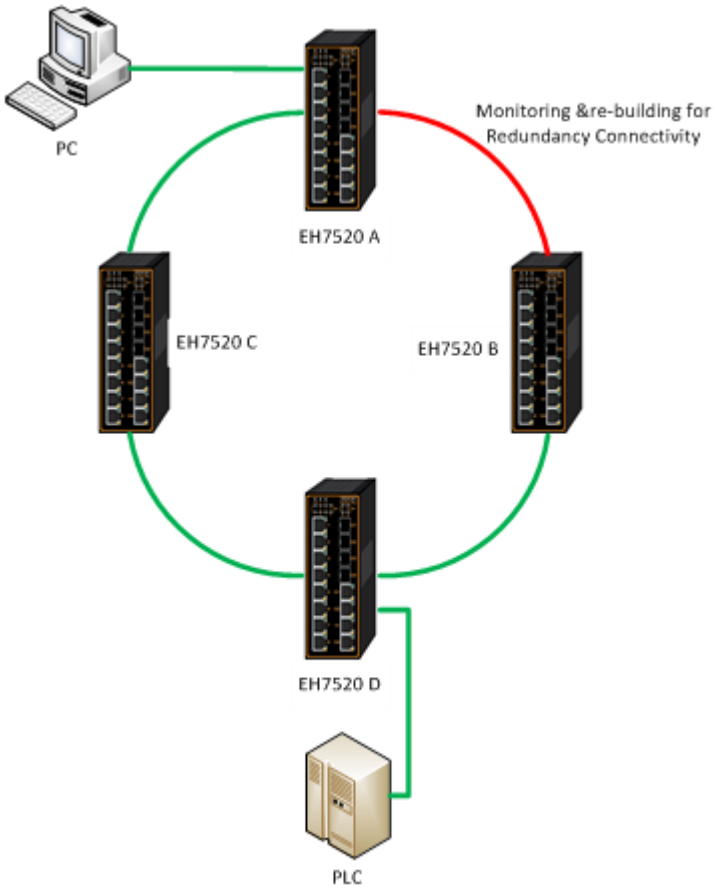


Figure 2.252iA-Ring Example Topology (Example made on EH7520)

Figure 2.253shows **iA-Ring Setting** webpage. The iA-Ring redundancy protocol can be enabled on this page. Note that theusers should disable **DIP Switch Control**as described in Section 2.3.12and disable**ERPS** as described in Section2.18.1first in order to enable/configure iA-Ring parameters on the web browser. Please follow the simple steps below based on Figure 2.253 to setup the iA-Ring.

1. Enable the **iA-Ring** by selecting **Enabled** from the dropdown list.
2. Choose whether the current managed switch is going to be the **Ring Master** by enabling the **Ring Master** option.
3. Select the **1st Ring Port** from the dropdown list.
4. Select the **2nd Ring Port** from the dropdown list.
5. Click on the **Update** button to save the change and allow the configuration to take effect.
6. Check the latest status of the iA-Ring configuration by clicking on the **Refresh** button.

Note that the lower part of the iA-Ring Setting webpage shows the **Status** of the iA-Ring which provides its **State**, **1st Ring Port Status** and **2nd Ring Port Status**. The description of the iA-Ring setting is summarized in Table 2.58.

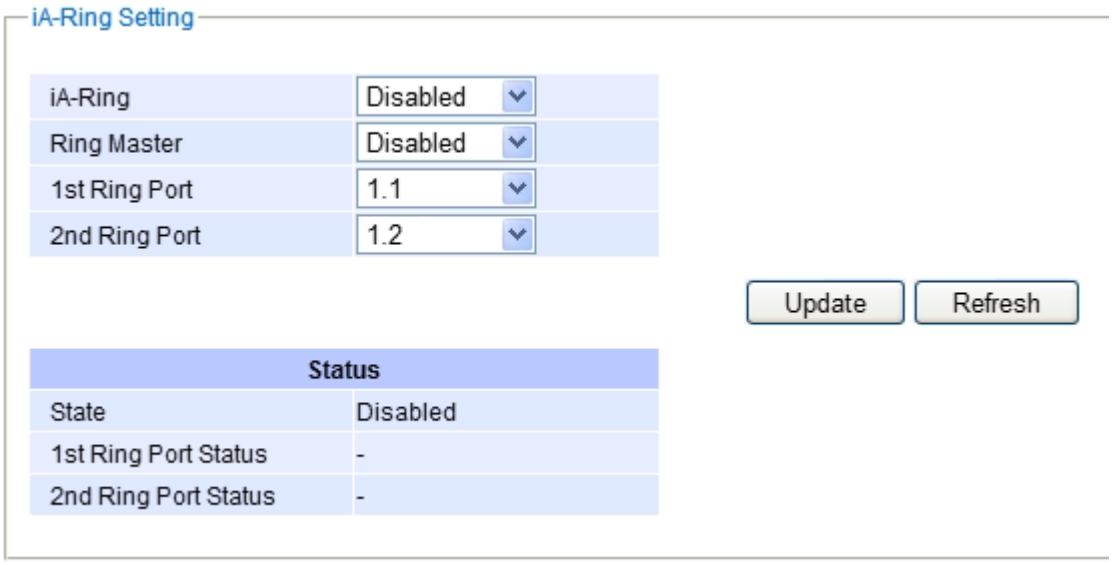


Figure 2.253iA-Ring Setting Webpage

Table 2.58Descriptions of iA-Ring Setting

Label	Description	Factory Default
iA-Ring	Enable iA-Ring or disable iA-Ring.	Disabled
Ring Master	Enabled:Master Mode. Disabled:Slave Mode.	Disabled
1st Ring Port	Select the primary port for the iA-Ring.	1.1
2nd Ring Port	Select the backup port for the iA-Ring.	1.2

2.18.3 C-Ring(Compatible-Ring) Settings

Compatible-Ring (**C-Ring**)is similar to iA-Ring. The only difference isthat it can be used for MOXA rings as well. For more information about this redundant ring protocol, please contact AtopTechnologies.

Figure 2.254shows how to set the Compatible-Ring (**C-Ring**)redundancy protocol. Note that the users should disable **DIP Switch Control**as described in Section 2.3.12and **ERPS**as described in Section 2.18.1first in order to enable/configure Compatible-Ring parameters on the web browser. Please follow the simple steps below based onFigure 2.254 to setup the C-Ring.

1. Enable the **C-Ring** by selecting **Enabled** from the dropdown list.
2. Select the **1st Ring Port** from the dropdown list.
3. Select the **2nd Ring Port** from the dropdown list.
4. Click on the **Update** button to save the change and allow the configuration to take effect.

Note that the lower part of the C-Ring Setting webpage shows the **Status** of the C-Ring which provides its **State**, **1st Ring Port Status** and **2nd Ring Port Status**. The description of the C-Ring setting is summarized in Table 2.59.

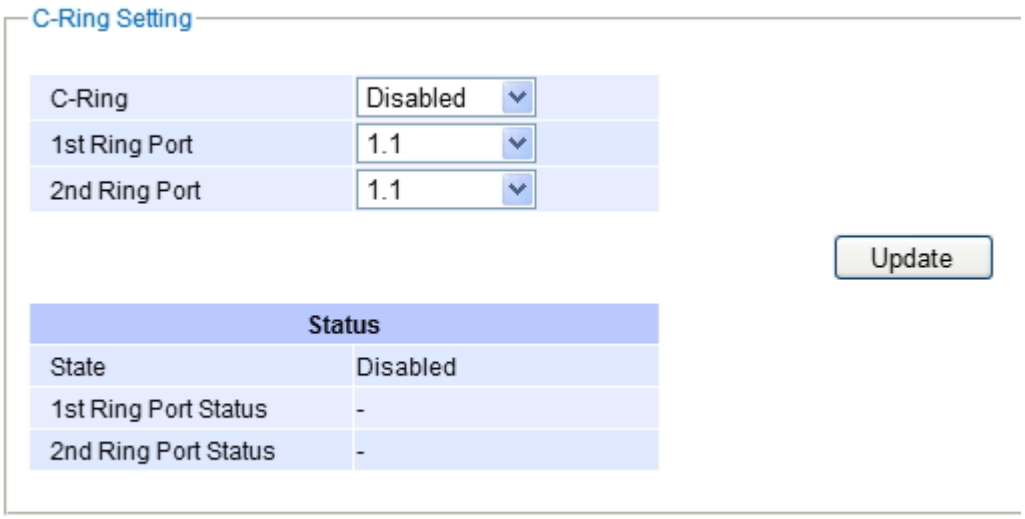


Figure 2.254Compatible-Ring (C-Ring) Setting Webpage

Table 2.59Descriptions of Compatible-Ring Setting

Label	Description	Factory Default
C-Ring (Compatible-Ring)	Enables Compatible-Ring or disable Compatible-Ring	Disabled
1st Ring Port	Selects the primary port for the Ring	1.1
2nd Ring Port	Selects the backup port for the Ring	1.1

2.18.4 U-Ring

This section enables the setup of U-Ring (Unicast Ring) on the managed switch. The U-Ring could provide redundancy connection between two RHG9XXX industrial managed switches which are not directly connected by physical wires but by two additional network devices on each switch**.** There are two examples of U-Ring application presented here to provide as guidelines when to choose this U-Ring feature.

First example is depicted in Figure 2.255 where there are two EH7520 managed switches. On each switch it is connected to two wireless Access Points(AP) via two different Ethernet LAN ports. Both wireless Access Points are connected to another two wireless Access Points as two separate wireless bridge connections. Based on Figure 2.255, EH7520 A has AP 1 on port 8 and AP 3 on port 7 while EH7520 B has AP 2on port 7 and AP 4 on port 8. The AP 1 and the AP 2 are connected as wireless Bridge Connection 1 and the AP 4 and the AP 3 are connected as wireless Bridge Connection 2.

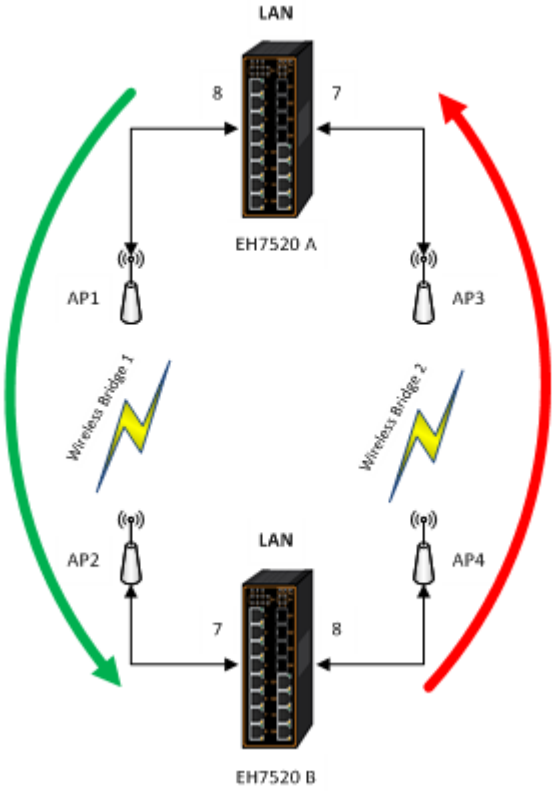


Figure 2.255 Example 1 of Two Wireless Bridge U-ring (Example made on EH7520)

Second example is illustrated in Figure 2.256 where there are also two EH7520 managed switches. On each switch it is connected to two wired Access Points (AP)via two different Ethernet LAN ports. Both wired Access Points are connected to another two wired Access Points as two separate wired bridge connections. Based on Figure 2.256, EH7520 A has AP 1 on port 8 and AP 3 on port 7 while EH7520 B has AP 2 on port 7 and AP 4 on port 8. The AP 1 and the AP 2 are connected as wired Bridge Connection 1 and the AP 4 and the AP 3 are connected as wired Bridge Connection 2. There are two physical lines between both pair of Aps. The U-ring protocol could be used in this environment. The different of this example from the previous example is that the AP_x could be:

- **Unmanaged-switch**
- **Transceiver**
- **XDSL bridge**

Note that care should be taken that if a dumbswitch is used as an AP (**A**ccess **P**oint). The one on the other side must be a dumbswitch as well. Again, care should also be taken when connecting the cables to the ports.

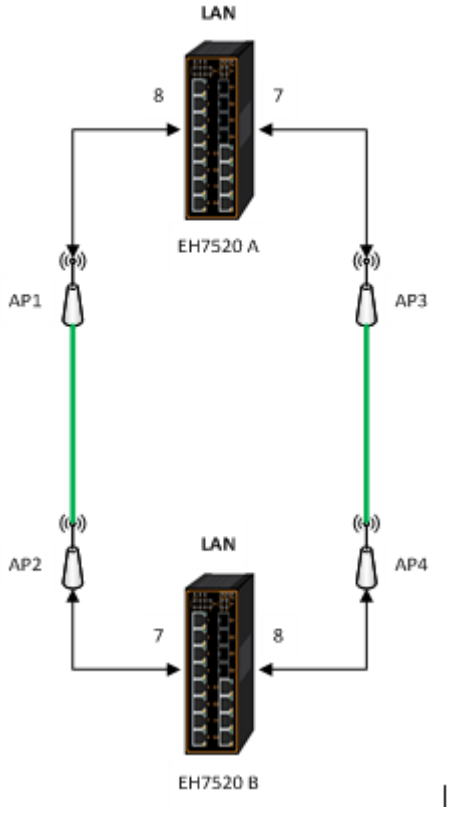


Figure 2.256 Example 2 of Two Wired Bridge U-ring (Example on EH7520)

To setup the U-Ring, the users need to configure a number of parameters on U-Ring Setting webpage as shown in Figure 2.257.Please follow the simple steps below to setup the U-Ring.

1. Enable the **U-Ring** by selecting **Enabled** from the dropdown list.
2. Choose whether the current managed switch is going to be the**Ring Master** by enabling the **Ring Master** option.
3. Select the **1st Ring Port** from the dropdown list.
4. Select the **2nd Ring Port** from the dropdown list.
5. Optionally, set the **Heartbeat Expire**periodwhich could be between 100 to 10000 milliseconds. Note that the default period is 100 ms.
6. Click on the **Update** button to save the change and allow the configuration to take effect.
7. Check the lateststatus of the U-Ring configuration by clicking on the **Refresh** button.

Note that the lower part of the**U-Ring Setting** webpage shows the **Status** of the U-Ring which provides its **State**, **1st Ring Port Status** and **2nd Ring Port Status**. The description of the U-Ring setting is summarized in Table 2.60.

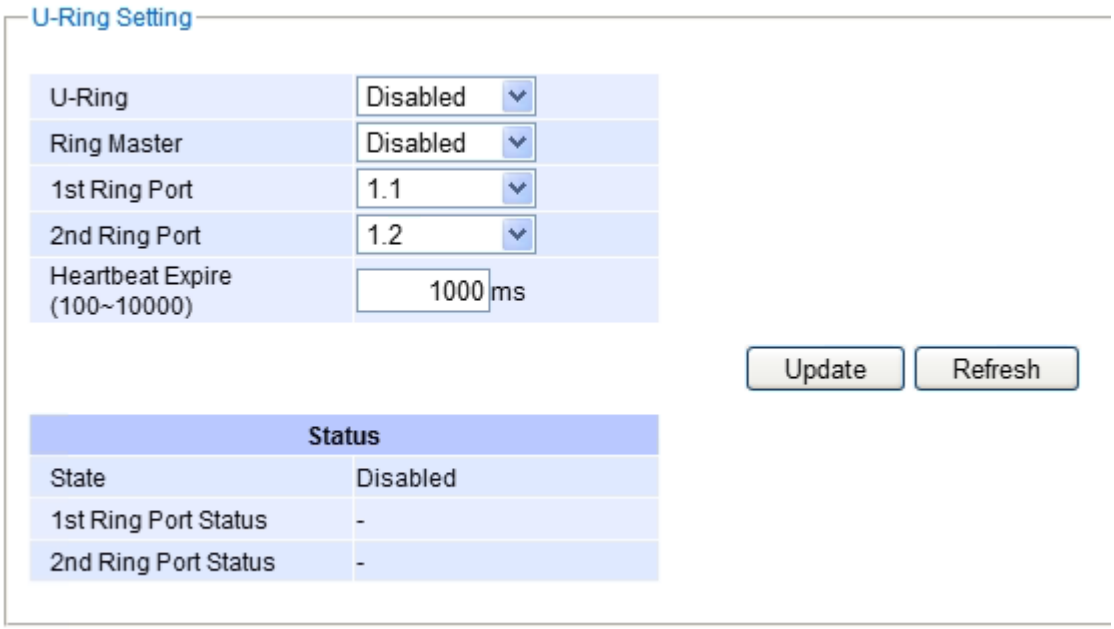


Figure 2.257U-Ring Setting Webpage

Table 2.60Descriptions of U-Ring Setting

Label	Description	Factory Default
U-Ring	Enabled or disabled the Unicast ring.	Disabled
Ring Master	Enabled or disabled this switch as the Ring Master of the Unicast Ring. For Ring Slave configuration, leave this option as disabled.	Disabled
1st Ring Port	Select which port on the managed switch will be the 1st Ring Port.	1.1
2ndRing Port	Select which port on the managed switch will be the 2nd Ring Port.	1.2
Heartbeat Expire	Time interval between checking-packets.	1000
Update	Click this button to allow the configuration to take effect.	-
Refresh	Obtain the latest status of the U-Ring Setting by clicking on this button.	-
State	Shows whether the device's state is normal or protected.	Disable
1st Ring Port Status	Displays the status of the 1st Ring Port.	-
2nd Ring Port Status	Displays the status of the 2nd Ring Port.	-

2.18.5 Compatible-Chain Settings

The **Compatible-Chain Setting**is provided on Atop's managed switches for compatible networking with Moxa switch's **Turbo Chain**. The MOXA's Turbo Chain is a technique that usesthe chain network topology and links the two ends (two network devices such as industrial managed switches)of the chain to a commonLAN. This can also be viewed as a form of Ring Topology. This Turbo Chain can provide redundancy on any type of network topology or on complex network topology such as multi-ring architecture. The Turbo Chain can create flexible and scalable topologies with a fast media-recovery time.

The fist switch on the **Compatible-Chain**will have a **Role State** as **Head** switch. The other switches along the **Compatible-Chain** will have a **Role State** as **Member** switches.The last switch on the **Compatible-Chain** will have a **Role State** as **Tail** switch.For Head switch, the first port which is connected to the common LAN is called **Head Port**, while the second port which is connected to the next switch in the Compatible-Chain is called **Member Port**. For **Member** switches, both ports of the Member switches are called **1st Member Port** and **2nd Member Port**. For **Tail**

switch, the first port which is connected to another Member switch is call **Member Port**, while the second port which is connected to the common LAN is called **Tail Port**. In Turbo Chain configuration, the Head Port is the main path while the Tail Port is the backup path of the redundant topology. During no link-failure operation on the chain's path, all traffic will be forwarded to the Head Port to the common LAN. When there is a failure on the path of the chain, the Tail Port will be used for forwarding the traffic to the common LAN.

To configure Compatible-Chain, select the Compatible-Chain menu under the ERPS/Ring Section. Figure 2.258 shows the Compatible-Chain Setting webpage.

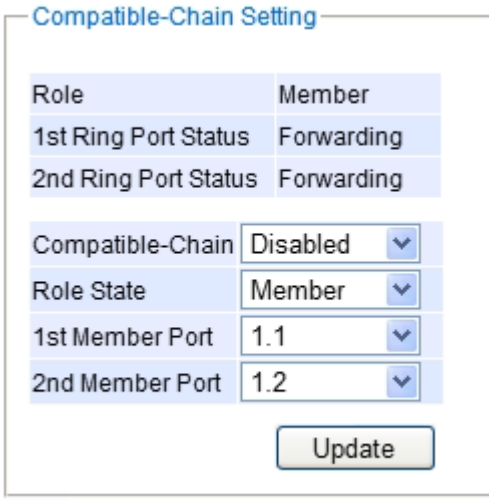


Figure 2.258 Compatible-Chain Setting Webpage

Please follow the simple steps below to setup the Compatible-Chain.

1. Enable the **Compatible-Chain** by selecting **Enabled** from the dropdown list.
2. Choose the **Role State**whether the current managed switch is going to be the **Head**, **Member** or **Tail** of the chain from the dropdown list of **Role State**.
3. If the current switch is the **Head** switch then select the **Head Port** from the dropdown list and select the**Member Port** from another dropdown list.
4. If the current switch is the **Member** switch then select the **1st Member Port** from the dropdown list and select the 2nd**Member Port** from another dropdown list.
5. If the current switch is the**Tail**switch then select the **Tail Port** from the dropdown list and select the **Member Port** from another dropdown list.
6. Click on the **Update** button to save the change and allow the configuration to take effect.

Note that the upper part of the**Compatible-Chain Setting** webpage shows the **Status** of the current switch in the chain which provides its **Role**, **1st Ring Port Status** and**2nd Ring Port Status**. The description of the Compatible-Chain setting is summarized in Table 2.60.

Table 2.61 Descriptions of Compatible-Chain Setting

Label	Description	Factory Default
Role	Display the role of the current switch in the Compatible-Chain: Head, Tail, or Member.	Member
1st Ring Port Status	Display the status of the 1st Ring Port.	Forwarding
2nd Ring Port Status	Display the status of the 2nd Ring Port.	Forwarding
Compatible-Chain	Enabled or Disabled the Compatible-Chain Ring	Disable
Role State	Choose the role of the current switch in the compatible chain:Head, Tail, or Member.	Member
Head Port	Select a particular port from the dropdown list to be the Head Port of the compatible-chain.	1.1
Tail Port	Select a particular port from the dropdown list to be the Tail Port of the compatible-chain.	1.1
Member Port	Select a particular port from the dropdown list to be the Member Port of the compatible-chain.	1.2
1st Member Port	Select a particular port from the dropdown list to be the Member Port of the compatible-chain.	1.1
2nd Member Port	Select a particular port from the dropdown list to be the Member Port of the compatible-chain.	1.2

2.18.6 MRP

The Media Redundancy Protocol (MRP)is a data network protocol for Ethernet switch standardized by the International Electro technical Commission as IEC 62439-2.MRP is mostly used in and suitable for Industrial Ethernet applications. It allows rings of Ethernet switches to overcome any single failure with recovery time much faster than those achievable by Spanning Tree Protocol. It supports very fast failure recovery time. For example, a worst-case recovery time for 14 switches is about 10ms and for 50 switches is about 30ms.

The MRP includes following properties.

- It operates at the MAC layer of the Ethernet switches.
- It is a ring topology.
- Any single failure can be recovered.
- For switches in the network, there can be two roles:
  - Ring manager(MRM)
  - Ring client(MRC)
- For ring ports, there are three possible statuses:disabled, blocked, and forwarding.
  - Disabled ring ports drop all the received frames.
  - Blocked ring ports drop all the received frames except the MRP control frames.
  - Forwarding ring ports forward all the received frames.
- In normal case, one of the MRM ring ports is blocked to avoid looping and both ring ports of all MRCs are forwarding.
- When a path of the ring fail, the other port on the MRM will become active and forwarding.

The Media Redundancy Protocol (MRP)menu under the EPRS/Ring enables an implementation of a redundant PROFINET communication through ring topology without the need for switches. Figure 2.259 shows the MRP Setting webpage. Please follow the outlined steps here to setup the PROFINET's MRP:

1. Enter a desired **VLAN** ID in the field at the bottom of the **MRP** Setting webpage and click **Add** button as shown in Figure 2.259.

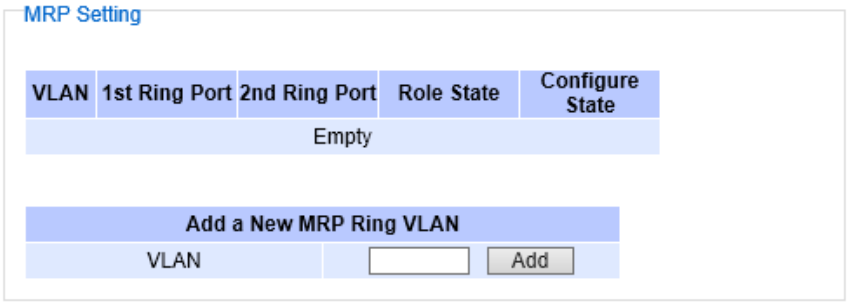


Figure 2.259 MRP Setting Webpage

2. After the MRP Ring is created with the desired VLAN, there will be an entry of the MRP VLAN on the table at the top of the page as shown in Figure 2.260. There will also be two new buttons at the end of the entry: **Configure** and **Remove**. The users can click on the Configure button the continue setting up the MRP Ring on the managed switch.

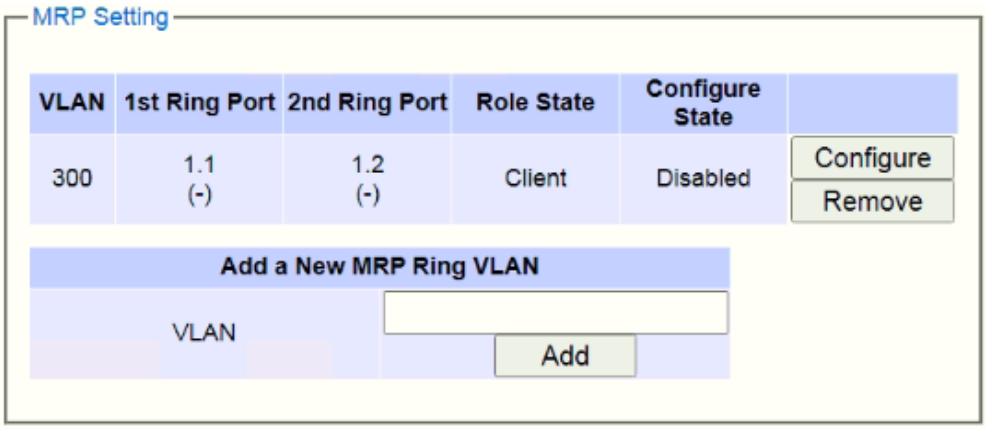


Figure 2.260 Example of PROFINET's MRP VLAN Entry

Table 2.62 Description of MRP Setting Webpage

Label	Description	Factory Default
VLAN	MRP Ring VLAN ID	Depend
Role State	Role status setting (Manager or Client)	Client
1st Ring Port	Port number and port status (Link Down, Blocked, Forwarding).	1.1
2ndRing Port	Port number and port status (Link Down, Blocked, Forwarding).	1.2
Configure State	Enabled or Disabled state of MRP Ring function	Disabled

3. After clicking the Configure button on the desired entry, a new webpage called MRP Ring Setting will show up as shown inFigure 2.261.

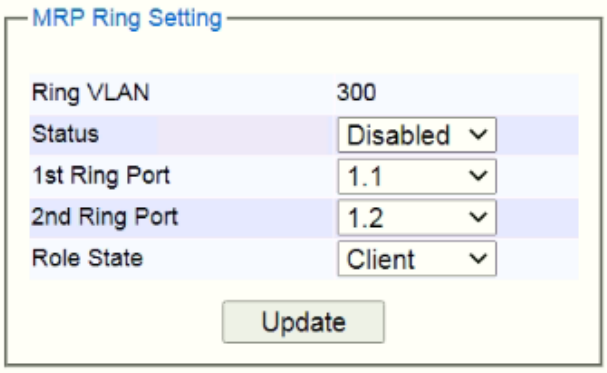


Figure 2.261 MRP Ring Setting Webpage

4. Then, the users can set MRP Ring parameters for the current switch, which are the **Status**, **1st Ring Port**, **2nd Ring Port**, and **Rote State** as described earlier.Table 2.62 summarizes the description of MRP Ring Setting parameters.

5. Click on the **Update** button to allow the configuration to take effect. Note that if there is other ERPS Ring Topology already setting up on the managed switch there may be an error message popping up as shown in Figure 2.262. Therefore, the users should disable the ERPS/Ring(Section2.18.1) and DIP Switch Control(Section 2.3.12)first before setting up this MRP Ring.

Figure 2.262 MRP Ring Setting Error Message

2.19 LLDP

Link **L**ayer **D**iscovery **P**rotocol (**LLDP**)is anIEEE802.1ab 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 neighbors. LLDP is a “one hop” unidirectional protocol in an advertising mode.

LLDP information can only be sent to and received by devices, nosolicit 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.

Link **L**ayer **D**iscovery Protocol (LLDP)section consists of **LLDP Setting** and **LLDP Neighbors**as shown in Figure 2.263.

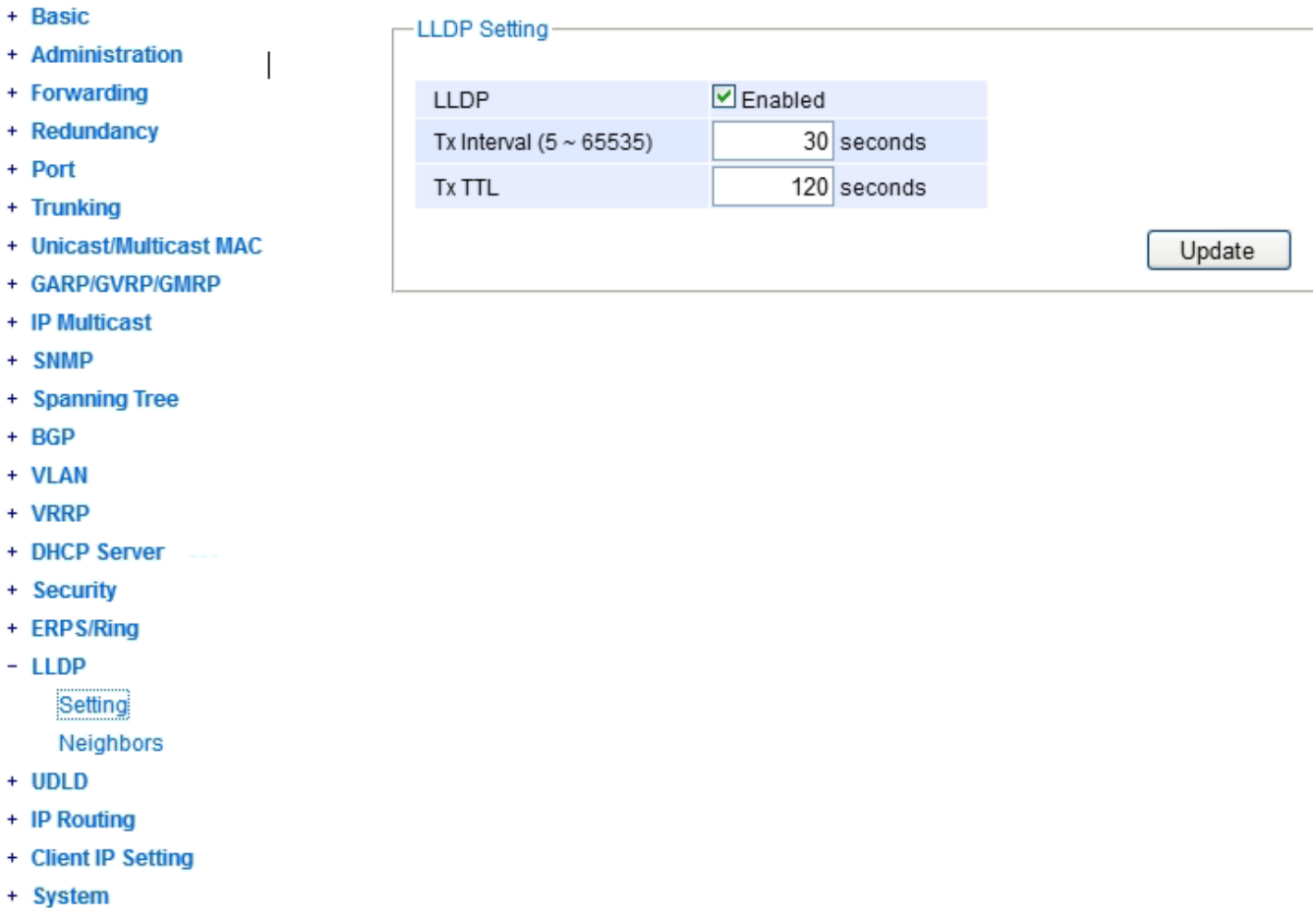


Figure 2.263 LLDP Dropdown Menu

2.19.1 LLDPSettings

InFigure 2.264, the LLDP Setting webpage allows users to have options for enabling or disabling the LLDP, as well as setting LLDP transmission parameters. This LLDP function should be enabled if users want to use Atop's Device Management Utility (formerly called Device View)to monitor the switches' topology of all LLDP devices in the network.For more information about using Device Management Utility, please refer to Chapter 5 of this document.Table 2.63 describes the LLDP Setting parameters which are transmit interval and transmit time-to-live of the LLDP advertisement packets.

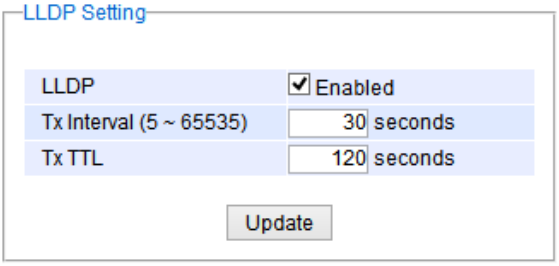


Figure 2.264LLDP Setting Webpage

Table 2.63Descriptions of LLDP Setting

Label	Description	Factory Default
LLDP	Choose to either enable or disable LLDP.	Enabled
Tx Interval	Set the transmit interval of LLDP messages. Range from 5 to 65535 seconds.	30
TxTTL	*Tx Time-To-Live*. Amount of time to keep neighbors' information.The recommend TTL value is 4 times of *Tx Interval*. The information is only removed when the timer is expired. Range from 5 to 65535 seconds.	120

2.19.2 LLDP Neighbors

This menu allows the user to view the LLDP's neighbor information of the managed switch as shown in Figure 2.265.The Neighbor Information table contains Chassis ID, Port ID, Port Description, Device Name, Device Description and Management Address on each Port of the managed switch. The users can click on the **Refresh** button to get the latest Neighbor Information table or click on the **Clear** button to clear all the information on the display Neighbor Information table.

An example of neighbor information table is depicted in Figure 2.266. Note that this example is based on a display format of an early version of EH7520 managed switch in which System Name is changed to Device Name and System Description is changed to Device Description in the latest version of RHG9XXX's firmware.

Table 2.64 summarizes the descriptions of each column of the LLDP's Neighbor Information.

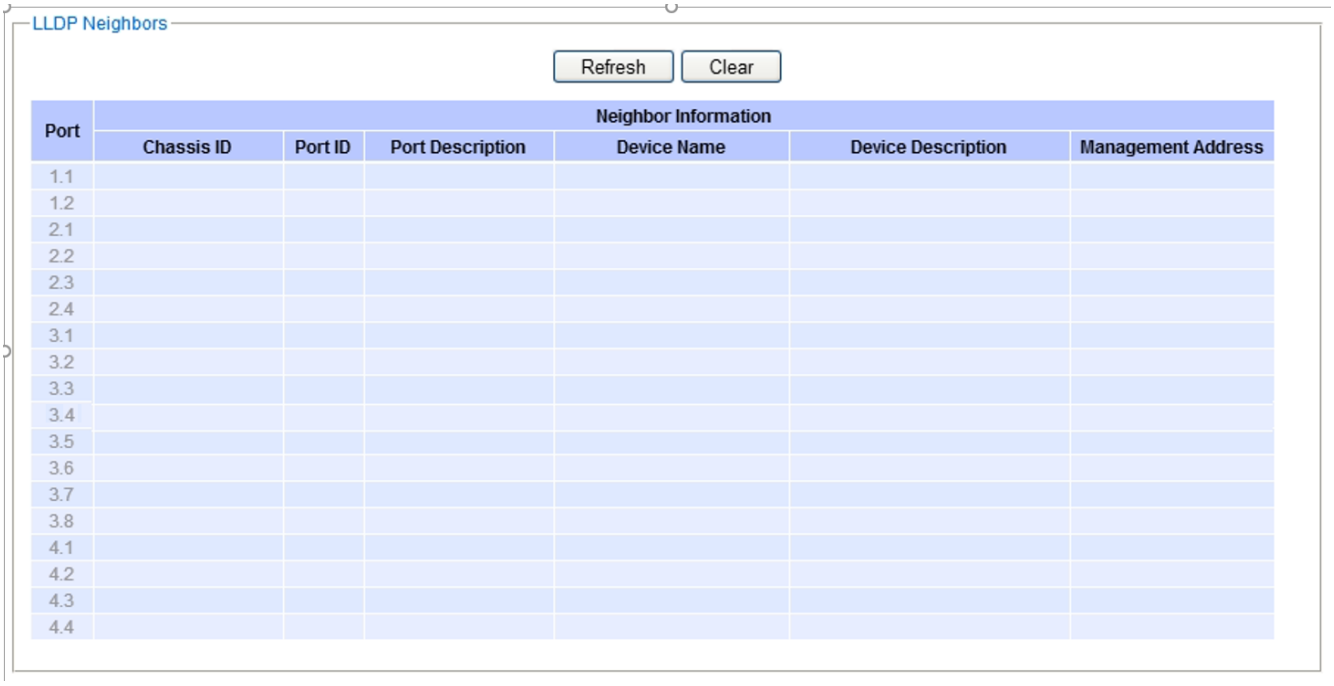
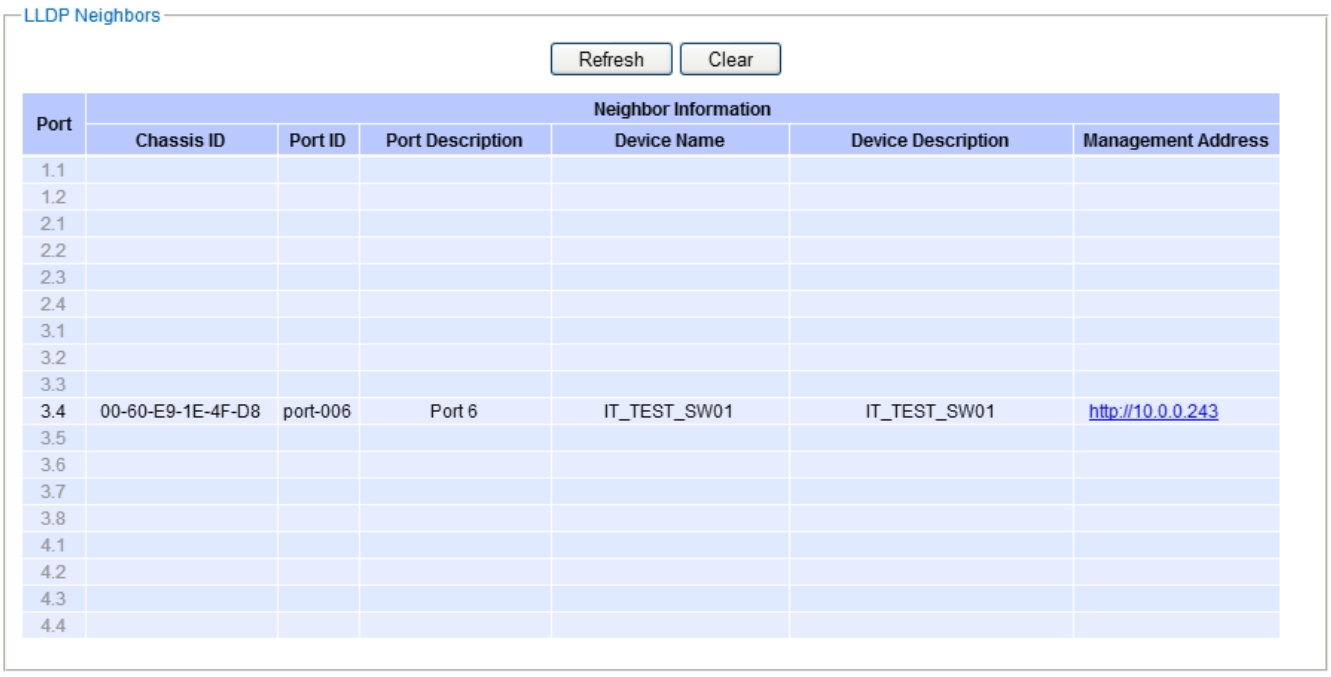


Figure 2.265LLDP Neighbors Webpage



Port	Neighbor Information					
	Chassis ID	Port ID	Port Description	Device Name	Device Description	Management Address
1.1						
1.2						
2.1						
2.2						
2.3						
2.4						
3.1						
3.2						
3.3						
3.4	00-60-E9-1E-4F-D8	port-006	Port 6	IT_TEST_SW01	IT_TEST_SW01	http://10.0.0.243
3.5						
3.6						
3.7						
3.8						
4.1						
4.2						
4.3						
4.4						

Figure 2.266Example of LLDP NeighborsWebpage

Table 2.64Descriptions of LLDP Neighbors Webpage

Label	Description
Port	Indicates particular port number of the switch.
Chassis ID	Indicates the identity of the neighbor of this particular port.
Port ID	Indicates the port number of this Neighbor.
Port Description	Shows a textual description of the neighbor port.
Device Name	Indicates the device name/hostname of the Neighbor.
Device Description	Shows a more detailed description of the neighbor's device.
Management Address	Indicates neighbor's management IP address.

2.20 UDLD

The Unidirectional Link Detection (UDLD) protocol is a protocol that can be used to prevent Layer-2 switching loops in the network. The network loop problem usually occurs in Spanning Tree network topology (mis-wiring or malfunction of the network interface). UDLD is a data link layer (Layer-2) protocol that keeps track of physical layer configuration (fiber or copper). It helps detect switching loops and one-way connections. UDLD protocol requires that two neighboring switches UDLD packets to detect the unidirectional link. UDLD packets are transmitted periodically (hello interval) to its neighbor switches on LAN ports that has UDLD protocol enabled. If the UDLD packets are not echoed back within a specific time, the port will be shut down and flagged as unidirectional link. ATOP's RHG96XX supports this protocol: the user can configure it under the UDLD menu as shown in Figure 2.267. Under the UDLD menu, there are three submenus: Setting, Port-info, and Reset.

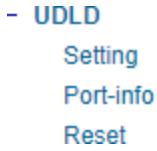


Figure 2.267 UDLD Menu

2.20.1 UDLD's Setting

To enable UDLD protocol on RHG96XX, the userneeds to configure UDLD VLAN first by electing the Setting submenu under the UDLD menu. The user needs to set the UDLD VLAN in the UDLD Port Setting part before enabling UDLD protocol. The user must select a VLAN ID from a drop-down list and then select one or multiple ports from the list of the UDLD Port Setting part on the webpage as shown in Figure 2.268. Then, click **Update** button at the end of the webpage to configure a UDLD VLAN. An entry of VLAN ID and UDLD Port will show up in the Current UDLD Setting part in the middle of the webpage.

Figure 2.268 UDLD Setting Webpage

Next, the user can configure UDLD protocol's parameters which are Hello interval and Recovery interval. The Hello interval can be a number between 5 to 100 seconds. This interval is the time that the switch will send the next echo packet. The default value is 7 seconds. The Recovery interval can be a number between 30 and 86400 seconds. This interval is a time for the switch to try to bring an UDLD port that was disabled back from a reset state. The default value is 120 seconds.

Note that typically, UDLD can be operated in two modes: Normal and Aggressive. In Aggressive mode, UDLD protocol can detect unidirectional links that were caused by one-way traffic on fiber-optic and twisted-pair links and that caused by misconnected interfaces on fiber-optic links. In normal mode, UDLD can detect unidirectional links that was caused by misconnected interfaces on fiber-optic connection. Currently RHG96XX supports only Aggressive mode which means that the user cannot choose the operation mode.

Finally, click on the Enable box for UDLD option at the top of the UDLD Setting partand click on the **Update** button under UDLD Setting part to enable the UDLD protocol on the managed switch. Note that the user needs to configure another managed switch on the other side of the port to successfully detect the unidirectional problem.

Note that if you did not follow the above procedure and only check the Enable box and click **Update** button at the top part of the webpage. An error message will be displayed as shown inFigure 2.269.

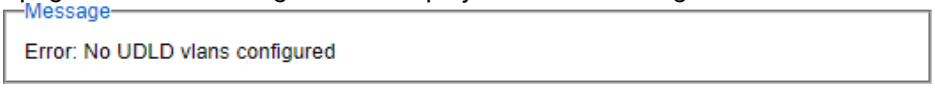


Figure 2.269 Error Message when No UDLD VLAN was configured

2.20.2 UDLD's Port-info

This submenu provides information about ports that are monitor for unidirectional problem called UDLD ports as shown in Figure 2.270. The user can check the information about VLAN ID, Port, Link, State, and Neighbor Information in each entry. The Neighbor Information also consists of Device ID, Device Name, Port ID, and Hello interval. An example of UDLD entry is depicted in Figure 2.270.

Figure 2.270 UDLD's Port-info Webpage with an Example

2.20.3 UDLD's Reset

This submenu allows the user to reset all UDLD ports that were shutdown by UDLD protocol as shown in Figure 2.271. The use can click on the **Reset** button to reset the UDLD port.

Figure 2.271 UDLD's Reset Webpage

2.21 IP Routing (Layer-3 Switching Features)

In this menu, the user can enable IP routing protocol on the RHG96XX Industrial L3 Managed Switch. There are three routing mechanisms that can be enabled on the managed switch: **IPv4 Static Routing**, **RIP (Routing Information Protocol)**, and **OSPF (Open Shortest Path First)**. Figure 2.272shows **the IP Routing** menu.

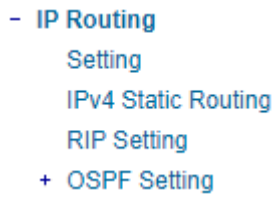


Figure 2.272 IP Routing Menu

2.21.1 IP Routing's Setting

To enable the Internet Protocol (IP)routing or Layer-3 (L3)routing function on the RHG96XX Industrial L3 Managed Switch, select the **IP Routing** menu, click **Enabled** box behind the **IP Routing Setting** option, and press the **Update** button as shown in Figure 2.273. Note that the default value of IP Routing is disabled. This IP routing option should be enabled before any other IP routing functions (static routing in Section 2.21.2and dynamic routing in Section 0 and Section2.21.4)can be used.

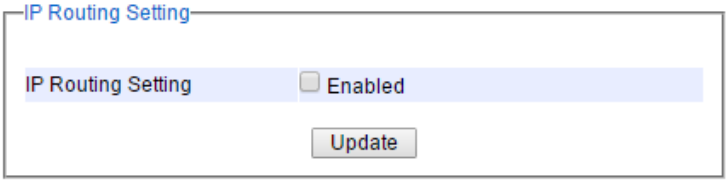


Figure 2.273 IP Routing Webpage

2.21.2 IPv4 Static Routing

Note: IPv4 Static Routing function is an old feature of firmware version 3.21 and is not available in firmware version 4.25.

Static routing is a form of routing based on IP address at OSI Layer 3 that occurs when a router uses a manually configured routing entry to forward packet. The users can define the routes by themselves by specifying what is the next hop (or the next router) based on IP address that the Layer 3 switch will forwarddata packet for a specific subnet.Note that to allow **IPv4 Static Routing** to operate properly, please enable the **IP Routing** function as described in Section2.21.1 above first. If the **IP Routing** function is not enabled, there will be an error message showing up as illustrated in Figure 2.274.

Figure 2.274 Error message when IP Routing is disabled.

By default, there is no IPv4 static routing entry in the routing table of RHG96XX industrial L3 managed switch. When the users would like to add a new IPv4 static routing, first select the **IPv4 Static Routing** submenu under the **Administration** menu as shown in Figure 2.275. Then, enter a static routing name in the **Name** field. Then, fill in the IP related information, which are the **Destination IP Address**, **Subnet Mask**, and **Gateway IP Address**. Finally, enter the value of the Metric for this route. Note that the routing metric will be used by the L3 switch to make routing decision. The default value for this field is 0 or lowest metric which is equivalent to a route to adefault gateway. Please click on the **Update** button to add the IPv4 static routing to the routing table of the L3 managed switch. An

example of a static routing entry is shown in Figure 2.276. Descriptions of IPv4 Static Routing configurations are summarized in Table 2.65.

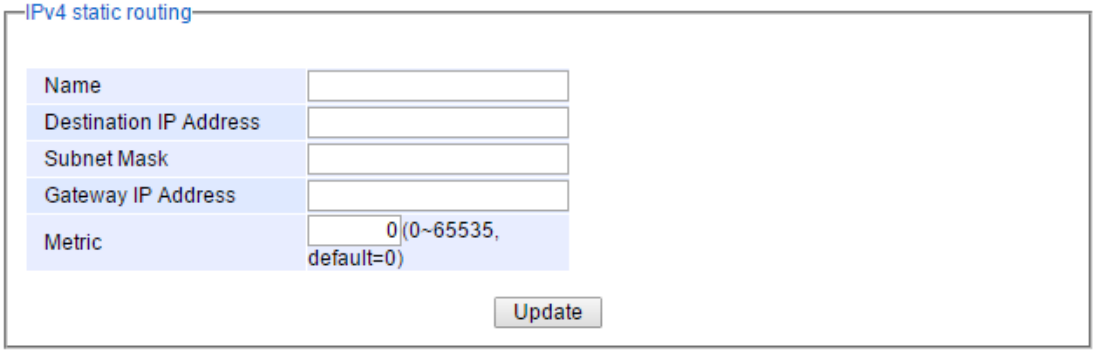


Figure 2.275 IPv4 Static Routing Webpage

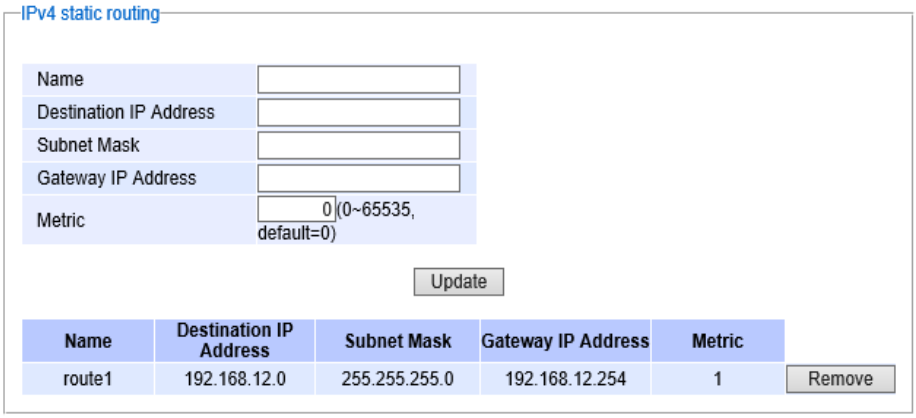


Figure 2.276 Example ofan Entry in IPv4 Static Routing Table

Table 2.65 Descriptions of IPv4 Static Routing Settings

Label	Description	Factory Default
Name	Name of an IPv4 static route (Max. 16 Characters)	Blank
Destination IP Address	IPv4 address of the interface of the next hop or router such as 192.168.12.0	Blank
Subnet Mask	Subnet mask of the IPv4 interface such as 255.255.255.0	Blank
Gateway IP Address	IPv4 address of the gateway to the next hop such as 192.168.12.254	Blank
Metric	The routing metric which is used to by L3 managed switch to make routing decision.Value is between 0 and 65535.	0

2.21.3 RIP Setting

The Industrial L3 managed switch also implements a dynamic routing protocol to allow automatically learning and updating of routing table.In this subsection, one of the dynamic routing protocol can be setup by the users. Routing Information Protocol (RIP)is a distance vector-based routing protocol that can make decision on which interface the L3 managed switch should forward Internet Protocol (IP)packet and can share information about how to route traffic among network devices that use the same routing protocol. RIP sends routing-update messages periodically

and when there is a change in network topology. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. RIP can also be used to automatically build up a routing table.

To enable the RIP, first check the **Enable** box as shown in Figure 2.277. Then, select the **Version** of RIP protocol from the dropdown box. Note that RHG96XX support RIP**Version 1** and **Version 2**. Then, choose the corresponding box for **Distribution**:**Connected** or**Static** or **OSPF**.Note that the Distribution option is to set which routing information the RIP will be used to populate its routing table. When the **Connected** box is selected, the RIP will add the connected routes (subnets directly connected to the RHG96XX's interface)to its routing table. When the **Static** box is selected, the RIP will add the static routes (configured in previous subsection)to its routing table. Finally, click on the **Update** button to allow the configuration of the RIP to take effect. Note that once there is any information about RIP routing information, it will be shown in the RIP Routing Table part at the bottom of the webpage.

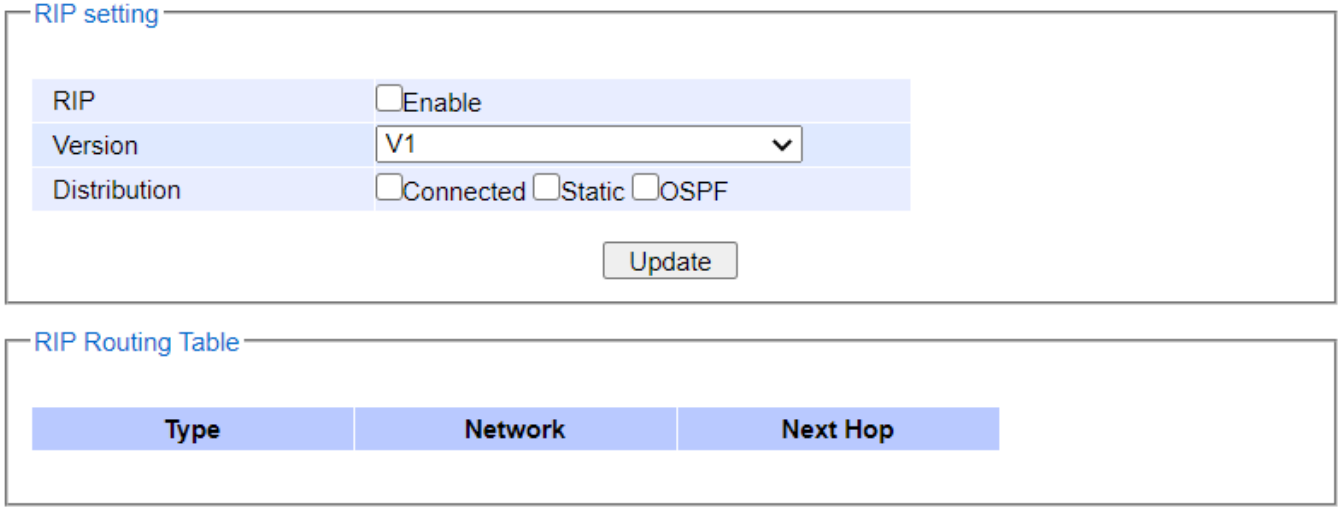


Figure 2.277 RIP Setting Webpage

2.21.4 OSPF Settings

Note: OSPF function is anold feature of firmware version 3.14 and is not available in firmware version 4.25.

OSPF (Open Shortest Path First) version 2 is another routing protocol supported by RHG96XX industrial L3 managed switch. It is described in RFC2328. OSPF is an IGP (Interior Gateway Protocol) which uses link states for route selection. It propagates link-state advertisements (LSAs) to its Neighbor switches. When compared with RIP (Routing Information Protocol) which is a distance vector-based routing protocol, OSPF can provide scalable network support and faster convergence time for network routing state. OSPF is widely used in large networks such as ISP (Internet Service Provider) backbone and enterprise networks.

To configure OSPF under the RHG96XX industrial L3 managed switch, the user can select the **OSPF Setting**submenu from the **Administration** menu as shown in the last item under the **Administration** menu inFigure 2.11. Under the **OSPF Setting** submenu, there are five more menus which are **Global Setting**, **Area Setting**, **Interface Setting**, **Virtual Link Setting**, and **Area Aggregation Setting** as shown in Figure 2.278.

Figure 2.278 OSPF Setting Submenu

2.21.4.1 OSPF Global Setting

To enable OSPF routing protocol on RHG96XX, first the user should enable it on the **Global Setting** webpage as shown in Figure 2.279. Checking the **Enable** box to activate the OSPF function and entering the **Router ID** for your RHG96XX industrial L3 managed switch. Note that the **Router ID** is in a form of IP address (not necessary be an actual IP address) or four groups of number between 0 and 255 which are separated by dots. This number can be any IP address which is only used by the OSPF process to uniquely identify the router. One algorithm for Router ID assignment is to choose the largest or smallest IP address assigned to the router. The last option for **OSPF Global Setting** is to enable re-distribution of routes into OSPF processwhich is called **Distribution** on the **Global Setting**webpage. Note that re-distribution is the use of a routing protocol to advertise routes that are learned by another routing protocol, static routes, or directly connected routes. The re-distribution of routes or **Distribution** in RHG96XX can come from **Connected** routes, **Static** routes, and/or **RIP**'s routes. The user can check any or all boxes of the corresponding routes behind the **Distribution** option that you want to re-distribute into OSFP routing protocol.After finished setting up the OSPF, click on the **Update** button to allow the setup to take effect.

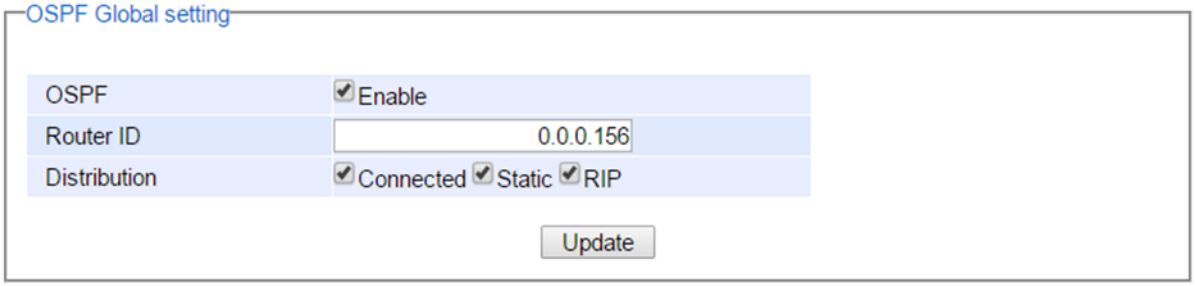


Figure 2.279 OSPF's Global Setting Webpage

Table 2.66 Descriptions of OSPF's Global Setting Webpage

Label	Description	Factory Default	Note/restriction
OSPF	Enable or disable OSPF	Disable	IP Routing must be enabled first before enable OSPF.
Router ID	Setting the Router ID in OSPF	Null	Router ID cannot be set to 0.0.0.0.
Distribution	Check corresponding box(es)for re-distribution of routes from another routing protocol (RIP),Static routes, and/or Connected routes into OSPF	Unchecked	N/A

2.21.4.2 OSPF Area Setting

An OSPF's area is a logical collection of OSPF networks, routers/switches, and links that have the same area identification number (**Area ID**). The OSPF network or domain can be divided into sub-domains called areas. Any switch or router within an area must keep a topological database for the area that it belongs. This area scheme is

to restrict the propagation of routes and reduce the amount of resources required by each router/switch to maintain its link state database. The propagation of routes is done via different types of Link State Advertisements (LSAs). Some area types will limit the types of LSAs that can be advertised within an area. Generally, each area is connected to a central backbone which is called area zero ore backbone area. An area is interface specific. A router/switch that has all of its interfaces within the same area is called an internal router (IR). Routers/switches that belong to multiple areas and connect these areas to the backbone area are called Area Border Routers (ABRs).A router that has interfaces in multiple areas is called an area border router (ABR). Routers that act as gateways (redistribution) between OSPF and other routing protocols (IGRP, EIGRP, IS-IS, RIP, BGP, Static) or other instances of the OSPF routing process are called autonomous system boundary router (ASBR). Any router can be an ABR or an ASBR.

On this webpage, the user can configure OSPF's area(s) as shown in Figure 2.280. The OSPF **Area ID** is defined in IP address format or four groups of number between 0 to 255 separated by dots. Typically, the backbone area is labelled as area 0.0.0.0. Next, the user can select the **Area Type** of OSPF which can be **Stub** area, **NSSA** (Not-So-Stubby-Area), or **Normal** area type. The **Normal** or standard area type is the area that has no restriction access to the rest of the network and switch(s)/router(s) in this area need to maintain a full link state database. Note that the backbone area is essentially a normal/standard area. For **Stub** area, there will be no external routes propagate into the area but a default route will be injected into the **Stub** area. This is to save the resource of the routers/switches within this area. For **NSSA** or Not-So-Stubby-Area, it is similar to the **Stub** area but still allow advertisement of external links from autonomous system boundary router (ASBR) to the area border router (ABR) connected to the NSSA. After finish configuring the OFPF Area, click on the **Add-Modify** button to save the **OSPF Area setting**. If the user wanted to remove an area, the user can click on the **Delete** button. A summary of all configured OSPF Area(s) is reported in the lower part of which is called**OSPF Area Table**.

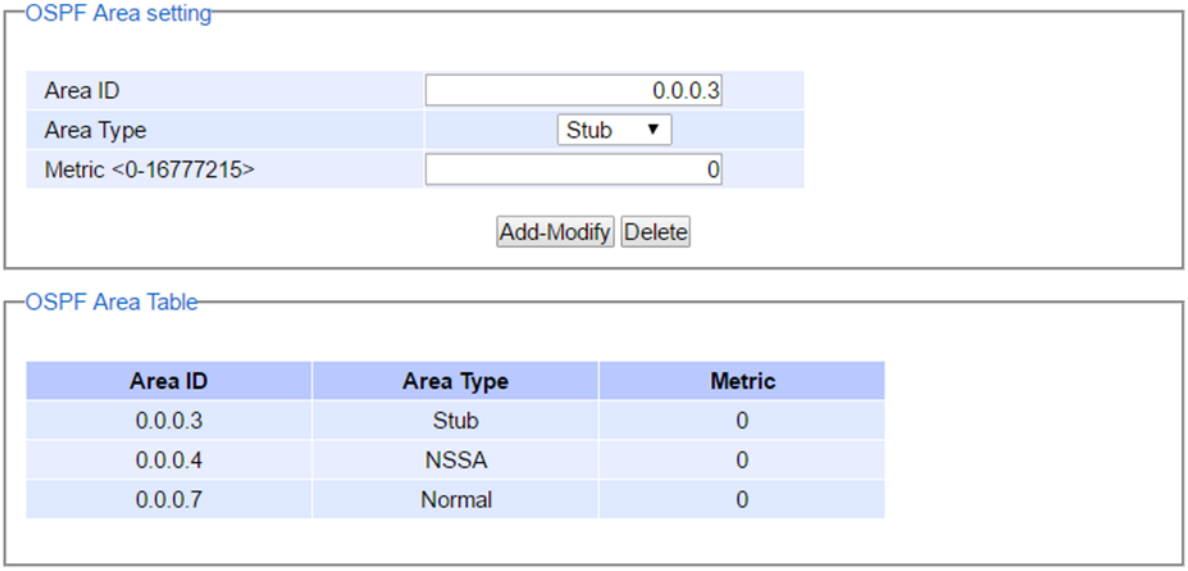


Figure 2.280 OSPF's Area Setting Webpage

Table 2.67 Descriptions of OSPF Area Setting Webpage

Label	Description	Factory Default	Note/restriction
Area ID	Setting of OSPF Area ID which is also in a form of IP address (4 groups of number between 0 and 255 separated by dots)	N/A	N/A
Area Type	Setting of OSPF Area Type which can be selected from Stub Area, NSSA (Not-So-Stubby-Area), and Normal option.	Stub	N/A
Metric	Routing metric which can set the value between0 and 16777215.	0	Metric can only be set to 0 under the "Normal" Area Type

2.21.4.3 OSPF Interface Setting

This webpage as shown in Figure 2.281 allows the user to configure OSPF interface on the RHG96XX industrial L3 managed switch. Note that you need to configure a VLAN ID as discussed in Section 2.14.1 first for the **Interface Name** that will be used for OSPF. There are basic parameters on this webpage which are related to assigning area, setting priority, configuring hello protocol (keepalive mechanism), setting OSPF's packet authentication, and assigning metric or cost of the interface. To properly configuring the OSPF on an interface, you must assign that interface to an **Area ID**. Then, you should set the priority using number between 0 to 255 for the RHG96XX in the **Router Priority** field. The router with the highest priority will be elected as Designated Router (DR) on a network segment that belongs to on and only one OSPF area. Note that the DR election is performed using the Hello protocol which is a form of keepalive used by OSPF routers (or RHG96XX) in order to acknowledge their existence on a segment. The **Hello Interval** specifies the length of time, in seconds, between the hello packets that the RHG96XX sends on an OSPF interface. The **Dead Interval** is the number of seconds that the RHG96XX's Hello packets have not been seen before its neighbors declare the OSPF router down. OSPF requires these intervals to be exactly the same between two neighbors. If any of these intervals are different, these routers/switches will not become neighbors on a particular network segment.

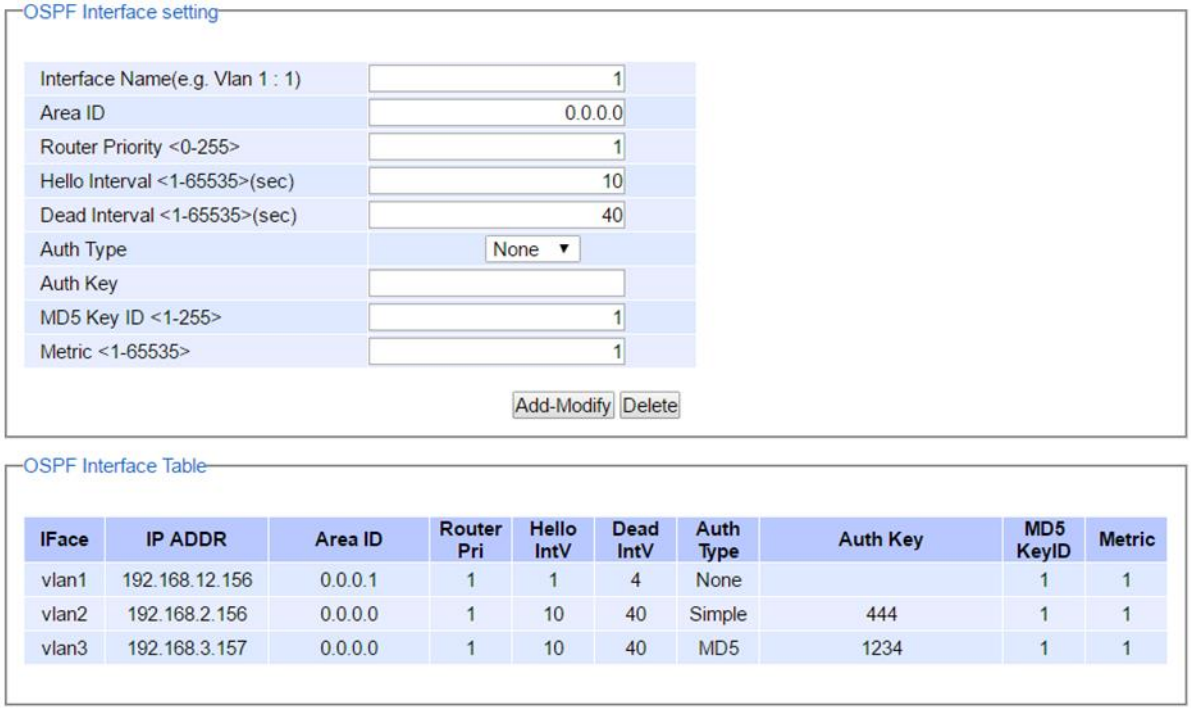


Figure 2.281 OSPF Interface Setting Webpage

RHG96XX can be configured to enable or disable OSPF Authentication by selecting an **Auth Type**. The **Auth Type** or authentication type for RHG96XX can be **None**, **Simple**, or **MD5**. By default, RHG96XX sets the authentication to None which means that routing exchanges over a network is not authenticated. If the **Simple** authentication type is selected, the **Auth Key** which is a simple password must be entered. Note that RHG96XX and other switches or routers in the same area that want to participate in the routing domain must be configured with the same **Auth Key**. Note that the **Auth Key** is transmitted over the network; therefore, it is vulnerable to eavesdropping attack. It is strongly recommended that the user chooses the **MD5Auth Type** because it is a cryptographic authentication which is more secure. This authentication type will use MD5 algorithm over OSPF packet, **Auth Key**, and **MD5 Key ID** to generate a message digest which will be appended to OSPF packet. The last parameter is the **Metric** or cost of the OSPF interface. The **Metric** is an indication of the overhead required to send packets across this interface which can be based on the bandwidth or the delay. It is inversely proportion to the bandwidth of that interface. That is the higher the bandwidth of the interface, the lower the metric value. After configuring each interface, please click **Add-Modify** button. If you want to remove an interfere, click on the **Delete** button. Table 2.68 summarizes the **OSPF Interface Setting** webpage.

Table 2.68 Descriptions of OSPF Interface Setting Webpage

Label	Description	Factory Default	Note/restriction
Interface Name	Set Interface Name	1	VLAN of interface must exist
Area ID	Set Area ID in a form of IP address (4 groups of number between 0 and 255 separated by dots)		N/A
Router Priority	Set Router Priority which can have a value between 0 to 255	1	If router priority is set to 0, it is a non-designated router (NDR). That is this interface will not be elected as Designated Router (DR) or Backup Designated Router (BDR).
Hello Interval	Set hello interval in second which can have a value between 1 to 65535.	10	N/A
Dead Interval	Set dead interval in second which can have a value between 1 to 65535.	40	N/A
Auth Type	Set Authentication Type for the interface which can be **None**, **Simple**, or **MD5.**Note that MD5 is more secure and recommended.	None	N/A
Auth Key	Set Authentication Key or password for OSPF interface according to the **Auth Type** selected in previous option. If **Auth Type** = **None**, **Auth Key** is empty or Null. If **Auth Type** = **Simple** or **MD5**, please enter a password in this field.	Null	The **Auth Key** or password can be a string of up to 8 characters.
MD5 Key ID	Set MD5 Key ID that can be a value between 1 to 255.	1	N/A
Metric	Set Metric or cost of the OSPF interface which can have a value between 1 and 65535.	1	N/A

2.21.4.4 OSPF Virtual Link Setting

There are two use cases for virtual link in OSPF. First, it can be used to link an area that does not have a physical connection to the backbone because all areas in an OSPF autonomous system must be connected to the backbone area or area 0. The virtual link can be used to connect an area to the backbone area (area 0) through a non-backbone area. Second, it can be used to patch the backbone of OSPF in case that there is a discontinuity of area 0. That is the virtual links can connect two parts of a partitioned backbone through a non-backbone area. Note that the non-backbone area that you configure the virtual link is called a transit area. The transit area cannot be a stub area and must have full routing information.

To configure a virtual link for OSPF in RHG96XX industrial L3 managed switch, there are two parameters needed to be entered on **Virtual Link Setting** webpage as shown in Figure 2.282. First parameter is the **Transit Area ID** which is in the form of IP address or four groups of number separated by dots. The transit area is the area that your RHG96XX is directly connected to. Second parameter is the **Neighbor Router ID** which is also in the form of IP address. The Neighbor router is a router that is also connected to the same transit area and connected to the backbone area (or area 0) or another partition of the backbone. After entering both parameters, please click on the **Add** button to add an entry of virtual link to RHG96XX's **OSPF Virtual Link Table** as shown at the bottom of Figure 2.282. To remove a virtual link, please fill in the corresponding **Transit Area ID** and **Neighbor Router ID** then click on the **Delete** button to remove that entry from the **OSPF Virtual Link Table**. Table 2.69summarizes the descriptions of **OSPF Virtual Link Setting** webpage.

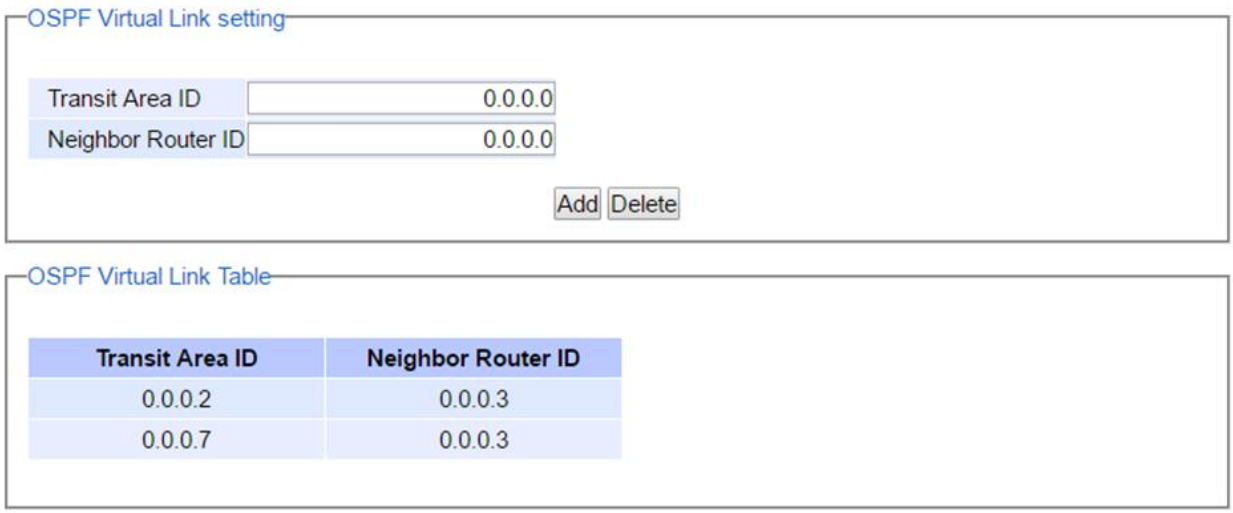


Figure 2.282 OSPF Virtual Link Setting Webpage

Table 2.69 Descriptions of OSPF Virtual Link Setting Webpage

Label	Description	Factory Default	Note/restriction
Transit Area ID	Setting of Transit Area ID which is in a form of IP address (4 groups of number between 0 and 255 separated by dots)	0.0.0.0	The backbone area cannot be set as a transit area.
Neighbor Router ID	Setting of Neighbor Router ID which is in a form of IP address (4 groups of number between 0 and 255 separated by dots)	0.0.0.0	N/A

2.21.4.5 OSPF Area Aggregation Setting

The OSPF Area Aggregation is a technique that combines groups of routes with common addresses into single routing table entry. RHG96XX supports the uses of subnet masks to achieve OSPF area aggregation. The user can specify the **Area ID** and the **Destination Network** then select the Subnet Mask from the available entry from the drop-down list. Figure 2.283 shows an example of OSPF Area Aggregation Setting webpage with an **OSPF Area Aggregation Table**. The user can add a new entry into the table by filling the required fields and clicking on the **Add** button. To remove an entry, please fill in the corresponding fields and click **Delete** button. Table 2.70 summarizes the descriptions of **OSPF Area Aggregation Setting** webpage.

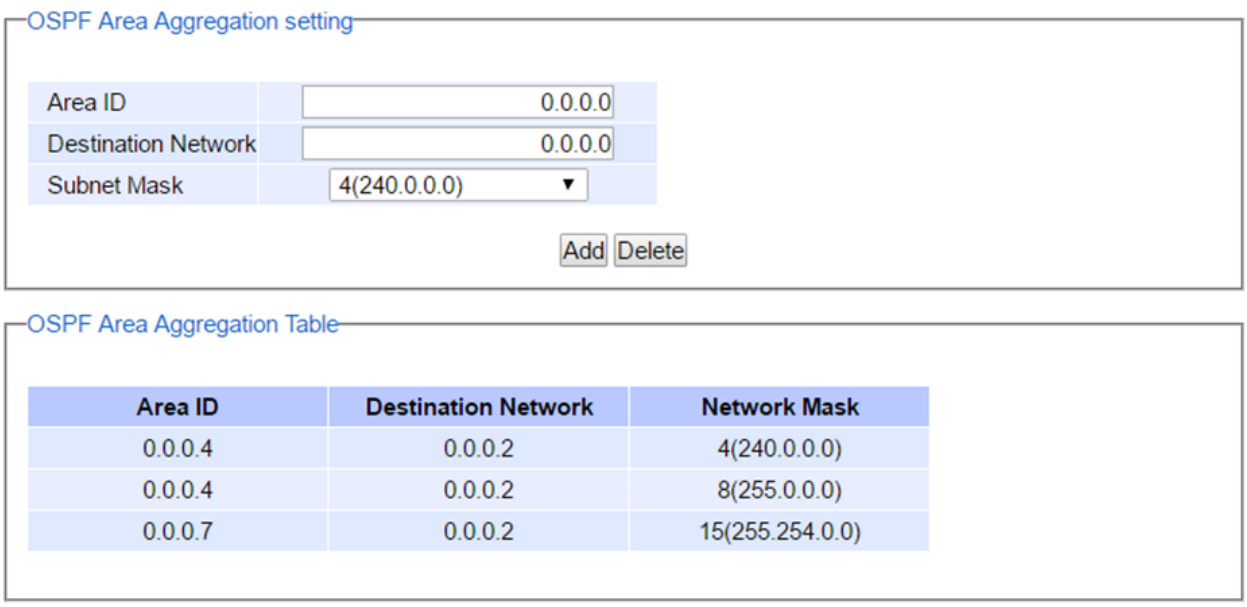


Figure 2.283 OSPF Area Aggregation Setting Webpage

Table 2.70 Descriptions of OSPF Area Aggregation Setting Webpage

Label	Description	Factory Default	Note/restriction
Area ID	Set Area ID in the form of IP address	0.0.0.0	N/A
Destination Network	Set Destination Network in the form of IP address	0.0.0.0	N/A
Subnet Mask	Set Subnet Mask by selecting an entry from a drop-down list.	4(240.0.0.0)	Prefix: 4 - 30

2.21.4.6 OSPF Routing Table

This webpage shows the current OSPF Routing Table and Neighbor Table as depicted in Figure 2.284.

OSPF Routing Table

Destination	Next Hop	Interface Name	VID
0.0.0.157	192.168.12.157	Vlan1	1

OSPF neighbor Table

Neighbor ID	Priority	State	Neighbor IP Address	Interface
0.0.0.157	1	Full/DR	192.168.12.157	Vlan1

Figure 2.284 OSPF Routing Table Webpage

2.22 Client IP Setting

The RHG9XXX industrial managed switch has two different approaches for setting up the IP addresses for the devices connected to its ports. The following are the submenus under the **Client IP Setting** section:

1. **DHCP Relay Agent**,
2. **DHCP Mapping IP**.

Figure 2.285 shows the dropdown menus under the **Client IP Setting** section.

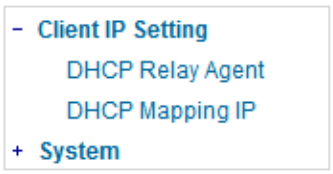


Figure 2.285 Client IP Setting Dropdown Menu

2.22.1 DHCP Relay Agent

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).

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 2.286shows the **DHCP Relay Agent** setting webpage. The users can enter up to four DHCP/BOOTP server IP addresses in the fields: **Server IP 1**, **Server IP 2**, **Server IP 3**, and **Server IP 4**. Then the users can enable the DHCP Relay by checking the **Enabled** box behind the DHCP Relay option.

The users can also have a choice to enable DHCP's **Option 82** which is the DHCP Relay Agent Information Option. When this Option 82 is enabled, the switch will insert information about the client's network location into the packet header of DHCP request 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 option 82 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 remove the option 82 information from the response packet and forward it to the client. The

Option 82 Type field in Figure 2.286 can be chosen from **IP**, **MAC**, **Client-ID**, or **Other** in the dropdown list. When **Other** type is selected, the **Option 82 Value** field will become active for entering the desired value by the users. After finishing the DHCP Relay Agent setup, please click on the **Update** button to allow the change to take effect.

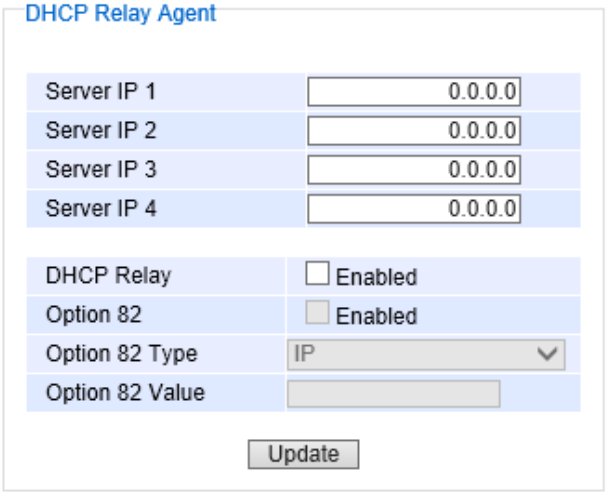


Figure 2.286 DHCP Relay Agent Webpage

2.22.2 DHCP Mapping IP

The user can reserve or map IP addresses to the device connected on the selected ports in this submenu. Figure 2.287shows the DHCP Mapping IP webpage where the desired IP address can be entered into the field for each Port. After finishing the DHCP IP mapping to the port(s), please click on the **Update** button to allow the change to take effect.

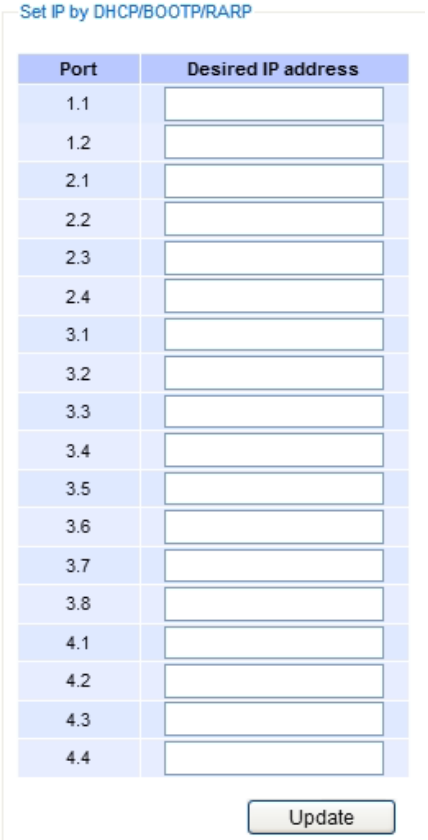


Figure 2.287 DHCP Mapping IP Webpage

2.23 SyncE

Ethernet network are asynchronous, whereas other network, such as SONET (Synchronous Optical Networks), are synchronous. SyncE (Synchronous Ethernet) allows synchronous and asynchronous networks using point-to-point connections. Its physical layer set how frequent connected access devices are synchronized. It is used to transfer clock signals over Ethernet interfaces.

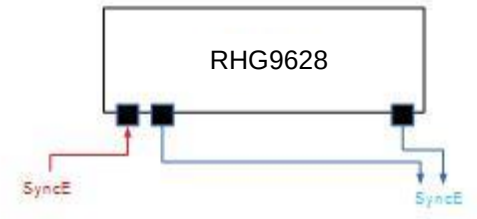


Figure 2.288How SyncE works in RHG9628

The followings are the description of how SyncE works:

1. When SyncE is enabled, the ethernet port will send SyncE signals out.
2. A Primary Port is used to receive SyncE signals of other devices. After receiving SyncE signals, change the SyncEfrequency of thedevice and send new SyncE signals out from the other ethernet ports.
3. If the Primary Port does not receive any SyncE signal from other device, it will start sending out the SyncE signal with its own frequency.
4. SyncE does not support 10G (In RHG9628,Port 4.1-4.4 no support SyncE). Because the frequency of 10G cannot be synchronized to 1G. (Note here that the frequency of 10G is 156Hz, and the frequency of 1G is a multiple of 25, such as 125Hz). Although synchronization between 10G connection may be possible, but experiments are still underwayed.

Figure 2.289shows SyncE Submenus in RHG96xx. User can set configuration through SyncE setting and check the status through SyncE Status.

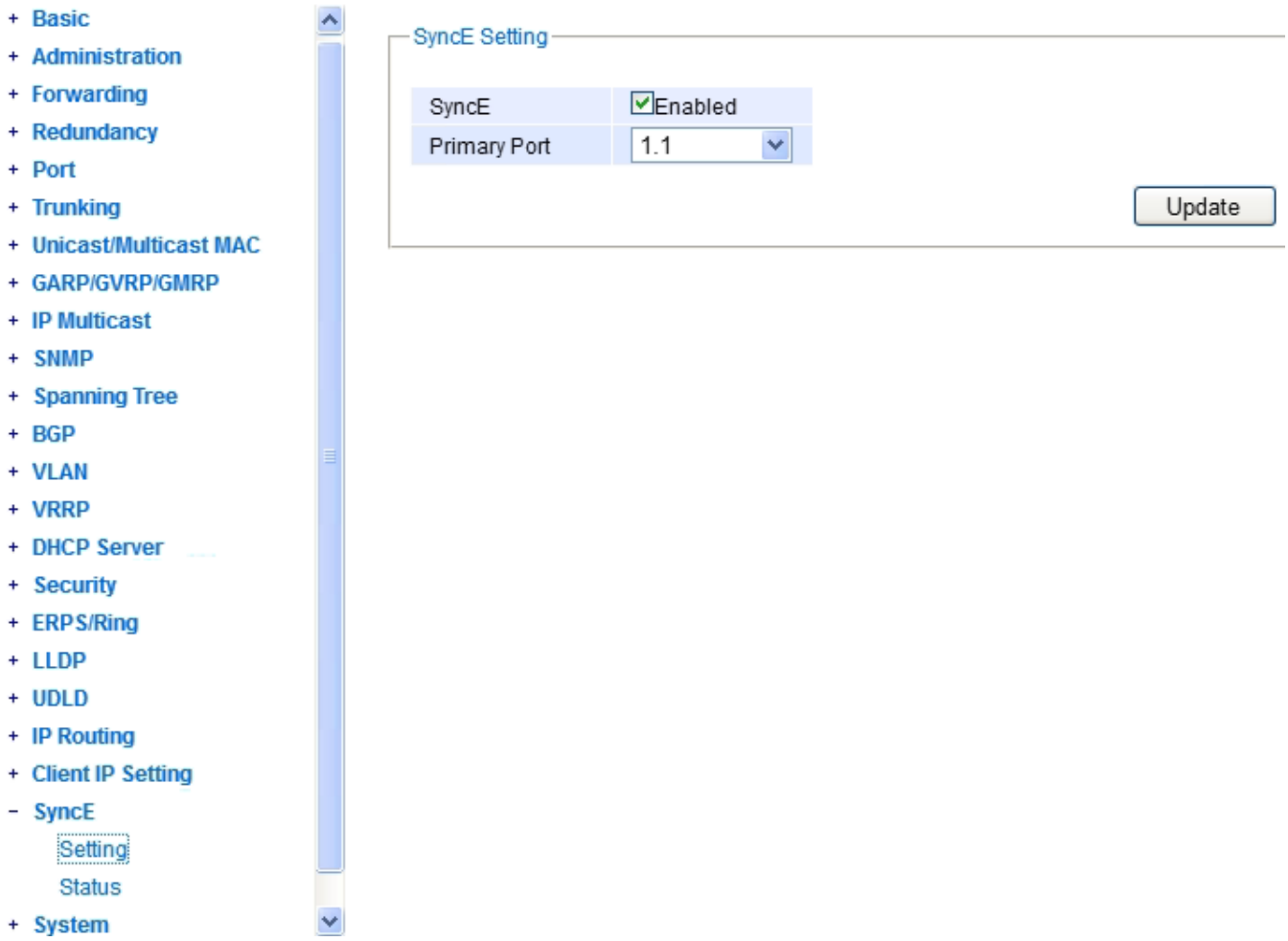


Figure 2.289SyncE Submenus in RHG96xx

2.23.1 SyncE Setting

Figure 2.290shows SyncE Submenus in RHG96xx. User can select each port and click enable SyncE function.

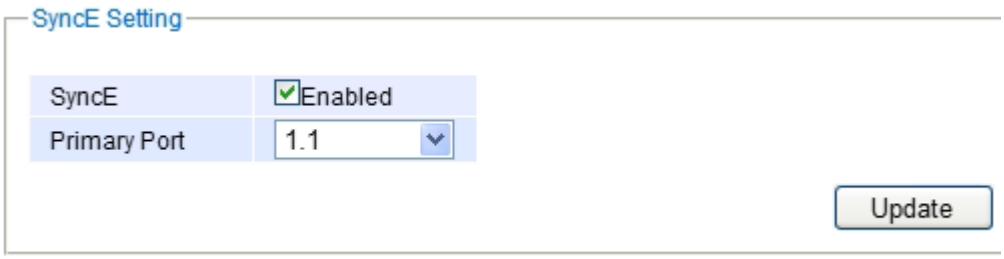


Figure 2.290SyncE Setting submenus in RHG96xx

2.23.2 SyncE Status

User can check SyncE status from SyncE Status submenu as shown in Figure 2.291and see the description of each setting as well as the default setting as shown in Table 2.71.

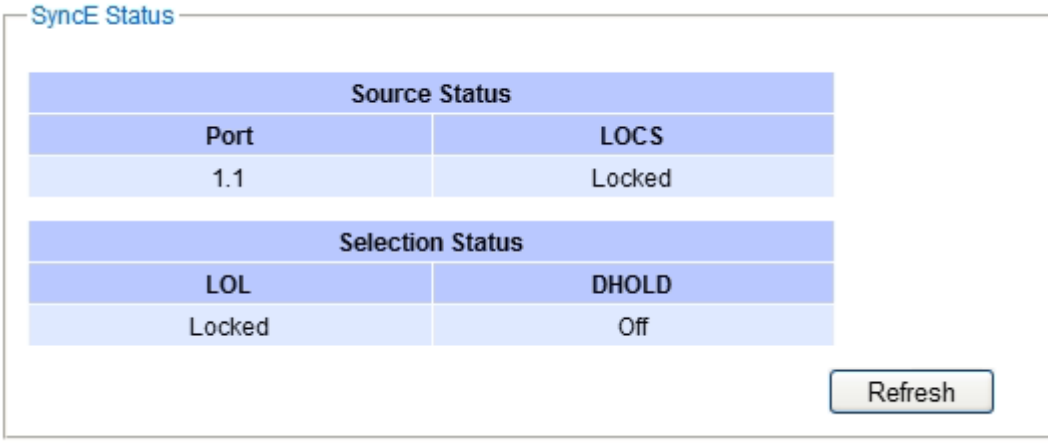


Figure 2.291SyncE Status submenus in RHG96xx

Table 2.71 Option and Default Setting of the SyncE Status

SyncE Status	Option	Default Setting
Source Status	Port	Depend
	LOCS (Signal is lost on this clock source)	Unlocked
Selection Status	LOL (Clock selector has raised the Loss of Lock alarm)	Locked
	DHOLD (Historical data of frequency is holdover if it is configured as“on”)	Off

2.24 System

This last section on the WebUI interface of the RHG9XXX managed switch provides miscellaneous tools for network administrator to check the internal status of the switch via system log, warning, and alarm notification. It also allows the administration to perform device maintenance operations such as backing up and restoring device’s configuration, updating the firmware, reversing the device to factory default setting, or reboot the system/device. Figure 2.292 shows all the dropdown menus under the **System** section.

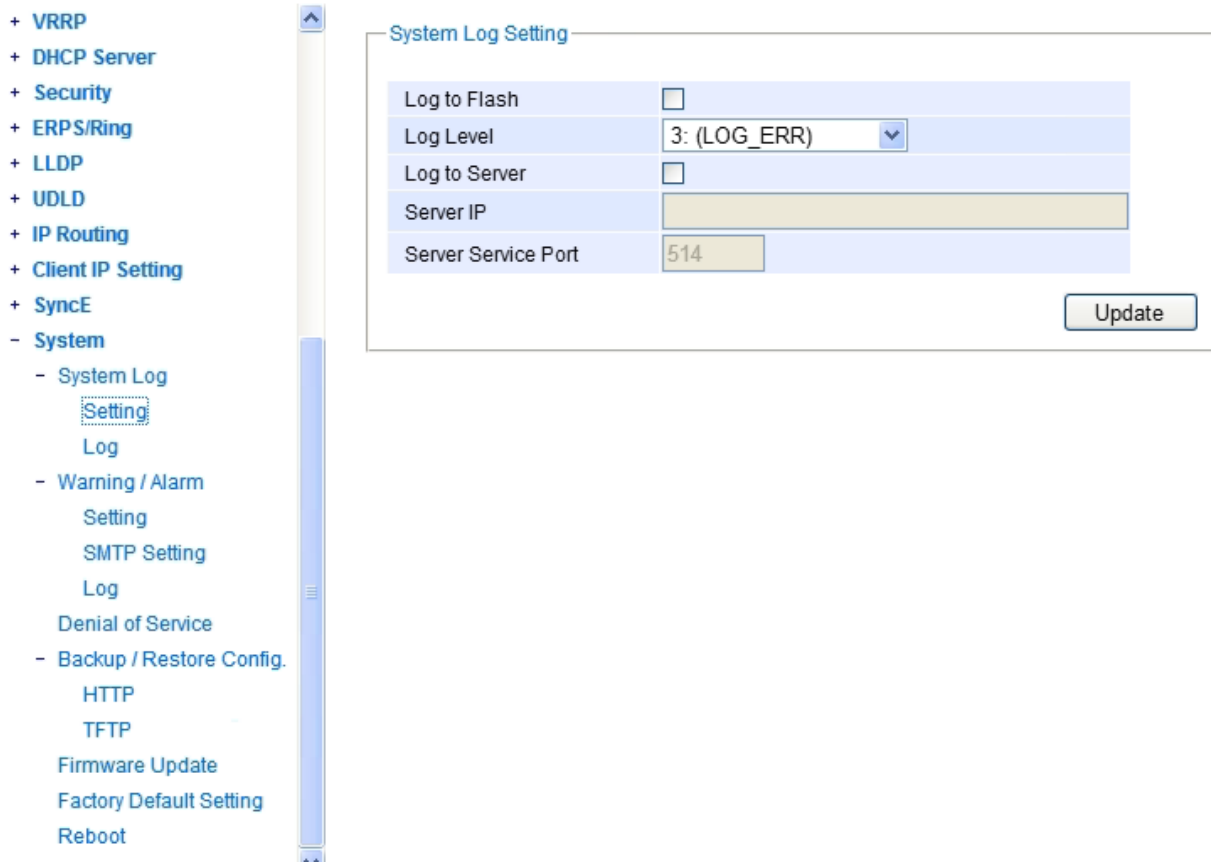


Figure 2.292 System Dropdown Menu

It is important for network administrators to know what's happening in their networks,and know where the events are happening. However, it is difficult to promptly locate network devices that are at the endpoints of systems. Thus, Ethernet switches connected to these devices play an important role of providing first-moment alarm messages to networkadministrators, so that network administrators can be informed instantaneously when accidents happen. Emailalertsand relays outputs under the System sectionis used to provide fast and reliable warning alerts for administrators.

2.24.1 System Log

The submenus under the System Log are:**Setting** and **Log**.

2.24.1.1 System Log Settings

Figure 2.293shows System Log related settings configuration. The actual recorded log event will be shown in Event Log on the next subsection. Here the users can enable how the log will be saved and/or delivered to other system. The log can be save to flash memory inside the managed switch and/or it can be sent to a remote log server. The users need to select the log level and provide the IP address of a remote log server and the service log service port. Please click on the Update button after finishing the setup. Table 2.72 describes the details of parameters setting for the system log.

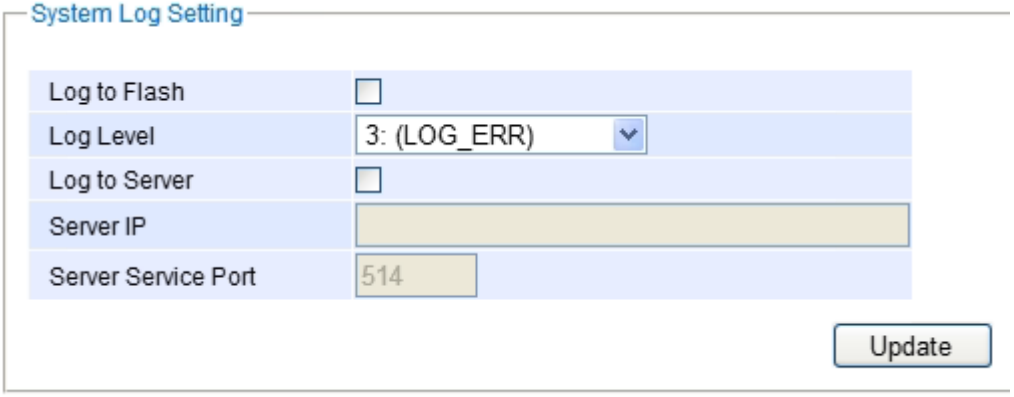


Figure 2.293System Log SettingWebpage

Table 2.72Descriptions of System Log Settings

Label	Description	Factory Default
EnableLog Event to Flash	**Checked**:Saving log event into flash memory. The flash memory can keep the log event files even if the switch is rebooted. **Unchecked**: Saving log event into RAM memory. The RAM memory cannot keep the log event files after each reboot.	Uncheck
Log Level	Set the log level to determine what events to be displayed on the next webpage(**Log**). The level selection is inclusive. For example, if 3:(Log_ERR)is selected, all 0, 1, 2 and 3 log levels will be implied. Range from Log 0 to Log 7.	3:(LOG_ERR)
Enable System Log Server	**Checked**:Enable Syslog Server. **Uncheck**: Disable Syslog Server. If enabled, all recorded log events will be sent to the remote System Log server.	Uncheck
System Log Server IP	Set the IP address of Syslog server	0.0.0.0
System Log Server Service Port	Set the service port number of System Log server. Range from Port 1 to Port 65535.	514

2.24.1.2 System Log-Log

Figure 2.294shows an example of all of the event's logs. Note that they are sorted by date and time. Table 2.73 provides explanation of each column and the button's functions on the System Log webpage.

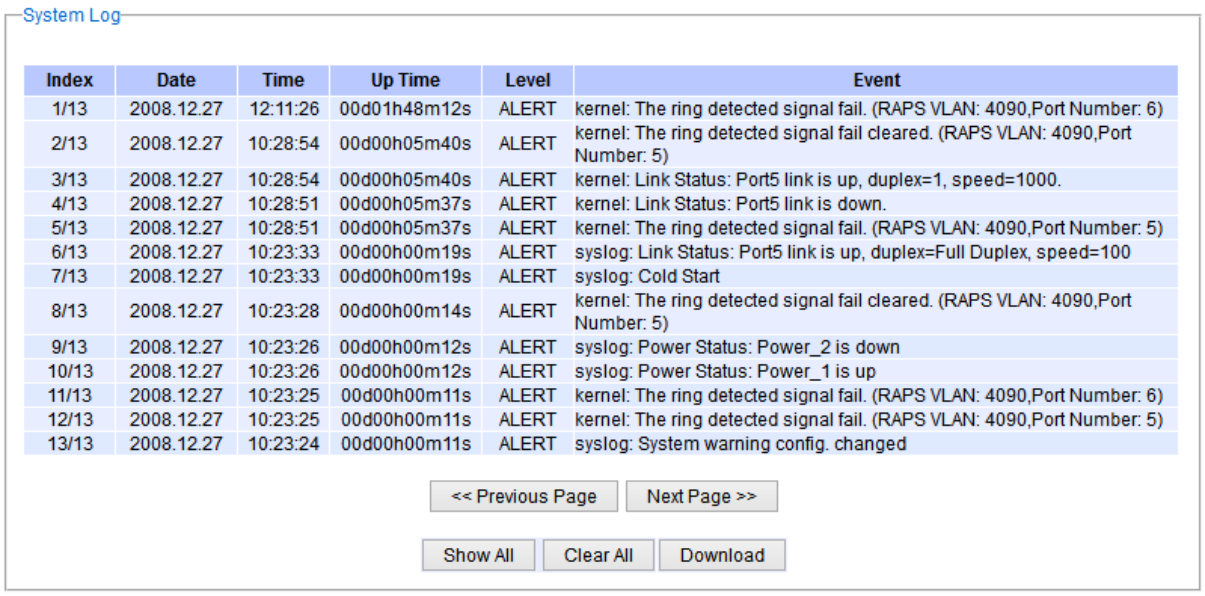


Figure 2.294Event Log Webpage

Table 2.73Descriptions of Event Log

Label	Description
Index	Indicate the index of a particular log event
Date	Indicate the system date of theoccurred event
Time	Indicate the time stamp that this event occurred
Up Time	Indicate how long the system(managed switch)has been up since this event occurred
Level	Indicate the level of this event
Event	Details description of this event
Previous Page	Display events on the previous page
Next Page	Display events on the next page
Show All	Click to display all events
Clear All	Click to clear all events
Download	Download or save the event log to the local computer

2.24.2 Warning/Alarm

The warning/alarm section consists of three subsections:**Setting**,**SMTP Setting**, and **Log**.

2.24.2.1 Warning/ Alarm Settings

There are three different types of Warning or Alarm: Link Status Alarms, Power Status Alarms, and System Log Alarms as shown in Figure 2.295. The Link Status Alarmsare related to the activities of particular port(s).Power Status Alarms keep track of power status of the switch based on the available input connectors.System Log Alarms are related to the overall functionalities of the switch. This webpage allows the users to configure how each type of the alarm events will be sent or notify the users. For link status and power status alarms, there are three possible notification methods via Relay, E-mail, and Alarm LED. For System Log alarms, there are only two possible notification methods via Relay and E-mail. After finish configuring the alarms, please click the **Update** button. Note that there is an **Assert Relay** button which can be used to test an external Relay connected to the managed switch.

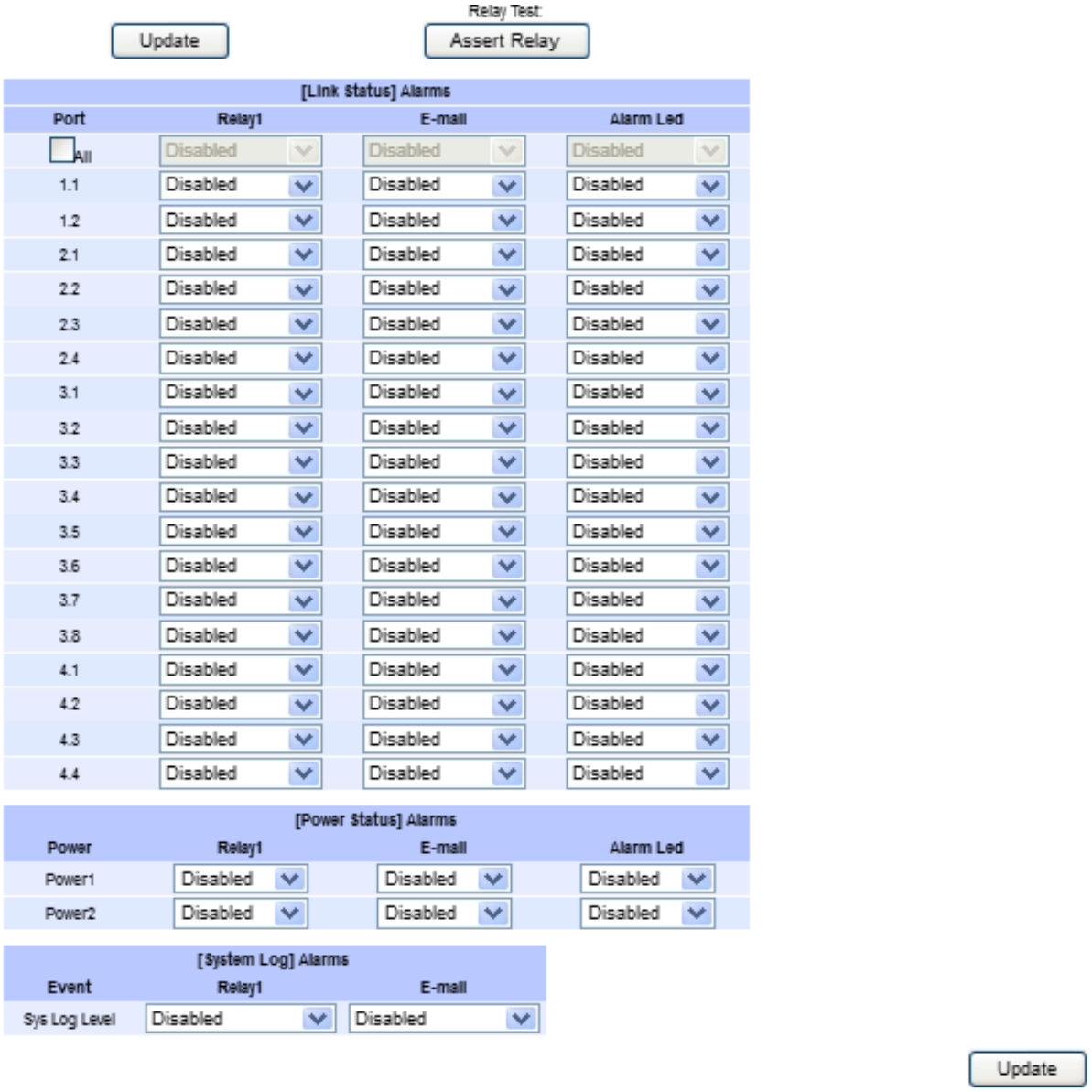


Figure 2.295 Webpage ofWarning Event Selection

In Link Status Alarms, users have three conditions whether to send notifications via **Relay**, **E-mail**, or **Alarm LED** in case if Link is UP, Link is Down, or Link is UP/DOWN. Table 2.74 summarizes the link status alarm event selection. Note the users can enable the alarm events for all ports simultaneously by checking the box in front of the **All** entries.

Table 2.74 Descriptions of Link Status Alarm Event Selection

Label	Description	Factory Default
Port	Indicates eachport number.	-
Port state event	**Disabled:**Disables alarm function, i.e.no alarm message will be sent. **Link Up:**Alarm message will be sent when this port/link is up and connection begins.	Disabled

Label	Description	Factory Default
	Link Down: Alarm message will be sent when this port/link is down and disconnected. **Link Up/Down:**Alarm message will be sent whenever there's a change, i.e. connection begins or connection disrupted.	

In power status alarms, the users have twoconditions to send notification (via **Relay**, **E-mail** and **Alarm LED**)which are**Power On**, or **Power Off**.Table 2.75 summarizes the Power Status Alarm event selection.

Table 2.75 Descriptions of Power Status Alarm Event Selection

Label	Description	Factory Default
Power	Indicate specific power supply	Disabled
Power status event	Disable: Disables alarm function. Power On: Sends an alarm when power is turned on. Power Off: Sends an alarm when power is turned off.	Disabled

In System Log Alarms, the users have can only send notification via **Relay** and **E-mail**. Table 2.76 describes the System Log Level which can be selected for the System Log Alarm event notification.

Table 2.76 Descriptions of System Log Alarm Event Selection

Label	Description	Factory Default
System log event	Disable**:** Disable power status detection. 0: (**LOG_EMERG**): Enable log level 0~7 detection. 1: (**LOG_ALERT**): Enable log level 1~7 detection. 2: (**LOG_CRIT**): Enable log level 2~7 detection. 3: (**LOG_ERR**): Enable log level 3~7 detection. 4: (**LOG_WARNING**): Enable log level 4~7 detection. 5: (**LOG_NOTICE**):Enable log level 5~7 detection. 6: (**LOG_INFO**): Enable log level 6~7 detection. 7: (**LOG_DEBUG**): Enable log level 7 detection. See note below for specific log level description.	Disabled

***NOTE:-Log levels** are inclusive. In other words, when log level is set to 0, an alarm is triggered whenever 0, 1, 2…6, and/or 7 happens.When log level is set to 5, an alarm is triggered whenever 5, 6, and/or 7 happens.

0:Emergency:system is unstable
1:Alert:action must be taken immediately
2:Critical:critical conditions
3:Error:error conditions
4:Warning:warning condition
5:Notice:normal but significant condition
6:Informational: informational messages
7:Debug:debug-level messages

2.24.2.2 SMTP Settings

Simple **M**ail **T**ransfer **P**rotocol (**SMTP**)is an internet standard for email transmission across IP networks. In case any warning events occur as configured in Section 錯誤! 未知的選項引數。, the system can send an alarm message to users by e-mail. Here, the users will be allowed to modify E-mail-related settings for sending the system alarms(Link Status, Power Status, and System Log), as shown inFigure 2.296.

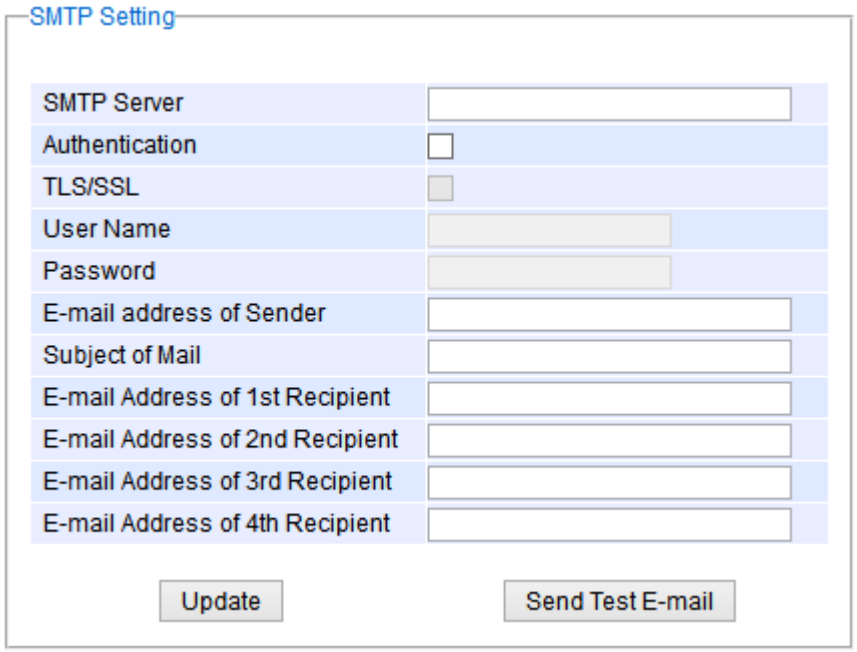


Figure 2.296 SMTP Setting Webpage

An example of SMTP Setting is shown in Figure 2.297. After entering all the necessary fields, please click on the Update button to allow the setting to take effect. Note that the users can try to send a Test E-mail according the SMTP setting on this webpage by clicking on the **Send Test E-mail** button. The description of each SMTP Setting parameter is summarized in 錯誤! 未知的選項引數。.

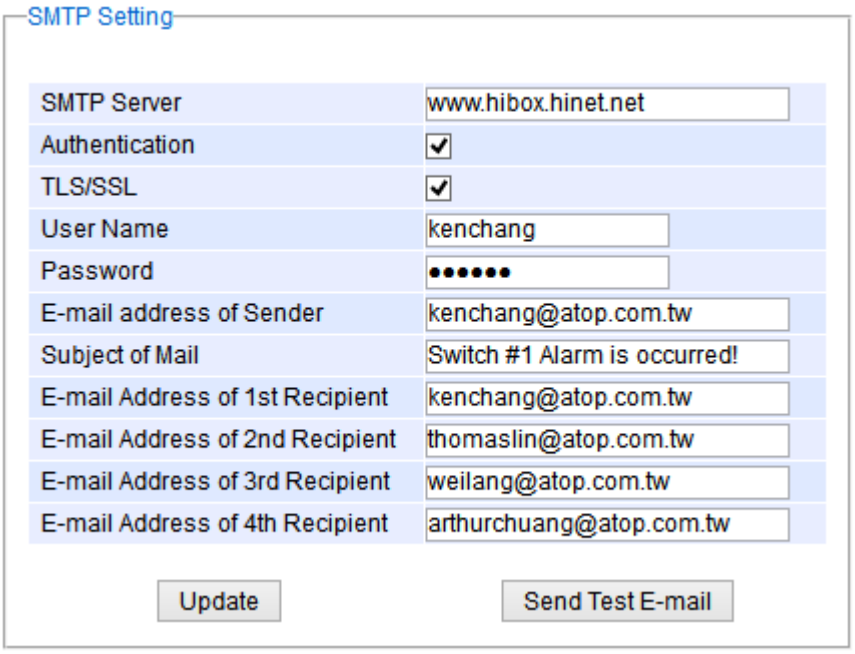


Figure 2.297 Example of SMTP Setting

Table 2.77Descriptions of SMTP Setting

Label	Description	Factory Default
SMTP Server	Configure the IP address of an out-going e-mail server	NULL
Authentication	Enable or disable authentication login by checking on the box. If enabled, SMTP server will require authentication to login.Thus, the users will also need to setup User Name and Passwordto connect to the SMTP server	Disable (Unchecked)
TLS/SSL	Enable or disable Transport Layer Security (TLS)or Secure Sockets Layer (SSL)which is an encryption mechanism for communication with the SMTP Server	Disable (Unchecked)
Username	Set the user name (or account name) to login.Max. 31 char.	NULL
Password	Set the account password for login. Max. 15 characters.	NULL
E-mail Address of Sender	Configure the sender e-mail address	NULL
Mail Subject	Type the subject of this warning message. Max. 31 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
Update	Update these modificationson the managed switch	-
Send Test E-mail	Send a test email to recipient(s)above to check accuracy.	-

2.24.2.3 Log

Managed switchwarns its users in case any event occurs. Atable calledWarning/Alarm Log in this section displays the warning eventsas shown in Figure 2.298 Warning/Alarm Log Webpage. At the top of the table, the users can

click on the **Reset Relay** button to turn off the Relay or click on the **Clear Log** to remove all entries in the **Warning/Alarm Log** table. To obtain the latest event on the able, the users have to click on the **Refresh** button.

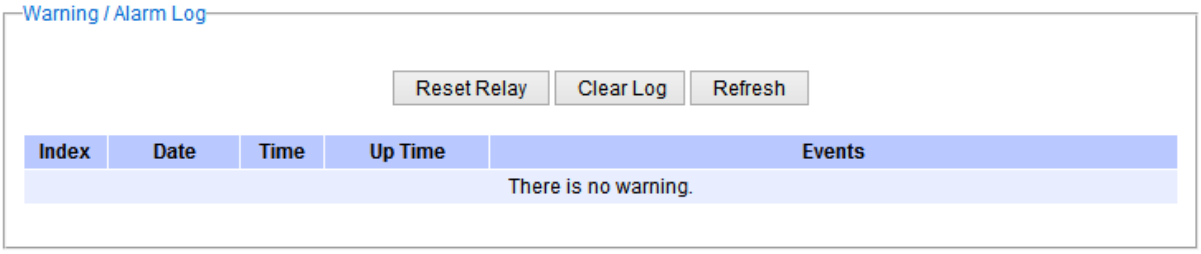


Figure 2.298 Warning/Alarm Log Webpage

An example of **Warning/Alarm Log** table is shown in Figure 2.299. Note that the display format and buttons is slightly different from the current EGH7XXX format above. A short list of alarm messages is shown on the top portion of the web browser interface.

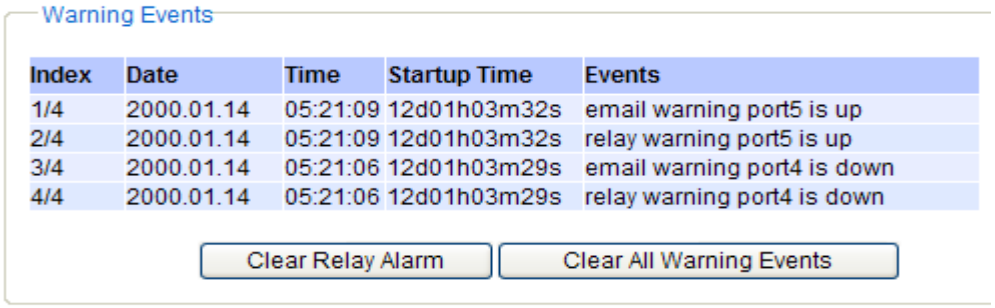


Figure 2.299Example of Warning Events

Table 2.78Descriptions of Warning/AlarmLog

Label	Description	Factory Default
Reset Relay	Sets Hardware Relay Alarm to off.	Relay is off
Clear Log	Clears all warning events that are displayed.	-
Refresh	Obtain the latest Warning /Alarm events	-
Index	Display the index of the Warning/Alarm events as an entry number over a total number of events	-
Date	The date that the alarm/event occurred.	-
Time	The time that the alarm/event occurred.	-
Startup Time	The duration of time since the start up time of the switch until the alarm/event occurred.	-
Events	Description of the alarm events	-

2.24.3 Denial of Service

Denial of Service (DoS)is a malicious attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. RHG9XXX industrial managed switch is designed so that uses can filter out various types of attack as shown in Denial of Service setting webpage(Figure 2.300). The followings are some vulnerable attacks that can be prevented by theRHG7XXX switch function.

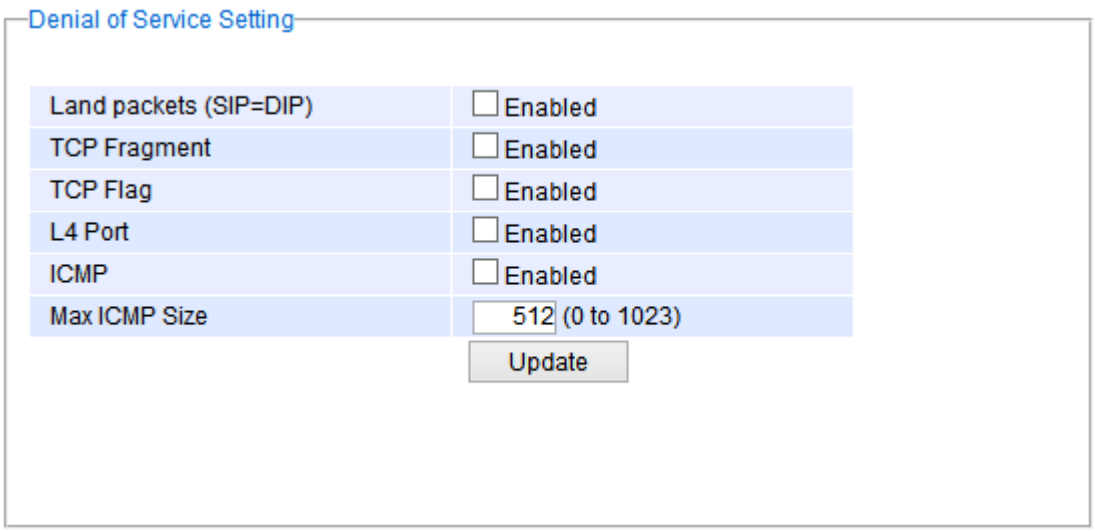


Figure 2.300 Denial of Service Setting Webpage

First is the Local Area Network (LAND)DoS attack. LAND is a layer 4 DoS attack in which the attacker sets the source and destination information of a TCP segment to be the same. Specifically, TCP SYN packet is created such that the source IP and port are set to be the same as the destination address and port, which in turn is set to point to an open port on a Victim's machine. A vulnerable machine would receive such a message and reply to the destination address effectively sending the packet for reprocessing in an infinite loop. A vulnerable machine will crash and freeze due to the packet being repeatedly processed by the TCP stack. To enable/disable the protection against the Local Area Network (LAND)DoS attack, click**Enabled** box on LAND packet (SID=DID)function.

Second vulnerability attack is TCP fragmentation attacks also known as tear drop attack, which is targeting TCP/IP reassembly mechanism, preventing them from putting together fragmented data packets. As a result, the data packets overlap and quickly overwhelm the victim's servers, causing them to fail. To enable/disable the protection against the TCP fragment DoS attack, click **Enabled** box on TCP Fragment function. However, to set the mitigation method, some certain inputs are needed to set rules of filtering. For example, whether the first fragment is allowed or not and the minimum TCP header size that is allowed. In some datalink protocols such as Ethernet, only the first fragment contains the full upper layer header, meaning that other fragments look like beheaded datagrams. No additional overhead imposed over network because all fragments contains their own IP header. Only the first fragment contains the ICMP header and all remaining fragments are generated without the ICMP header.

The third vulnerability is called TCP flag DoS attack. The attack sends out TCP packets with flag indicating that they are ACK packets. This attack is similar to SYN flood except SYN flood also open a connection with the server. Although the devices are mostly tuned for more common attack as SYN flood. TCP flag DOS attack will force the server to keep dropping the packets, causing resource exhaustion. To enable/disable the protection against the TCP Flag DoS attack or called ACK flood, click **Enabled** box on TCP Flag function.

The fourth vulnerability is called L4 port DoS attack. There are various types of L4 port DoS attack. In UDP attack, a large number of UDP packets are sent to victim until it is overloaded. UDP-Lag attacks in bursts as to not hit the target offline completely. SUDP attack is the same as UDP but spoofs the request to make it harder to mitigate. SYN/SSYN/ESSYM attacks are abuse the hand shake of the TCP protocol until the victim is overloaded. DNS/NTP/CHARGEN/SNMP attacks are an amplified UDP attack that abuses vulnerable server by sending a spoofed request with the targets IP as the sender. The servers then send the target the information overloading the system.To enable/disable the protection against all these L4 Port DoS attacks, click **Enabled** box on L4 Port function.

Last vulnerability is so called ICMP fragmentation attack. The attack involves the transmission of fraudulent ICMP packets that are larger than the network's MTU. In this switch, administrators can filter these packets out by enabling ICMP function and set **Maximum ICMP size** range from 512 to 1023 bytes. As these ICMP packets are fake, and are unable to be reassembled, the target server's resources are quickly consumed, resulting in server

unavailability. To enable/disable the protection against the ICMP DoS attack, click **Enabled** box on ICMP function. Table 2.79 provides descriptions of the Denial of Service Setting.

Table 2.79 Descriptions of Denial of Service Setting

Label	Description	Factory Default
LAND packets	**Enabled:**Enabled prevention over the attack using TCP SYN packet that has the same source and destination's IP and port.	Disabled
TCP Fragment	**Enabled:**Enabled prevention over the TCP fragmentation attackwhich is targeting TCP/IP reassembly mechanism	Disabled
TCP Flag	**Enabled:**Enabled prevention over the TCP flag DOS attack which force the server to keep dropping the packets, causing resource exhaustion.	Disabled
L4 Port	**Enabled:** Enabled prevention over various types of L4 port DoS attacks that are intended to overload the server.	Disabled
ICMP	**Enabled:** Allow filtering ICMP that has packet size higher than the maximum ICMP size defined in the next field	Disabled
Max ICMP Size	512 to 1023 bytes	512

2.24.4 Backup/Restore Config.

In **Backup/Restore Config**function, the current configuration of the RHG9XXX industrial managed switch can be downloaded to alocal computer and saved it as a backup. Additionally, the users can restore a previously backup configuration from a local computer to the RHG9XXX industrial managed switch. It will replacethe current configuration. These backups and restore function can be done through two different protocols: **HTTP** or **TFTP**. Figure 2.301 depicts the **Backup/Restore Configuration** dropdown menu.

Figure 2.301Backup/Restore Config.Dropdown Menu

2.24.4.1 Backup/Restore Config. Via HTTP

Figure 2.302 shows the webpage for Backup/Restore the configuration via HTTP. It is divided into two parts: **Backup the Configuration** and **Restore the Configuration**. When clicking on the **Download** button on the upper part of the page(**Backup the Configuration**), the users will be prompt to **Opening** the file name IP-10.0.50.1.bin by an application or to **Save File** to a destination. Choosing to Save File will back up the switch's current configuration to your local drive on the local computer.

To restore a configuration file to the switch, please move down to the **Restore the Configuration** part, then click the **Browse…**button to choose a configuration file from the local drive. Before clicking the **Upload** button, the users can check any of the options below the upload file which are to **Keep the current username & password setting** and to **Key the current network setting**. This will help prevent the users from the necessity to logging-inusing a previously storedusername, password or network configuration after settings are restored.

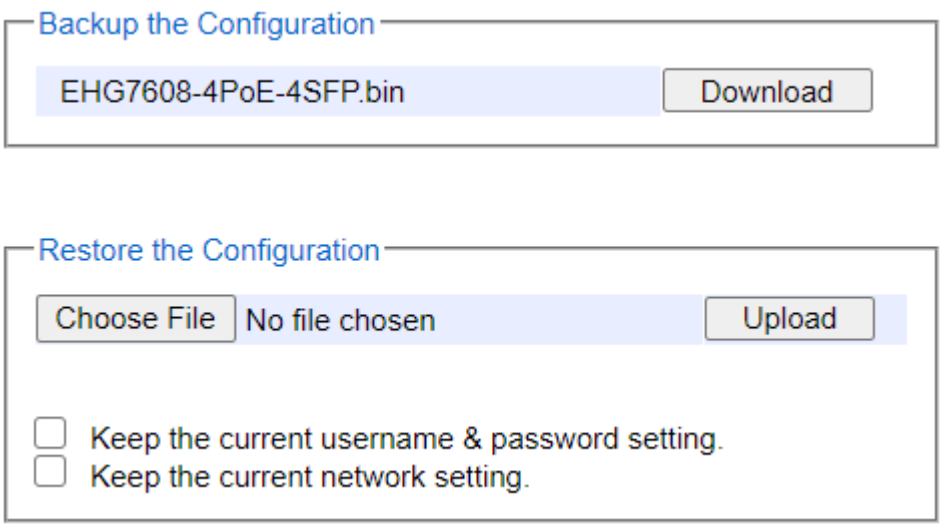


Figure 2.302 Backup/Restore Configuration via HTTP

2.24.4.2 Backup/Restore Config. Via TFTP

Trivial File Transfer Protocol (TFTP) is designed to be small and easy to implement. The users are allowed to upload configuration settings to a TFTP server as a backup copy,and download these settings from a TFTP server when necessary to restore or replace the configuration of the RHG9XXX industrial managed switch. Figure 2.303 shows the TFTP webpage which is divided into three parts: **Download the Configuration from TFTP**, **Upload the Configuration to TFTP**, and **DHCP Option 66/67 Setting**. Table 2.80 summarizes the descriptions of TFTP Setting.

- To download a configuration file from a TFTP server, the user need to specify the IP address of the TFTP server and the Remote File Name. Then, click the **Download** button.
- To upload a configuration file from a TFTP server, the users need to specify the IP address of the TFTP server and the Desired File Name. Then, click the **Upload** button.
- The last part of the TFTP page is the DHCP Option 66/67 Setting. This feature enables the managed switch to learn of the TFTP Server Name and Boot filename, which is a data in DHCP IPv4 packet Option 66 (RFC2132), and Filename, which is a data in DHCP IPv4 packet Option 67 (RFC2132). Checking the **Enabled** box and then click on the **Update** button to set this feature.

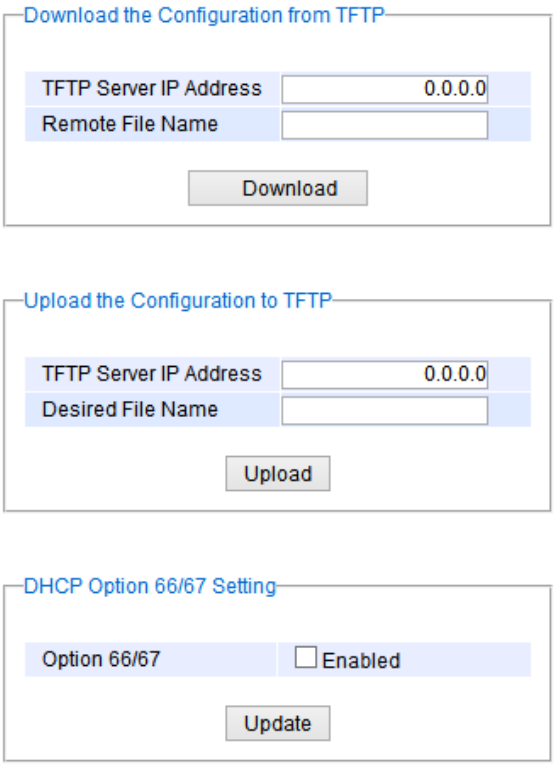


Figure 2.303 Backup/Restore Configuration via TFTP

Table 2.80Descriptions of TFTP Settings

Label	Description	Factory Default
TFTP Server IP Address	Sets the IP address ofthe remote TFTP server domain name.	NULL
Remote File Name	Type in name of the file to be downloaded.	NULL
Download	Click to start download remote configuration into the Switch.	-
Desired File Name	Type in name of the file to be uploaded.	NULL
Upload	Click to start upload Switch configuration to the remote TFTP server.	-
Option 66/67	Enable this option to allow the managed switch to learn of TFTP Server Name and the filename to be used from a DHCP packet	Disable
Update	Update the setting of DHCP Option 66/67 setting	-

2.24.5 Firmware Update

The users can update thedevice firmwarevia web interface as shown in Figure 2.304. To update the firmware, the users can download a new firmware from Atop's website and save it in a local computer. Then, the users can click **Browse…**buttonand choose the firmware file that is already downloaded. The switch's firmware typically has a ".dld"extension such as RHG9628-K470A470.dld. After that, the users can click **Update**buttonand wait for the

update process to be done. Alternatively, the firmware update can also be performed using the Device Management Utility discussed in Chapter 5.

Note:please make sure that the switch is plug-in all the time during the firmware upgrade.

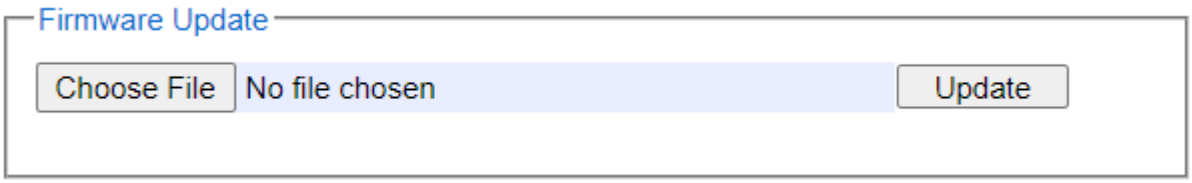


Figure 2.304Firmware Update Webpage

2.24.6 Factory Default Setting

When the managedswitch is not working properly, the users can reset itback to the originalfactory default settings by clicking on the**Reset**button as shown in Figure 2.305.

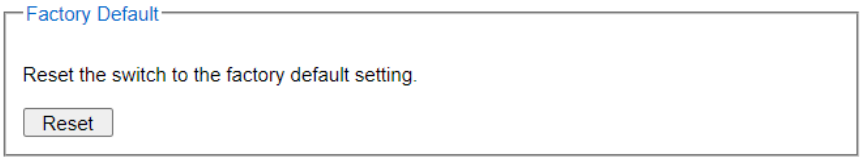


Figure 2.305Factory Default Setting Webpage

2.24.7 Reboot

An easy reboot function is provided in this webpage requiring only one single clickon the **Reboot** button as shown inFigure 2.306.

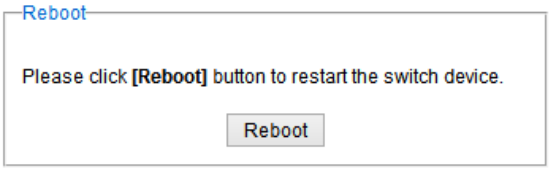


Figure 2.306Reboot Webpage

2.24.8 Logout

An logout function is provided in this webpage requiring only one single click on the **Logout** button as shown in Figure 2.306.

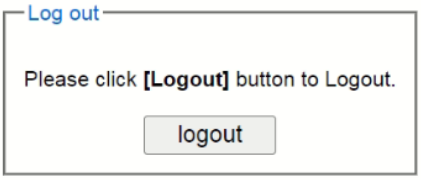


Figure 2.307 Logout Webpage

3 Configuring with a Serial Console

A managedswitch can also be configured by using a serial console. Note that a special serial console cable is required to connect to the console port on top of the RHG9XXX's chassis. Please contact Atop Technologies to obtain the cable, is needed. This method is similar to the web browser one. The options are the same, so users can take the same procedures as those examples in Chapter 2.

3.1 Serial Console Setup

After users install **Tera Term**, perform the following steps to access the serial console utility.

1. Start **Tera Term**. In **New Connection** window, select **serial** and appropriate port.

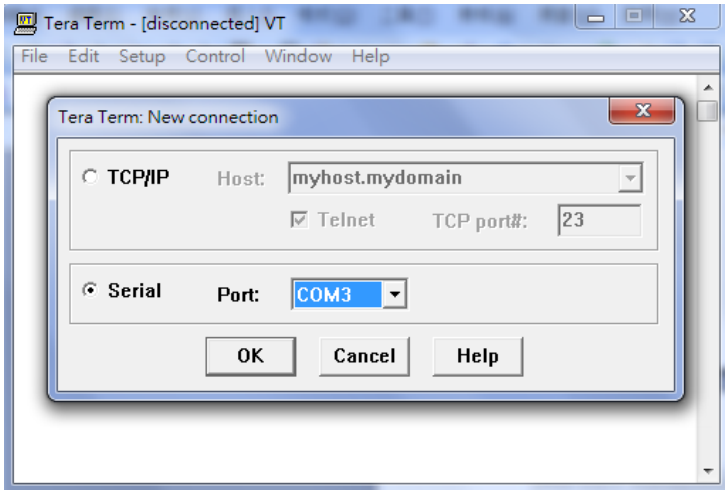


Figure 3.1Setting of New Connection in Tera Term Program

2. Click **Setup**-> Choose**Serial Port**.

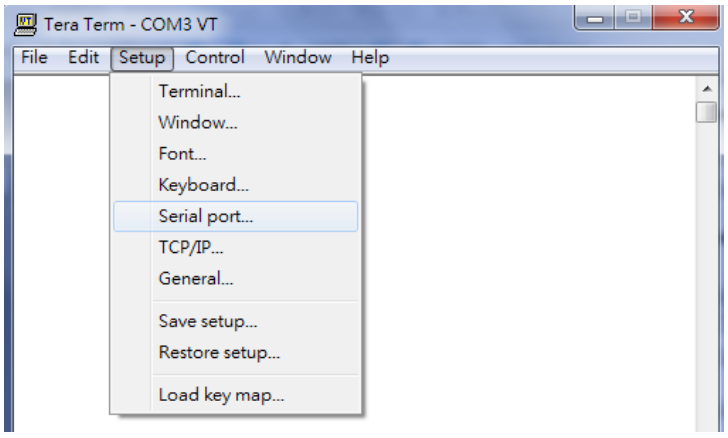


Figure 3.2Setup Menu

3. The **Serial Port Setup** window pops up. Select an appropriate port for **Port**, **115200** for **Baud Rate**, **8 bits** for **Data**, **none** for **Parity**, and **1 bit** for **Stop**, as shown in Fig.3.3.

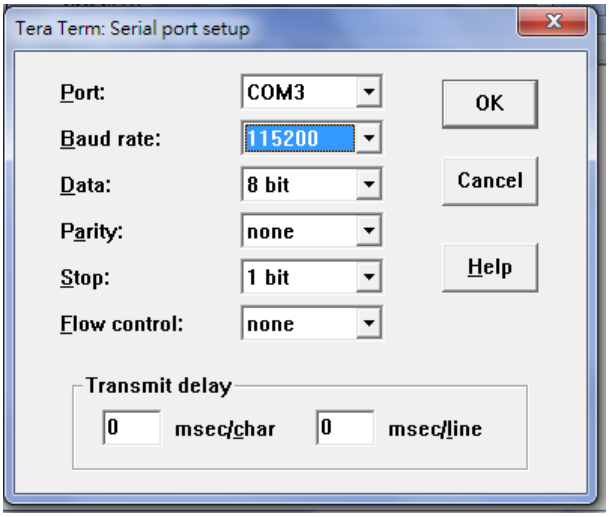


Figure 3.3Setting for the Serial Port

4. After finishing settings and clicking **OK**, a **Command Line Interface**(**CLI**)will be brought up.

3.2 Command Line Interface Introduction

The Command Line Interface supports two types of privileges, which are operator and manager privileges. Users with operator privileges may only view the information, while those with manager privileges are allowed to view information and configure settings. Operator and manager privileges are initially entered without the need for passwords, but a user may be assigned witha password for both the operator and manager privileges. If passwords are assigned, then when the user attempts to enter CLI on the next time, they will need to enter the correct username and password.

If a user is in the user mode and wants to switch to the privileged mode, he/she may simply type in the command "**enable**" and then enter the correct username and password after the prompt:
Username: ***(enter username here)***
Password: ***(enter password here)***
Switch#

If a useris in the user mode and wants to switch to the privileged mode, he/she may simply type in the command "**enable**"and then enter the correct username and password after the prompt:

*Switch>**enable***
*Username:**(enter username here)***
*Password:**(enter password here)***
Switch#

To enter the "configuration" mode, you need to be in the privileged mode, and then type in the command "**configure**":

*Switch# **configure***
Switch(config)#

Anillustration of the modes, related privileges and screen prompt is shown in Figure 3.4.

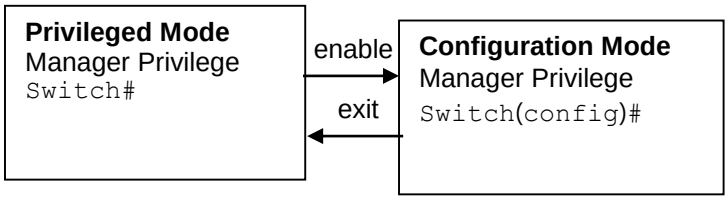


Figure 3.4Modes, privileges, and prompts

Users may enter "**?**" at any command mode and the CLI will return possible commands at that point, along with some description of the keywords:

*Switch(config)# **ip ?***
ip Configure network setting
ipv6 Configure network setting
ip-routing IP Routing configuration

Users may use the <Tab> key to do keyword auto completion:
*Switch(config)# **sysl<Tab>***
*Switch(config)# **syslog***

3.3 General Commands

The table below shows some useful commands that may be used anytime when using serial console.

Table 3.1Command Description

Commands	Descriptions
Configure	Enter configuration mode
?	List all available option.
Exit	Go back to the previous menu.
Logout	Log out of CLI
No history	Disable command history
Show history	List last history commands

3.4 Command Example

The serial console is another method to add/delete/change configuration, same as the web browser method. These two methods have similar functionalities. The picture below shows all the options on CLI.Two examples of making configurations: **Administration** and **Spanning Tree** using serial console method,which are shown in the following sub-sections, are the same as what are explained in Chapter2. The only difference is thatthe web browser method is usedin Chapter 2.

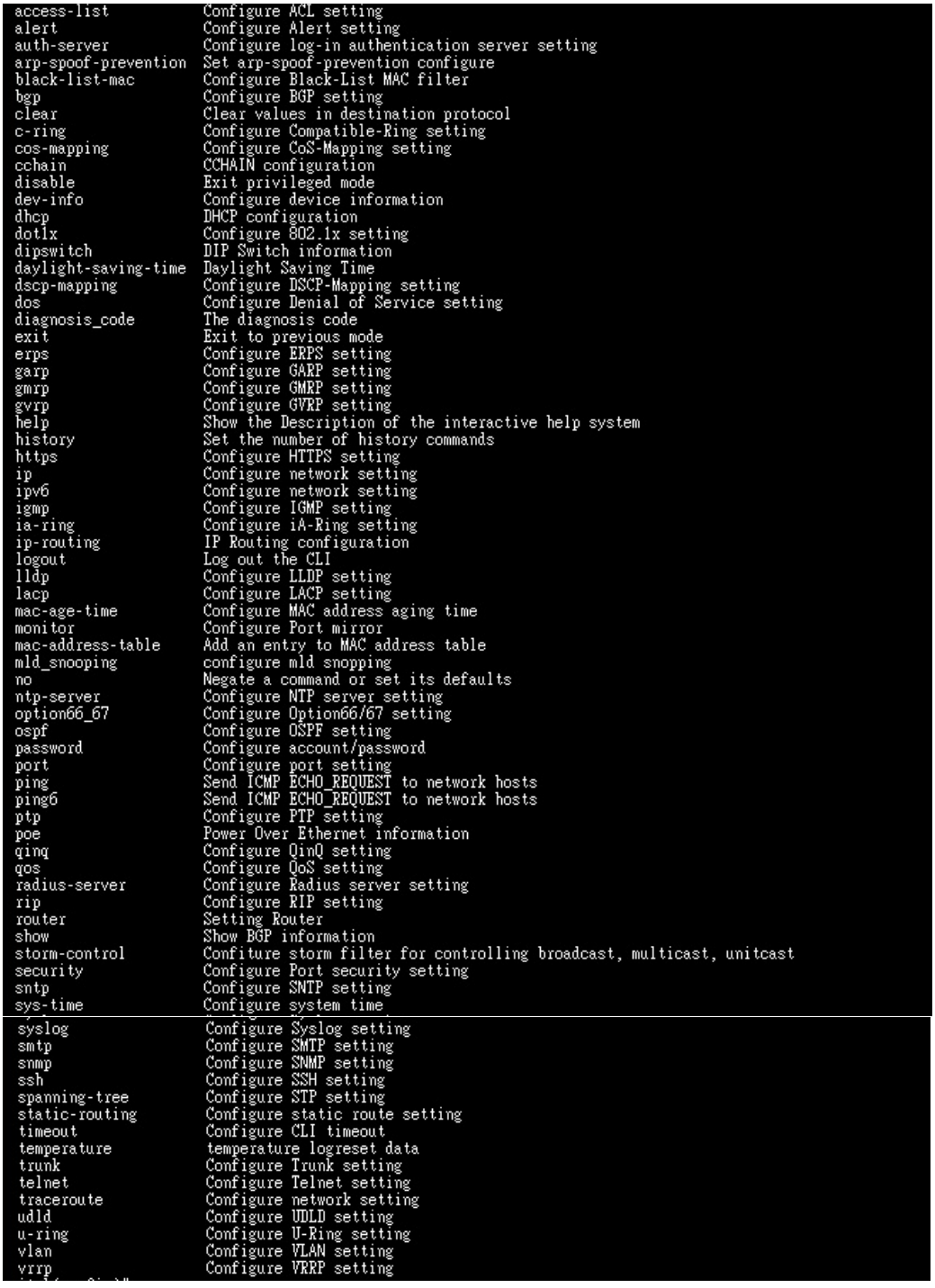


Figure 3.5Example of Commands

3.4.1 Administration Setup using Serial Console

This section shows how users can findthe administrative information and make changes using commands. Detailed explanations of each technical term can be found in Chapter 2 of this manual.Table below show the descriptions of administrative commands for setting up.

Table 3.2Descriptions of Administrative Commands for Setting Up

Command	Description
vlan ip address 1 dhcp enable	Enable DHCP
show vlan ip address 1	Shows DHCP status

vlan ip address 1 <ip-addr><sub-mask>	Set IP address and subnet mask
Ip default-gateway <ip-addr>	Set the gateway IP address (if DHCP is activated)
show vlan ip address	Show IP address, subnet mask
reload	Use this command to reboot the switch
show running-config	Display the running configurations of the switch.
copy running-config startup-config	Backup the switch configurations.
erase startup-config	Reset to default factory settings at the next boot time.
show arp	Show the IP ARP translation table
ping ip-addr <1~999>	Send ICMP Echo-Request to the network host. <1 ~ 999> specifies the number of repetitions.

3.4.2 Spanning Tree Setup using Serial Console

This section shows how users can see spanning tree information and make changes using commands. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

Table 3.3Descriptions of Commands for Setting up Spanning Tree

Command	Description
[no] spanning-tree enable	Enable/disable spanning-tree
[no] spanning-tree bpdu-guard enable	Enable/Disable spanning-tree BPDU-Guard
spanning-tree forward-delay <4~30>	Set the amount of forward delay in seconds. Ex: spanning-tree forward-delay 20: Set forward delay time to 20 seconds.
spanning-tree hello-time <1~10>	Set hello time in seconds
spanning-tree maximum-age <6~40>	Set the maximum age of the spanning tree in seconds
spanning-tree priority <0~61440>	Set priority of the spanning tree bridge
spanning-tree protocol-version <mstp/rstp/stp>	Choose protocol version. A detailed description of mstp/rstp/stp can be found in section Spanning Tree of chapter 2
[no] spanning-tree port edge-port <port #>	Set the port to be edge connection.
[no] spanning-tree port enable-stp <port #>	Enable/Disable spanning-tree for a specific port
[no] spanning-tree port enable-bpdu-guard <port #>	Enable/Disable spanning-tree for a specific port
[no] spanning-tree port non-stp <port#>	Enable or disable spanning tree protocol on this port.
spanning-tree port path-cost <0 ~ 2E8><port #>	Set path cost for a specific port
spanning-tree port priority <0 ~ 240><port #>	Set priority to a specific port
[no] spanning-tree port point-to-point-mac <auto | true | false><port #>	Set the port to be point to point connection. Auto: Specify point to point link auto detection. True: Set the point-to-point link to true. False: Set the link to false.
show spanning-tree	Show spanning-tree information
show spanning-tree port <port #>	Show port information

3.4.3 VRRP Setup using Serial Console

This section shows how users can see VRRP (Virtual Router Redundancy Protocol) information and make changes using commands. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

The following command line interface (CLI) can be used to configure Virtual Routers in the VRRP Setting.

Table 3.4 Descriptions of Commands for Setting up VRRP

Command	Description
vrrp	Enable VRRP
no vrrp	Disable VRRP
vrrp add vrid **<1-255>** vlan **<1-4096>** state **<MASTER|BACKUP>** preempt **<0|1>** priority **<1-254>** advt **<1-255>** auth **<NONE|PASS>** [code **<code>]**	Add a new VRRP instance with vrrp-id, VLAN, state, preempt, priority, advertisement interval, and authentication details such as type (NONE|PASS) and code (in case type is PASS).
no vrrp vrid **<1-255>**	Delete existing VRRP instance
no vrrp vrid all	Delete all existing VRRP instances
vrrp vrid **<1-255>** state **<MASTER|BACKUP>**	Set the VRRP state for existing vrrp-id MASTER or BACKUP.
vrrp vrid **<1-255>** vif**<AA:BB:CC:DD>**	Set a Virtual IP to the existing vrrp-id
no vrrp vrid **<1-255>** vif **<AA:BB:CC:DD>**	Delete an existing virtual IP from existing vrrp-id
vrrp vrid **<1-255>** pre-empt	Enable a preemption mode for an existing vrrp-id
no vrrp vrid **<1-255>** pre-empt	Disable a preemption mode for an existing vrrp-id
vrrp vrid **<1-255>** priority **<1-254>**	Set the Priority 0-255 for an existing vrrp-id, 255 is the highest priority. 0 means master doesn't want to participate.
no vrrp **<1-255> vrid** priority	Set the Priority to default value (100) for an existing vrrp-id.
vrrp vrid **<1-255>** advt **<1-255>**	Set the VRRP packet Advertisement Interval timer
vrrp vrid **<1-255>** auth <**NONE|PASS> [pass-code]**	Set the interface authentication type as NONE or PASS for an existing vrrp-id. If set it to PASS, enter pass-code.
show vrrp vrid **[<1-255>]**	Display the information of all existing virtual routers, if no vrid is entered. Otherwise, if vrid is entered, display the information of that virtual router.
show vrrp vrid **<1-255>** state	Display the state of existing vrrp-id
vrrp restart	Restart vrrp
show vrrp status	Show VRRP Status

Below is the screenshot for the CLI command "**show vrrp vrid**". In this example, three virtual routers are added to VRRP.

```
virtual router id: 53
        configured state: Backup
        running state: Unknown
        vlan: 1
        vlan ip address: 10.0.50.30/255.255.0.0
        priority: 150
        preempt: Disable
        advt interval: 10
        authentication type: No authentication
        virtual interface:
              10.0.50.252
              10.0.50.254

virtual router id: 54
        configured state: Backup
        running state: Unknown
        vlan: 1
        vlan ip address: 10.0.50.30/255.255.0.0
        priority: 100
        preempt: Disable
        advt interval: 10
        authentication type: Password  auth code: check12
        virtual interface:
              10.0.50.56

virtual router id: 55
        configured state: Backup
        running state: Unknown
        vlan: 10
        vlan ip address: 192.168.10.1/255.255.0.0
        priority: 150
        preempt: Disable
        advt interval: 10
        authentication type: No authentication
        virtual interface:
              192.168.10.20
```

Figure 3.6 Example of Virtual Routers Configuration for VRRP

3.4.4 DHCP Server Setup using Serial Console

This section shows how users can see DHCP Server information and make changes using commands. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

The following command line interface (CLI) can be used to configure VLANs in the DHCP Server's setting configuration.

Table 3.5 Descriptions of Commands for Setting up DHCP Server

Command	Description
dhcp server vlan <1-4094>	Add VLAN interface of the DHCP server
show dhcp server vlan [<1-4094>]	Show configuration of DHCP server's VLAN
dhcp server vlan <1-4094>**leasetime***<3200-7200>*	Set lease time for each VLAN
dhcp server vlan <1-4094>**range**<A.B.C.D><A.B.C.D>	Add dynamic IP range for the DHCP server address pool
dhcp server vlan <1-4094>**dns**<A.B.C.D><P.Q.R.S>	Set domain name servers of a VLAN (0.0.0.0 if not used)
dhcp server vlan <1-4094>**gateway**<A.B.C.D><P.Q.R.S>	Set gateways of a VLAN (0.0.0.0 if not used)

Command	Description
dhcp server vlan <1-4094>**netbios-server**<A.B.C.D><P.Q.R.S>	Set netbios servers of a VLAN (0.0.0.0 if not used)
dhcp server vlan <1-4094>**staticip**<*A.B.C.D*>host <*STRING_Y*> mac <*AA:BB:CC:DD:EE:FF*>	Add static IP DHCP server address pool
no dhcp server vlan <1-4094> **range**<*A.B.C.D*>	Delete dynamic IP range from DHCP server address pool
no dhcp server vlan <1-4094>**dns**<*A.B.C.D*>	Delete domain name server from the DHCP server VLAN
no dhcp server vlan <1-4094>**gateway**<*A.B.C.D*>	Delete gateway from the DHCP server VLAN
no dhcp server vlan <1-4094>**netbios-server**<*A.B.C.D*>	Delete netbios server from the DHCP server VLAN
no dhcp server vlan <1-4094>**staticip**<*A.B.C.D*>	Delete static IP from the DHCP server VLAN
show dhcp server	Show running state of DHCP server
no dhcp server	Disable DHCP server
dhcp server	Enable DHCP server

Below is the screenshot for showing VLAN configurations in the DHCP server. In this example, three VLANs are added to the DHCP server.

```
EHG7508# configure
EHG7508(config)# show dhcp server vlan
vlan: 1, ip addr: 10.0.50.30
    domain server1: 0.0.0.0, domain server1: 0.0.0.0
    gateway1: 0.0.0.0, gateway2: 0.0.0.0
    netbios-server1: 0.0.0.0, netbios-server2: 0.0.0.0
    Dynamic ip address range(1)
        [0] 10.0.0.10 10.0.0.20
    Static ip address range(1)
        [0] 10.0.50.1 aa:bb:cc:ab:cd:ef
================================================
vlan: 5, ip addr: 192.168.10.1
    domain server1: 192.168.10.0, domain server1: 192.168.1.0
    gateway1: 0.0.0.0, gateway2: 0.0.0.0
    netbios-server1: 0.0.0.0, netbios-server2: 0.0.0.0
    Dynamic ip address range(0)
    Static ip address range(0)
================================================
vlan: 10, ip addr: 172.168.0.10
    domain server1: 0.0.0.0, domain server1: 0.0.0.0
    gateway1: 0.0.0.0, gateway2: 0.0.0.0
    netbios-server1: 0.0.0.0, netbios-server2: 0.0.0.0
    Dynamic ip address range(1)
        [0] 172.168.0.20 172.168.0.30
    Static ip address range(2)
        [0] 172.168.0.1 aa:bb:cc:dd:ee:ff
        [1] 172.168.10.10 aa:bb:cc:dd:ee:ff
================================================
EHG7508(config)#
```

Figure 3.7 Example of CLI for VLAN Configurations in DHCP Server

3.4.5 PIM SM Setup using Serial Console

This section shows how users can configure Protocol Independent Multicast Sparse Mode (PIMSM) using commands. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

The following command line interface (CLI) can be used to configure PIMSM to support multicast routing.

Table 3.6Descriptions of Commands for PIMSM Configuration

Command	Description
ip pim-sm	Enable PIM-SM
no ip pim-sm	Disable PIM-SM
ip pim-sm hello interval <30-18724>	Configure hello interval for PIM-SM
ip pim-sm spt-switchover no ip pim-sm spt-switchover	Configure Spanning Tree (SPT) type
ip pim-sm vid <1-4094> dr-priority <1-4294967294> route-distance <1-255> route-metric <1-1024>	Configure DR-Priority, Route-Distance and Route-Metric
ip pim-sm rp-priority <0-255> bsr-priority <0-255>	Configure RP priority and BSR priority
ip pim-sm election <static|bootstrap>	Configure PIM-SM election type as either static or bootstrap
ip pim-sm rp-candidate vid <vlan-id> group <A.B.C.D/M>	Configure RP candidate group IP addresses
ip pim-sm rp-address <A.B.C.D> group <A.B.C.D/M>	Configure Static RP address and group address
Static-routing add <name><Dest. IP><mask><Gateway IP>	Add static routing
show ip pim-sm	Display PIM Sparse Mode Configuration
show ip pim-sm bsr	Display PIM Sparse Mode BSR
show ip pim-sm rp-address	Display PIM Sparse Mode Static RP Address
show ip pim-sm neighbor	Display PIM Sparse Mode Neighbor Table
show ip pim-sm routing	Display PIM SM Multicast Routing Table
ip pim-sm restart	Restart PIM SM process
igmp-query-interval	Display IGMP's Query Interval
ip igmp join vid <vlan-id> group <group-address>	Send IGMP join message (*,G)
ip igmp leave vid <vlan-id> group <group-address>	Send IGMP leave message (*,G)

Below is a screenshot of a command line that shows a PIM Sparse Mode configuration.

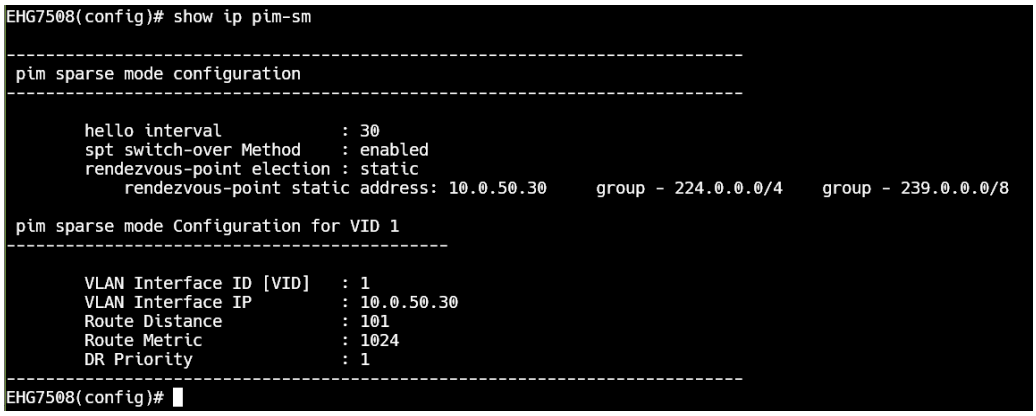


Figure 3.8 Example of PIM SM Configuration

3.4.6 PIM SSM Setup using Serial Console

This section shows how users can configure Protocol Independent Multicast Source Specific Mode (PIM SSM) using commands. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

The following command line interface (CLI) can be used to configure PIM SSM to support multicast routing.

Table 3.7 Descriptions of Commands for PIM SSM Configuration

Command	Description
ip pim-ssm	Enable PIM-SSM
no ip pim-ssm	Disable PIM-SSM
ip pim-ssm hello interval <30-18724>	Configure hello interval for PIM-SSM
ip pim-ssm add-group <A.B.C.D/M>	Configure source group IP addresses
no ip pim-ssm group <A.B.C.D/M>	Delete source group IP addresses
show ip pim-ssm	Display PIM SSM configuration
show ip pim-ssm neighbor	Display PIM SSM Neighbor table
show ip pim-ssm routing	Display PIM SSM multicast routing table
ip pim-ssm restart	Restart PIM SSM
ip pim-ssm vid <1-4094> dr-priority <1-4294967294> route-distance <1-255> route-metric <1-1024>	Configure Designated Router (DR) Priority, Route-Distance and Route Metric
ip igmp join vid <vlan-id> group <group-address>	Send IGMP join message (*,G) for any source multicast
ip igmp join vid <vlan-id> group <group-address. source <source-address>	Send IGMP join message (S,G) for SSM
ip igmp leave vid <vlan-id> group <group-address>	Send IGMP leave message (*,G) for any source multicast
ip igmp leave vid <vlan-id> group <group-address> source <source-address>	Send IGMP leave message (S,G) for SSM

Below is a screenshot of a command line that shows a PIM Source Specific Mode configuration.

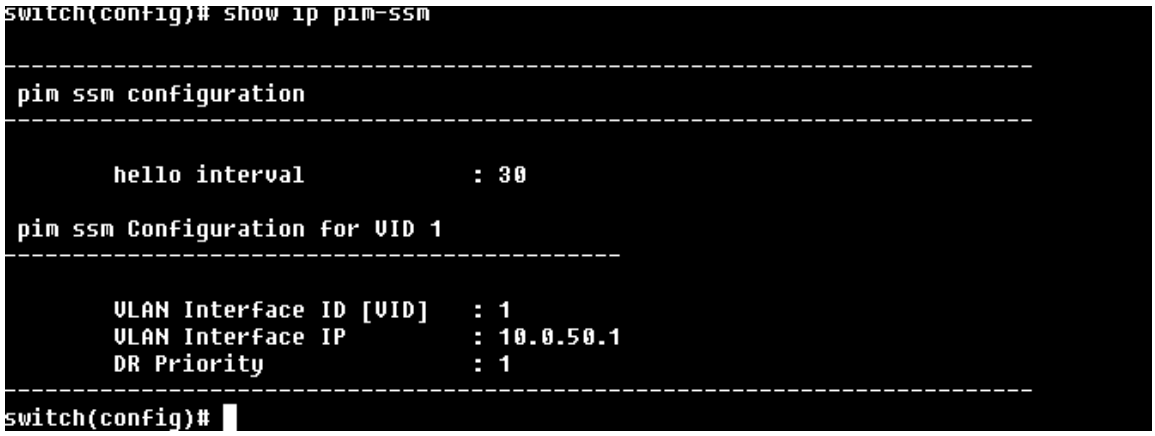


Figure 3.9 Example of PIM Source Specific Mode Configuration

3.4.7 PIM DM Setup using Serial Console

This section shows how users can configure Protocol Independent Multicast Dense Mode (PIM DM) using commands. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

The following command line interface (CLI) can be used to configure PIM DM to support multicast routing.

Table 3.8 Descriptions of Commands for PIM DM Configuration

Command	Description
ip pim-dm	Enable PIM-DM
no ip pim-dm	Disable PIM-DM
ip pim-dm vlan<1-4094> preference <1-255> metric <1-255>	Adding VLAN to PIM-DM
no ip pim-dm vlan <1-4094>	Delate VLAN from PIM-DM

Command	Description
ip pim-dm vlan <1-4094> preference <1-255>	Updating the preference ID for PIM-DM
ip pim-dm vlan <1-4094> metric <1-255>	Updating the metric for PIM-PM

3.4.8 BGP Setup using Serial Console

This section shows how users can inspect BGP information and make changes using commands. Detailed explanations of each technical term can be found in Chapter 2 of this manual.

The following command line interface (CLI) can be used to configure BGP feature of the switch.

Table 3.9 Descriptions of Commands for Setting up BGP Function

Command	Description
bgp bestpath as-path confed	This command specifies that the AS confederation path length must be usedwhen it is available in the BGP best path decision process. Putting "no" in the front of the command to reset to the default, where the device ignores AS confederation path length in the BGP best path selection process.
bgp bestpath compare-routerid	By default, when comparing similar routes from peers, BGP does not consider the router ID of neighbors advertising the routes - BGP simply selects the first received route. Use this command to include router ID in the selection process. That is the similar routes are compared and the route with the lowest router ID is selected. Putting "no" in the front of the command to disable this feature and return the device to the default state, where the device ignores the router ID in the BGP best path selection process.
neighbor <neighborid> port<portnum>	Use this command to specify the TCP port to which packets are sent to on a BGP neighbor.<*neighborid*>specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.<*portnum*>, rangingfrom *0*to*65535*,specifies the TCP port number. Putting "no" in the front of the command to reset the port number back to the default value (TCP port 179).
neighbor <neighborid> weight <weight>	Use this command to set default weights for routes from this BGP or BGP4+ neighbor. <*neighborid*>specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. <*weight*>rangingfrom *0* to *65535* specifies the weight that this command assigns to the route. Putting "no" in the front of the command to remove a weight assignment.
neighbor <*neighborid*> version <version>	Use this command to configure the device to accept only a particular BGP version. <*neighborid*>specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. <v*ersion*>{4} specifies the BGP version number. Use the **no** variant of this command to use the default BGP version (version 4).
Neighbor <*neighborid*> ebgp-multihop [<*count*>]	Use this command to accept and attempt BGP or BGP4+ connections to external peers on indirectly connected networks. <*neighborid*>specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. <*count*>ranging from *1* to *255* is the maximum hop count set in the TTL field of the BGP packets. Use the **no** variant of this command to delete BGP connections to external peers on indirectly connected networks.
Neighbor <*ipaddress*>interface <*interface*>	Use this command to configure the interface name of a BGP4+ speaking neighbor. <*neighborid*>specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. <*interface*> specifies the interface name of BGP neighbor, e.g. vlan2. Use the **no** variant of this command to disable this function.
show ip bgp filter-list<listname>	Use this command to display routes conforming to the filter-list within an IPv4 environment. Use the show bgp ipv6 filter-list (BGP4+ only) command

	to display routes conforming to the filter-list within an IPv6 environment. <*listname*> specifies the regular-expression access list name.
neighbor <*neighborid*> distribute-list <*access-list*> {in|out}	This command filters route updates from a particular BGP or BGP4+ neighbor using an access control list. <*neighborid*>The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. <*access-list*>The access-list used to filter routes. The following types of access-lists: <*WORD*>The name of IP access-list. <*1-199*>The ID number of a standard IP access-list. <*1300-2699*>The ID number of an extended IP access-list. in Indicates that incoming advertised routes will be filtered. out Indicates that outgoing advertised routes will be filtered. The **no** variant of this command removes a previously configured BGP or BGP4+ distribute-list.
neighbor <*peer-group*> peer-group	Use this command to create a peer-group for BGP and BGP4+. <*peer-group*> Enter the name of the peer-group. Use the **no** variant of this command to disable this function.
neighbor <*neighborid*> send-community {both|extended|standard}	Use this command to specify that a community attribute should be sent to a BGP or BGP4+ neighbor. <*neighborid*>Specify the IPv4 address of the BGP neighbor, entered in the format A.B.C.D. both →Sends Standard and Extended Community attributes. Specifying this parameter with the **no** variant of this command results in no standard or extended community attributes being sent. extended→Sends Extended Community attributes. Specifying this parameter with the **no** variant of this command results in no extended community attributes being sent. standard →Sends Standard Community attributes. Specifying this parameter with the **no** variant of this command results in no standard community attributes being sent. Use the **no** variant of this command to remove the entry for the community attribute.
neighbor <*neighborid*> attribute-unchanged {as-path|next-hop|med}	Use this command to advertise unchanged BGP or BGP4+ attributes to the specified BGP or BGP4+ neighbor. <*neighborid*> *s*pecifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. as-path AS path attribute. next-hop Next hop attribute. med Multi Exit Discriminator.
neighbor <*neighborid*> capability orf prefix-list {both|receive|send}	Use this command to advertise ORF (Outbound Route Filters) capability to neighbors. Use this command to dynamically filter updates. The BGP speaker can advertise a prefix list with prefixes it wishes the peer to prune or filter from outgoing updates. <*neighborid*>--Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. orf ---→ Advertises ORF capability to its neighbors. both-→Indicates that the local router can send ORF entries to its peer as well as receive ORF entries from its peer. receive-→Indicates that the local router is willing to receive ORF entries from its peer. Send-→Indicates that the local router is willing to send ORF entries to its peer. Use the **no** variant of this command to disable this function.
neighbor <*neighborid*> unsuppress-map <*route-map-name*>	Use this command to selectively leak more specific routes to a particular BGP or BGP4+ neighbor. <*neighborid*>specifies the IPv4 address of the BGP neighbor, entered in the format A.B.C.D. <*route-map-name*>specifies the

	name of the route-map used to select routes to be unsuppressed. Use the **no** variant of this command to remove selectively leaked specific routes to a particular BGP or BGP4+ neighbor.
neighbor {<*neighborid*>} default-originate [route-map <*routemap-name*>]	Use this command to control the number of prefixes that can be received from a BGP or a BGP4+ neighbor. *<neighborid>*specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. route-map→ If a route-map is specified, then the route table must contain at least one route that matches the permit criteria of the route map before the default route will be advertised to the specified neighbor. <*routemap-name*> is the route-map name. Use the **no** variant of this command to send no route as a default route.
neighbor <*neighborid*> capability route-refresh	Use this command to advertise route-refresh capability to the specified BGP and BGP4+ neighbors. *<neighborid>*specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to disable this function.
neighbor <*neighborid*> dont-capability-negotiate	Use this command to disable capability negotiation for BGP and BGP4+. *<neighborid>*specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to enable capability negotiation for BGP and BGP4+.
neighbor <*neighborid*> next-hop-self	Use this command to configure the BGP router as the next hop for a BGP speaking neighbor or peer group. *<neighborid>*specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to Disable the BGP router as the next hop for a BGP speaking neighbor or peer group.
neighbor <*neighborid*> override-capability	Use this command to override a capability negotiation result for BGP. *<neighborid>*specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to Delete a capability negotiation result for BGP.
neighbor <*neighborid*> passive	Use this command to configure the local BGP or BGP4+ router to be passive with regard to the specified BGP or BGP4+ neighbor. This has the effect that the BGP or BGP4+ router will not attempt to initiate connections to this BGP or BGP4+ neighbor but will accept incoming connection attempts from the BGP or BGP4+ neighbor. *<neighborid>*specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to disable this function.
neighbor <*neighborid*> route-server-client	Use this command to specify the peer as route server client. *<neighborid>*specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to delete route-server-client.
neighbor <*neighborid*> soft-reconfiguration inbound	Use this command to configure the device to start storing all updates from the BGP or BGP4+ neighbor, without any consideration of any inward route filtering policy that might be applied to the connection with this BGP or BGP4+ neighbor. *<neighborid>* specifies the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. Use the **no** variant of this command to disable this function for a BGP or BGP4+ neighbor.
bgp cluster-id *<ip-address>*	This command configures the cluster-id if the BGP cluster has more than one route reflector. A cluster includes one or more route reflectors and their clients. Usually, each cluster is identified by the router-id of its single route reflector. *<ip-address>--A.B.C.D* Route Reflector Cluster-id in IP address format. Use the **no** variant of this command removes the cluster ID.
set local-preference *<pref-value>*	This command changes the default local preference value. The local preference indicates the BGP local preference path attribute when there are multiple paths to the same destination. The path with the higher preference

	is chosen. *<pref-value>*ranging from0 to 4294967295, configures local preference value. The default local preference value is 100. The **no** variant of this command reverts to the default setting.
bgp default local-preference <*pref-value*>	This command changes the default local preference value. <*pref-value*> ranging from 0 to 4294967295 configures default local preference value. The default local preference value is 100. The **no** variant of this command reverts to the default local preference value of 100.
distance *<1-255><ip-address/m>*[<*listname*>]	This command sets the administrative distance for BGP and BGP4+ routes. The device uses this value to select between two or more routes to the same destination from two different routing protocols. Set the administrative distance for BGP routes in the Router Configuration mode, and for BGP4+ routes in IPv6 Address Family Configuration mode. *<1-255>*The administrative distance value you are setting for the route. *<ip-address/m>*The IP source prefix that you are changing the administrative distance for, entered in the form A.B.C.D/M. This is an IPv4 address in dotted decimal notation followed by a forward slash, and then the prefix length. *<listname>*The name of the access list to be applied to the administrative distance to selected routes. The **no** variant of this command sets the administrative distance for the route to the default for the route type.
set metric <metric value>	Use this command to add a metric set clause to a route map entry. *<metric-value>*ranging from0 to 4294967295. The **no** variant of this command to delete a metric set clause to a route map entry.
bgp bestpath med {[confed] [missing-as-worst]}	This command controls how the Multi Exit Discriminator (MED) attribute comparison is performed. *Confed*→ Compares MED among confederation paths. *missing-as-worst*→ Treats missing MED as the least preferred one. Use the **no** variant of this command to prevent BGP from considering the MED attribute when comparing paths.
ip as-path access-list <*listname*> {deny|permit} <*reg-exp*>	This command defines a BGP and BGP4+ Autonomous System (AS) path access list. The named AS path list is a filter based on regular expressions. If the regular expression matches the AS path in a BGP update message, then the permit or deny condition applies to that update. Use this command to define the BGP access list globally, then use neighbor configuration commands to apply the list to a particular neighbor. <*listname*> Specifies the name of the access list. <deny> Denies access to matching conditions. <permit> Permits access to matching conditions. <*reg-exp*> Specifies a regular expression to match the BGP AS paths ^ Caret Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match. $ Dollar sign Used to match the end of the input string. . Period Used to match a single character (white spaces included). * Asterisk Used to match none or more sequences of a pattern. + Plus sign Used to match one or more sequences of a pattern. ? Question mark Used to match none or one occurrence of a pattern. _ Underscore Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string. [ ] Brackets Specifies a range of single-characters. - Hyphen Separates the end points of a range The **no** variant of this command disables the use of the access list.

Below are the screenshot examples ofBGP configurationslisted inTable 3.9.

```
switch(config)#
switch(config)# bgp bestpath as-path confed
switch(config)#
switch(config)# show bgp bestpath as-path confed
bgp bestpath as-path confed
switch(config)#
switch(config)#
switch(config)# no bgp bestpath as-path confed
switch(config)#
switch(config)# show bgp bestpath as-path confed
Disabled bgp bestpath as-path confed
```

Figure 3.10 Examples of CLI for Neighbor Bestpath AS-Path Confed Configuration in BGP

```
switch(config)#
switch(config)# bgp bestpath compare-routerid
switch(config)#
switch(config)#
switch(config)# show bgp bestpath compare-routerid
bgp bestpath compare-routerid
switch(config)# no bgp bestpath compare-routerid
switch(config)#
switch(config)# show bgp bestpath compare-routerid
Disabled bgp bestpath compare-routerid
```

Figure 3.11 Examples of CLI for Neighbor Bestpath Compare-Routerid Configuration in BGP

```
switch(config)# bgp neighbor 10.0.50.4 port 65535
switch(config)#
switch(config)# show bgp neighbor port
neighbor 10.0.50.4 port 65535
switch(config)#
switch(config)#
switch(config)# no bgp neighbor 10.0.50.4 port 65535
switch(config)#
switch(config)# show bgp neighbor port
```

Figure 3.12 Examples of CLI for Neighbor Port Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.5 weight 65535
switch(config)#
switch(config)# show bgp neighbor weight
neighbor 10.0.50.5 weight 65535
switch(config)#
switch(config)# no bgp neighbor 10.0.50.5 weight 65535
```

Figure 3.13 Examples of CLI for Neighbor Weight Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.3 version 4
switch(config)#
switch(config)# show bgp neighbor version
neighbor 10.0.50.3 version 4
switch(config)#
switch(config)# no bgp neighbor 10.0.50.3 version 4
switch(config)#
switch(config)# show bgp neighbor version
```

Figure 3.14 Examples of CLI for Neighbor Version Configuration in BGP

```
switch(config)# bgp neighbor 10.0.50.4 ebgp-multihop 255
switch(config)#
switch(config)# show bgp neighbor ebgp-multihop
neighbor 10.0.50.4 ebgp-multihop 255
switch(config)# no bgp neighbor 10.0.50.2 ebgp-multihop 255
switch(config)#
switch(config)# show bgp neighbor ebgp-multihop
```

Figure 3.15 Examples of CLI for Neighbor EBGP-Multihop Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.5 interface vlan2
switch(config)#
switch(config)# show bgp neighbor interface
neighbor 10.0.50.5 interface vlan2
switch(config)#
switch(config)# no bgp neighbor 10.0.50.5 interface vlan2
switch(config)#
switch(config)# show bgp neighbor interface
switch(config)#
```

Figure 3.16 Examples of CLI for Neighbor Interface Configuration in BGP

```
switch(config)#
switch(config)# show ip bgp filter-list mylist
switch(config)# BGP: show ip bgp filter-list mylist

------------------------------------------------------------------------

bgpd> enable
bgpd# show ip bgp filter-list mylist
% mylist is not a valid AS-path access-list name
bgpd#
bgpd#
------------------------------------------------------------------------
========================================================================

switch(config)#
switch(config)#
```

Figure 3.17 Examples of CLI for Show Filter-List Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.2 distribute-list mylist out
switch(config)#
switch(config)# show bgp neighbor distribute-list name
neighbor 10.0.50.2 distribute-list mylist out
switch(config)#
switch(config)# bgp neighbor 10.0.50.2 distribute-list 199 in
switch(config)#
switch(config)# show bgp neighbor distribute-list
neighbor 10.0.50.2 distribute-list 199 in
switch(config)# no bgp neighbor 10.0.50.2 distribute-list 199 in
switch(config)#
switch(config)# show bgp neighbor distribute-list
switch(config)#
switch(config)#
```

Figure 3.18 Examples of CLI for Neighbor Distribute-List Name Configurations in BGP

```
switch(config)#
switch(config)# bgp neighbor group1 peer-group
switch(config)#
switch(config)# show bgp neighbor peer-group
neighbor group1 peer-group
switch(config)# no bgp neighbor group1 peer-group
switch(config)#
switch(config)# show bgp neighbor peer-group
switch(config)#
```

Figure 3.19 Examples of CLI for Neighbor Peer-Group Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.6 send-community extended
switch(config)#
switch(config)# show bgp neighbor send-community
neighbor 10.0.50.6 send-community extended
switch(config)#
switch(config)# no bgp neighbor 10.0.50.6 send-community extended
switch(config)#
switch(config)# show bgp neighbor send-community
switch(config)#
```

Figure 3.20 Examples of CLI for Neighbor Send-Community Extended Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.4 attribute-unchanged as-path
switch(config)# show bgp neighbor attribute-unchanged
neighbor 10.0.50.4 attribute-unchanged as-path
switch(config)#
switch(config)# no bgp neighbor 10.0.50.4 attribute-unchanged as-path
switch(config)#
switch(config)# show bgp neighbor attribute-unchanged
switch(config)#
```

Figure 3.21 Examples of CLI for Neighbor Attribute-Unchanged AS-Path Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.2 capability orf prefix-list send
switch(config)# show bgp neighbor capability orf prefix-list
neighbor 10.0.50.2 capability orf prefix-list send
switch(config)#
switch(config)# no bgp neighbor 10.0.50.2 capability orf prefix-list
switch(config)#
switch(config)# show bgp neighbor capability orf prefix-list
switch(config)#
```

Figure 3.22 Examples of CLI for Neighbor Capability ORF Prefix-List Configuration in BGP

```
switch(config)#
switch(config)#
switch(config)# bgp neighbor 10.0.50.5 unsuppress-map mymap
switch(config)#
switch(config)# show bgp neighbor unsuppress-map
neighbor 10.0.50.5 unsuppress-map mymap
switch(config)#
switch(config)# no bgp neighbor 10.0.50.5 unsuppress-map mymap
switch(config)#
switch(config)# show bgp neighbor unsuppress-map
```

Figure 3.23 Examples of CLI for Neighbor Unsuppress-Map Configuration in BGP

```
switch(config)# bgp neighbor 10.0.50.5 capability route-refresh
switch(config)#
switch(config)#
switch(config)# show bgp neighbor capability route-refresh
neighbor 10.0.50.5 capability route-refresh
switch(config)#
switch(config)# no bgp neighbor 10.0.50.5 capability route-refresh
switch(config)#
switch(config)# show bgp neighbor capability route-refresh
```

Figure 3.24 Examples of CLI for Neighbor Capability Route-Fresh Configuration in BGP

```
switch(config)# bgp neighbor 10.0.50.5 dont-capability-negotiate
switch(config)#
switch(config)# show bgp neighbor dont-capability-negotiate
neighbor 10.0.50.5 dont capability negotiate
switch(config)#
switch(config)# no bgp neighbor 10.0.50.5 dont-capability-negotiate
switch(config)#
switch(config)# show bgp neighbor dont-capability-negotiate
```

Figure 3.25 Examples of CLI for Neighbor Don't Capability Negotiate Configuration in BGP

```
switch(config)# bgp neighbor 10.0.50.2 next-hop-self
switch(config)#
switch(config)#
switch(config)# show bgp neighbor next-hop-self
neighbor 10.0.50.2 next-hop-self
switch(config)# show bgp neighbor next-hop-self
neighbor 10.0.50.2 next-hop-self
switch(config)#
switch(config)# no bgp neighbor 10.0.50.2 next-hop-self
switch(config)#
switch(config)# show bgp neighbor next-hop-self
switch(config)#
```

Figure 3.26 Examples of CLI for Neighbor Next-Hop-Self Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.5 override-capability
switch(config)#
switch(config)# show bgp neighbor override-capability
neighbor 10.0.50.5 override-capability
switch(config)#
switch(config)# no bgp neighbor 10.0.50.5 override-capability
switch(config)#
switch(config)# show bgp neighbor override-capability
```

Figure 3.27 Examples of CLI for Neighbor Override Capability Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.4 passive
switch(config)#
switch(config)# show bgp neighbor passive
neighbor 10.0.50.4 passive
switch(config)#
switch(config)# show bgp neighbor passive
neighbor 10.0.50.4 passive
switch(config)#
switch(config)# no bgp neighbor 10.0.50.4 passive
switch(config)#
switch(config)# show bgp neighbor passive
```

Figure 3.28 Examples of CLI for Neighbor Passive Configuration in BGP

```
switch(config)#
switch(config)# bgp neighbor 10.0.50.6 route-server-client
switch(config)#
switch(config)# show bgp neighbor route-server-client
neighbor 10.0.50.6 route-server-client
switch(config)#
switch(config)# no bgp neighbor 10.0.50.6 route-server-client
switch(config)#
switch(config)# show bgp neighbor route-server-client
switch(config)#
switch(config)#
```

Figure 3.29 Examples of CLI for Neighbor Route Server Client Configuration BGP

```
switch(config)#
switch(config)# show bgp neighbor soft-reconfiguration
neighbor 10.0.50.6 soft-reconfiguration inbound
switch(config)#
switch(config)# no bgp neighbor 10.0.50.6 soft-reconfiguration inbound
switch(config)#
switch(config)# show bgp neighbor soft-reconfiguration
switch(config)#
switch(config)#
switch(config)#
switch(config)# bgp neighbor 10.0.50.6 soft-reconfiguration inbound
switch(config)#
switch(config)# show bgp neighbor soft-reconfiguration
neighbor 10.0.50.6 soft-reconfiguration inbound
```

Figure 3.30 Examples of CLI for Neighbor Soft-Reconfiguration Inbound Configuration in BGP

```
switch(config)#
switch(config)# bgp cluster-id 10.10.1.1
switch(config)#
switch(config)# show bgp cluster-id
bgp cluster-id 10.10.1.1
switch(config)#
switch(config)# no bgp cluster-id 10.10.1.1
switch(config)#
switch(config)# show bgp cluster-id
switch(config)#
switch(config)#
```

Figure 3.31 Examples of CLI for Cluster-ID Configuration in BGP

```
switch(config)#
switch(config)# bgp set local-preference 2345555
switch(config)#
switch(config)#
switch(config)# show bgp set local-preference
set local-preference 2345555
switch(config)#
switch(config)# no bgp set local-preference 2345555
switch(config)#
switch(config)# show bgp set local-preference
switch(config)#
```

Figure 3.32 Examples of CLI for Set Local-Preference Configuraion in BGP

```
switch(config)#
switch(config)# bgp default local-preference 100
switch(config)#
switch(config)# show bgp default local-preference
bgp default local-preference 100
switch(config)#
```

```
switch(config)#
switch(config)# show bgp default local-preference
bgp default local-preference 100
switch(config)#
switch(config)# no bgp default local-preference 100
switch(config)#
switch(config)# show bgp default local-preference
switch(config)#
```

Figure 3.33 Examples of CLI for Default Local Preference Configurations in BGP

```
switch(config)# bgp distance 1 1.1.1.1/12 atop
switch(config)#
switch(config)# show bgp distance access-list
distance 1 1.1.1.1/12 atop
switch(config)# no bgp distance 1 1.1.1.1/12 atop
switch(config)#
switch(config)# show bgp distance access-list
```

Figure 3.34 Examples of CLI for Distance Configuration in BGP

```
switch(config)#
switch(config)# bgp set metric 4294967295
switch(config)#
switch(config)# show bgp set metric
set metric 4294967295
switch(config)#
switch(config)# no bgp set metric 4294967295
switch(config)#
switch(config)# show bgp set metric
Disabled Metric
switch(config)#
```

Figure 3.35 Examples of CLI for Set Metric Configuration in BGP

```
switch(config)#
switch(config)# bgp bestpath med missing-as-worst
switch(config)#
switch(config)# show bgp bestpath med
bgp bestpath med missing-as-worst
switch(config)#
switch(config)# show bgp bestpath med
bgp bestpath med missing-as-worst
switch(config)#
switch(config)# no bgp bestpath med missing-as-worst
switch(config)#
switch(config)# show bgp bestpath med
switch(config)#
```

Figure 3.36 Examples of CLI for Best Path Med Configuration in BGP

```
switch(config)#
switch(config)# bgp ip as-path access-list mylist permit ^
switch(config)#
switch(config)# show bgp ip as-path access-list
ip as-path access-list mylist permit ^
switch(config)#
switch(config)# no bgp ip as-path access-list mylist permit ^
switch(config)#
switch(config)# show bgp ip as-path access-list
switch(config)#
```

Figure 3.37 Examples of CLI for IP AS-PATH Access List Configuration in BGP

4 Configuring with a Telnet Console

An alternative configuration method is the Telnet method and it is described in this chapter.

4.1 Telnet

Telnet is a remote terminal software to login to any remote telnet servers. It is typically installed in most of the operating systems. In order to use it, users open a command line terminal (e.g., cmd.exe for Windows Operating System).

4.2 Telnet Log-in

After the command line terminal is opened, type in “telnet 10.0.50.1” as shown in Figure 4.1.Note that telnet command needs to follow by IP address or domain name.In this example, the default IP address is 10.0.50.1. If users change the switch IP address, the IP address to log-in should be changed to match the new switch IP address.

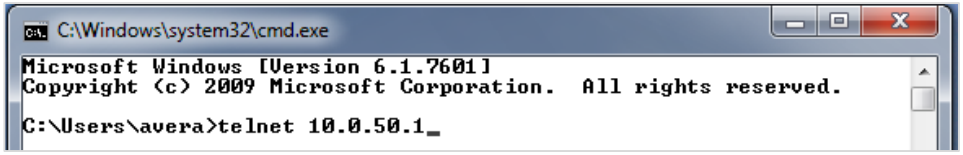


Figure 4.1Telnet Command

4.3 Command Line Interface for Telnet

After input the telnet command line, the switch's interface is displayed as shown in Figure 4.2.

Figure 4.2Log-in Screen using Telnet

Users will see the welcome screen to the switch interface. From Chapter 3, configuring through telnet is similar to configuring through the serial console. Users are automatically logged into the privileged mode. The configuration commands are also similar to the serial console methods. (Please refer to Chapter **錯誤! 未知的選項引數。** for more information on configuration).

4.4 Commands in the Privileged Mode

When users do not know the commands to use for the command line configuration, users type in "?"and the commands are displayed on screen as shown in **錯誤! 未知的選項引數。**.

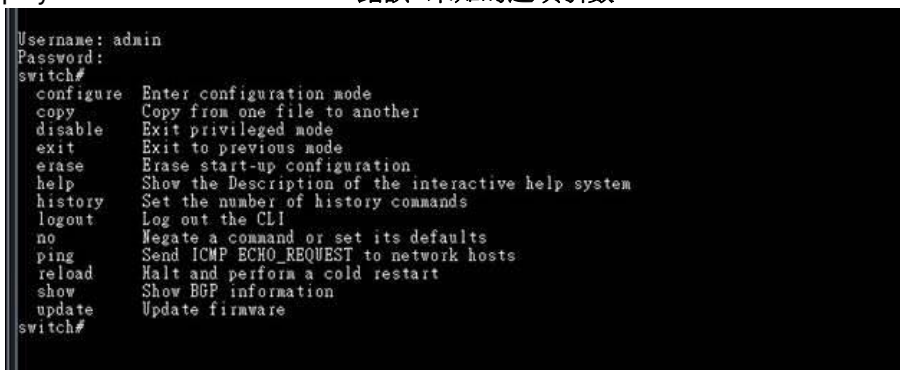


Figure 4.3Commands in the Privileged Mode

4.5 Commands in the Configuration Mode

When users type in "?"in configuration mode, a long list of commands isdisplayed on screen as shown in

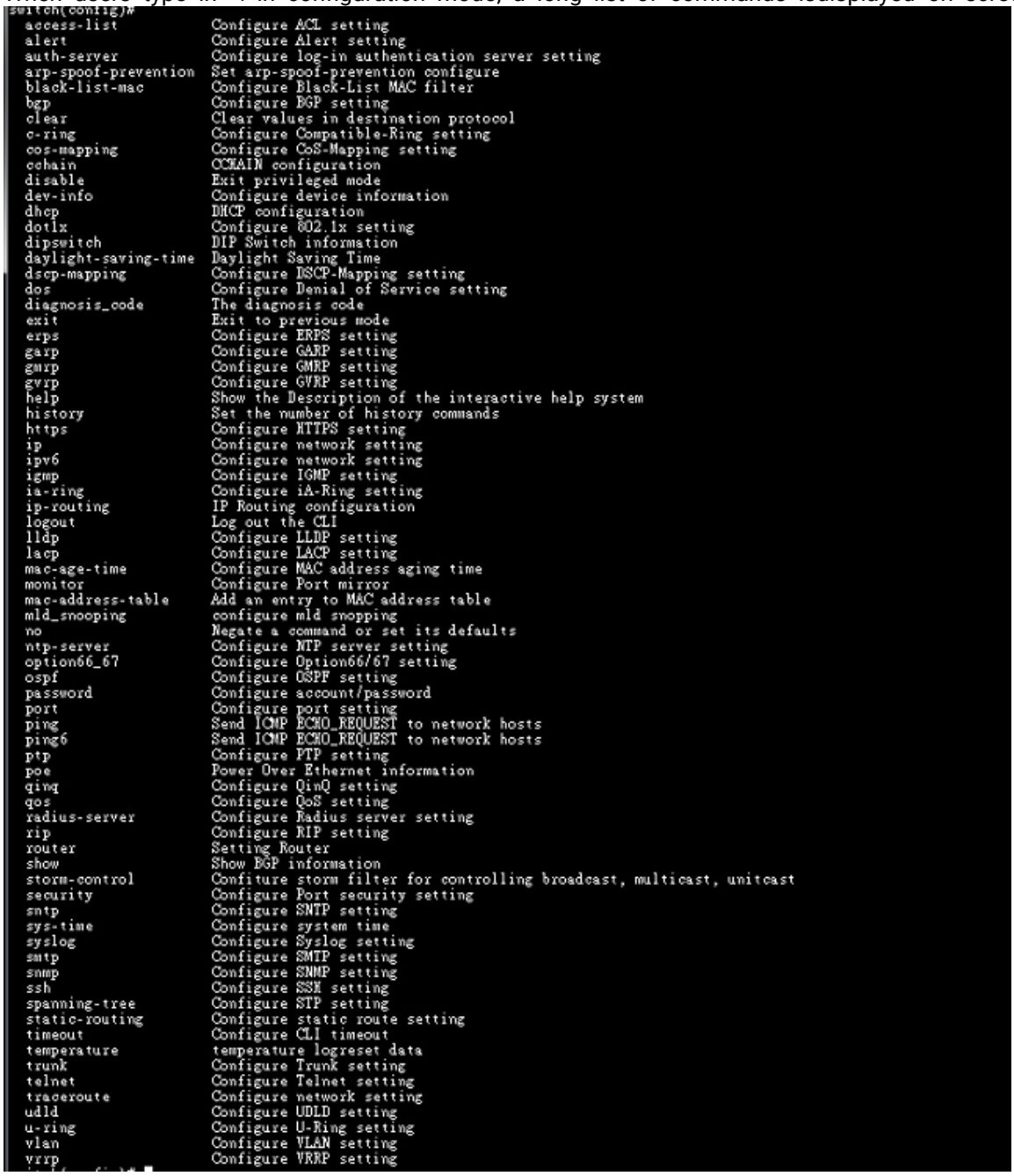


Figure 4.4. Table 4.1 shows all commands that can be used to configure the switch in the configuration mode.

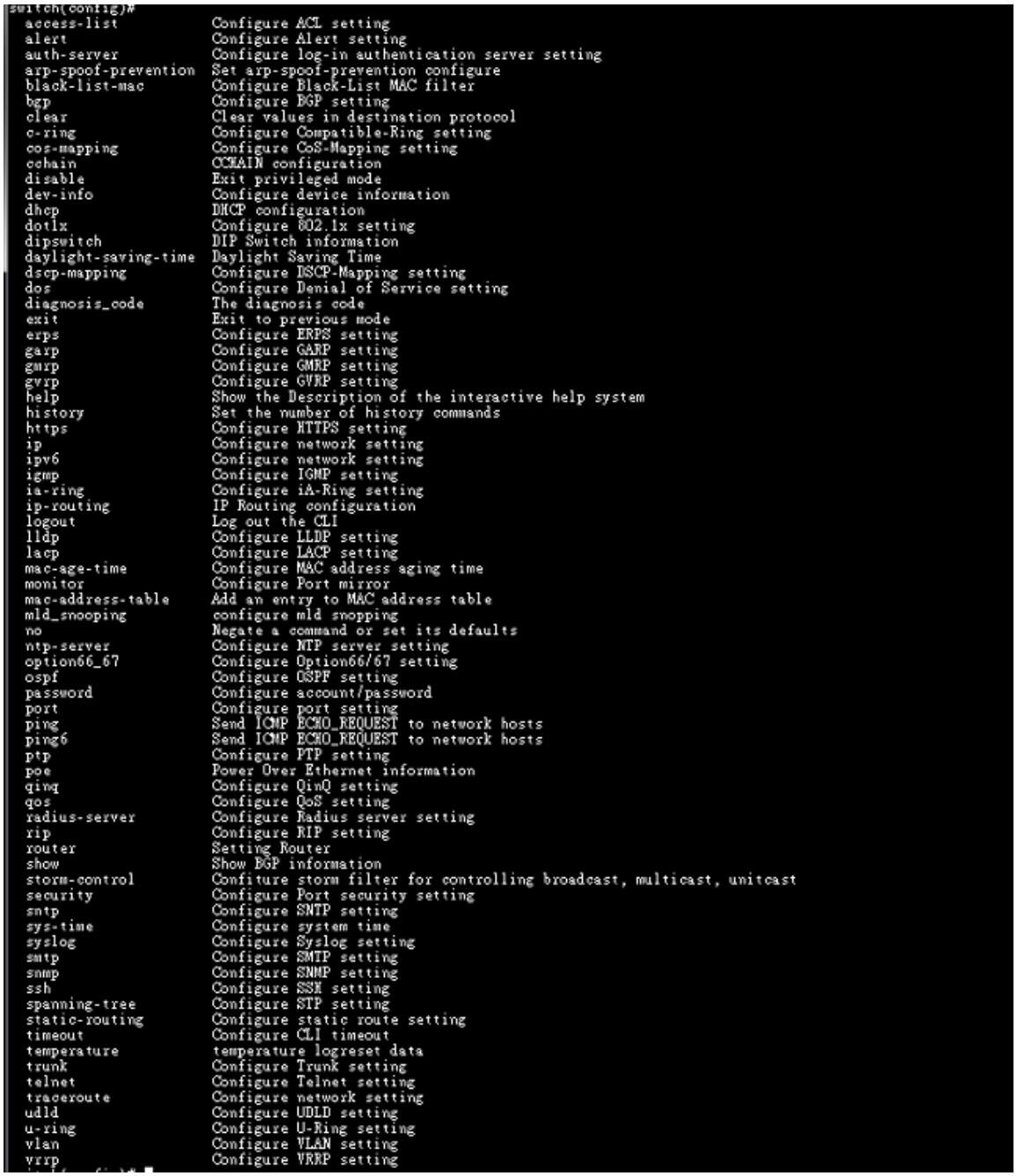


Figure 4.4Commands in the Configuration Mode

Table 4.1Commands in the Configuration Mode

Command	Descriptions
access-list	Configure ACL setting
alert	Configure Alert setting
auth-server	Configure log-in authentication server setting
arp-spoof-prevention	Set arp-spoof-prevention configure
black-list-mac	Configure Black-List MAC filter
bgp	Configure BGP setting
clear	Clear values in destination protocol
c-ring	Configure Compatible-Ring setting
cos-mapping	Configure CoS-Mapping setting

cchain	CCHAIN configuration
disable	Exit privileged mode
dev-info	Configure device information
dhcp	DHCP configuration
dot1x	Configure 802.1x setting
dipswitch	DIP Switch information
daylight-saving-time	Daylight Saving Time
dscp-mapping	Configure DSCP-Mapping setting
dos	Configure Denial of Service setting
diagnosis_code	The diagnosis code
exit	Exit to previous mode
erps	Configure ERPS setting
garp	Configure GARP setting
gmrp	Configure GMRP setting
gvrp	Configure GVRP setting
help	Show the Description of the interactive help system
history	Set the number of history commands
https	Configure HTTPS setting
ip	Configure network setting
ipv6	Configure network setting
igmp	Configure IGMP setting
ia-ring	Configure iA-Ring setting
ip-routing	IP Routing configuration
logout	Log out the CLI
lldp	Configure LLDP setting
lacp	Configure LACP setting
mac-age-time	Configure MAC address aging time
monitor	Configure Port mirror
mac-address-table	Add an entry to MAC address table
mld_snooping	configure mld snopping
no	Negate a command or set its defaults
ntp-server	Configure NTP server setting
option66_67	Configure Option66/67 setting
ospf	Configure OSPF setting
password	Configure account/password
port	Configure port setting
ping	Send ICMP ECHO_REQUEST to network hosts
ping6	Send ICMP ECHO_REQUEST to network hosts
ptp	Configure PTP setting
poe	Power Over Ethernet information
qinq	Configure QinQ setting
qos	Configure QoS setting
radius-server	Configure Radius server setting
rip	Configure RIP setting
router	Setting Router
show	Show BGP information
storm-control	Configure storm filter for controlling broadcast, multicast, unitcast
security	Configure Port security setting
sntp	Configure SNTP setting
sys-time	Configure system time
syslog	Configure Syslog setting
smtp	Configure SMTP setting

Note:Please see Chapter 3 for the details of switch configuration.

5 Device Management Utility

Atop also provides a software utility called **Device Management Utility** to assist the users in configuring the product. The Device Management Utility was formerly called Device View or Serial Manager. The latest Device Management Utility is version 5.20. This chapter will describe how to use the Device Management Utility with the RHG9XXX industrial managed switch. After installing the utility software on your PC. Please click on the Device Management Utility's icon to start the program. Figure 5.1 illustrates the GUI of the Device Management Utility.

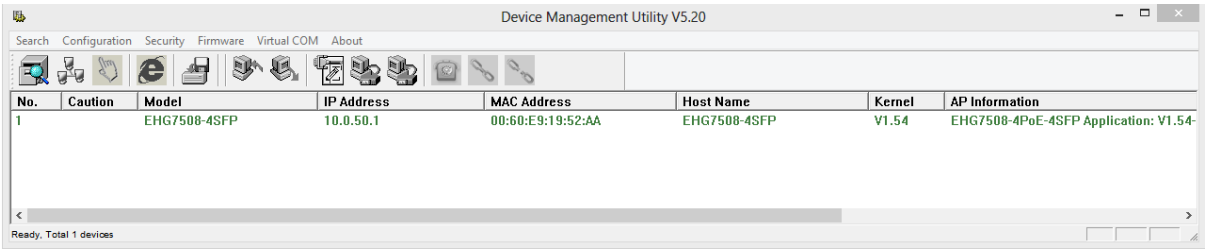


Figure 5.1 Device Management Utility

If the managed switch is on the same subnet as the PC that runs the Device Management Utility, the users should be able to find the switch on the list of the device as shown in Figure 5.1. If for some reason, it cannot be found, the user can click the first icon called **Rescan** on the icon bar to search for the device connected to the same subnet as the Device Management Utility. Depicts the Search icon.

Figure 5.2Rescan (Search) Icon

To perform any task on the desired device, please click to select the entry of that particular device on the list inside the window of Device Management Utility. Typically, when the users double-click the entry, the Device Management Utility will connect to the switch and perform a login process.

It is strongly recommended the users to setup the administration password for the managed switch for network security purpose. If no administration password is set, the Device Management Utility will be able to login to and change any configuration on the device.

If the**Local Login Setting** was configured in Section 2.3.1, a login dialog will pop-up as shown in when the Device Management Utility try to select the **Config by Browser** menu under the **Configuration** pulldown menu or click on the fourth icon on the icon bar. The users then can enter the **User Name** and **Password** to verify the identity. Note that the User Name is typically set to "admin" and Password is "default"for convenient.

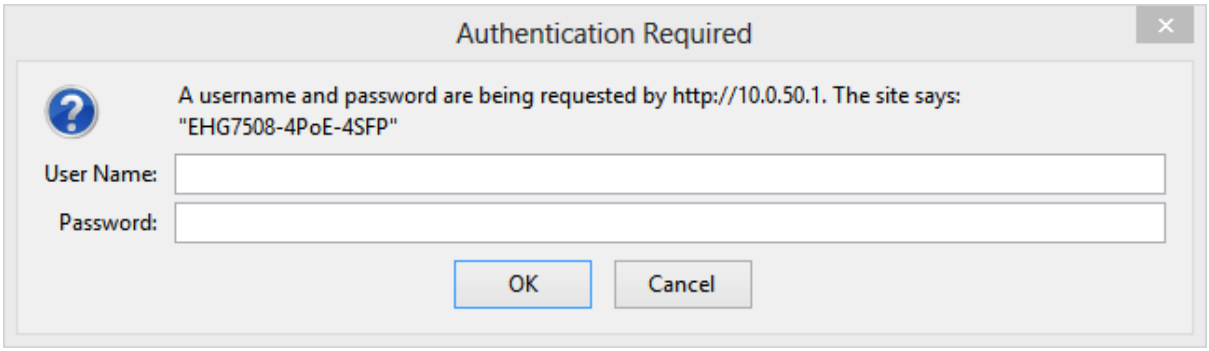


Figure 5.3 Authentication to Login to RHG9XXX switch

5.1 Network Setting

While the device is selected, the user can configure the network parameters by clicking on the Network icon, the second icon on the icon bar as depicted in Figure 5.4. Alternatively, the users can click on the pulldown menu **Configuration** and select **Network…** menu.

Figure 5.4 Network Configure Icon

The **Network Setting** dialog window will pop-up as shown in Figure 5.5. The users can enable the DHCP options by checking the box in front of **DHCP (Obtain an IP automatically)** option. This will allow the device to get its new IP address and other network parameters from a DHCP server from the network. Alternatively, the users can manually set the **IP address**, **Subnet mask**, **Gateway**, and **Host name**.

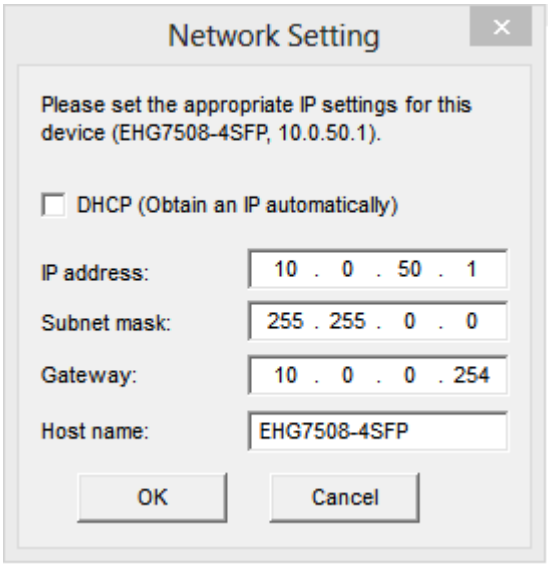


Figure 5.5 Network Setting Dialog

After clicking on the **OK** button, another dialog window will pop-up to ask for authorization in modification of this managed switch. The users are required to enter the correct **Password**. Note that the **User Name** is default as admin which cannot be changed. Then, click the **Authorize** button to allow the change of the network parameter.

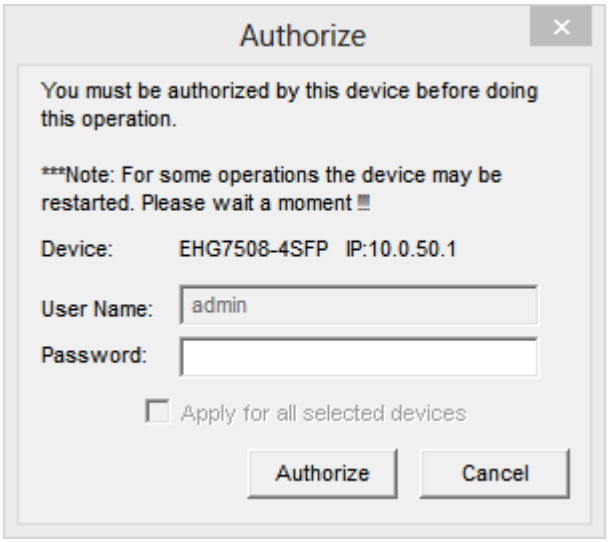


Figure 5.6 Administration Verification before Changing the Network Setting

A warning dialog will pop-up as shown in Figure 5.7 to inform the users that the device will restart after the network configuration was changed. Note that if the configurations were not changed, it may be because of the wrong user name, password, or IP configuration. The users should check these password settings or network settings of the product.

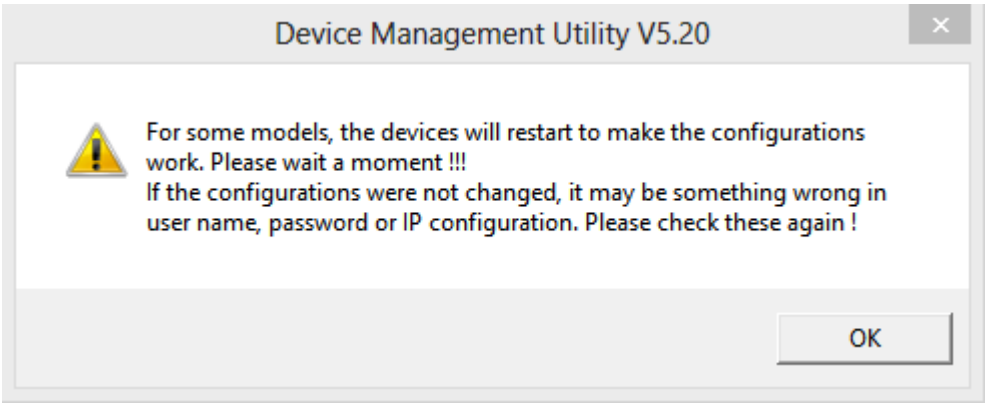


Figure 5.7 Warning Dialog before the Device Restart

If the IP address was changed, the users may need to search for the device again using the **Rescan** icon or the first icon on the icon bar.

5.2 Topology Diagram

Device management Utility comes with a visualization tool called **Topology Diagram** to automatically draw a network diagram. The users can select the **Topology Diagram** menu under the **Configuration** pulldown menu to start the visualization tool as shown in Figure 5.8. The current version of the Topology Diagram is 1.4.0. Note that the tools can display the device discovered by the Device Management Utility and draw a connection between devices in the network that can be reached by the Device Management Utility. Note that to be able to use the Topology Diagram, the switch's LLDP feature in Section 2.19.1 must be enabled.

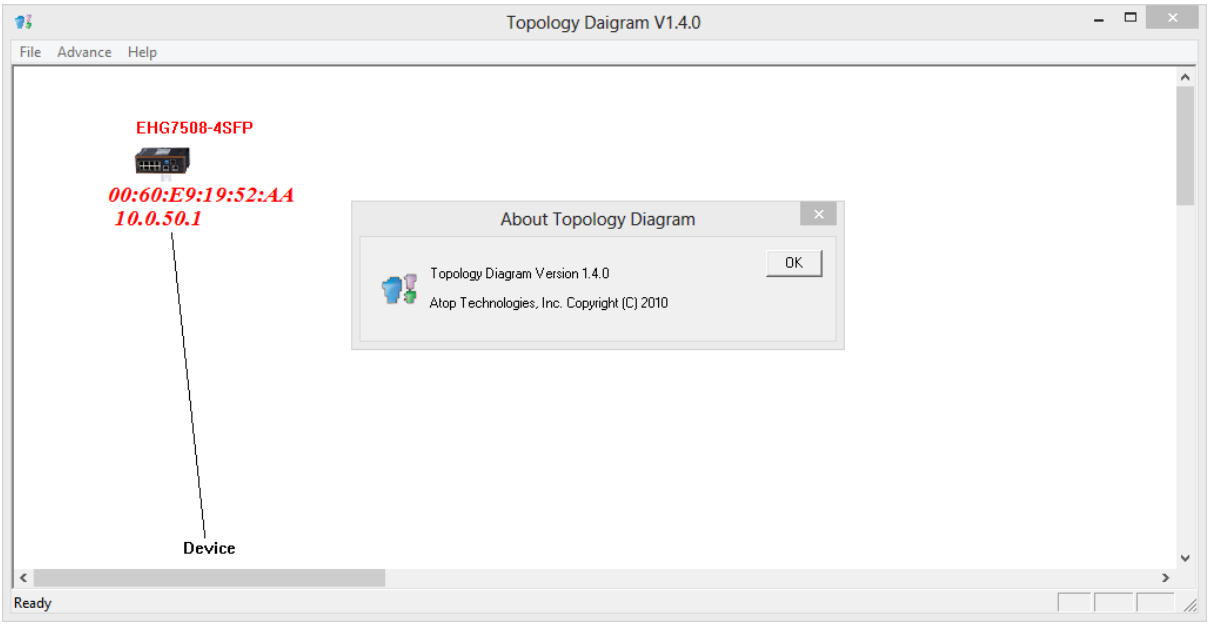


Figure 5.8 Topology Diagram

Additional information can also be display on the diagram which are the **Port** number and the **MAC address** of the device that is currently connecting to the RHG9XXX switch. Please select **Show Information** menu under the **File** pulldown menu. Figure 5.9 shows the result of additional information.

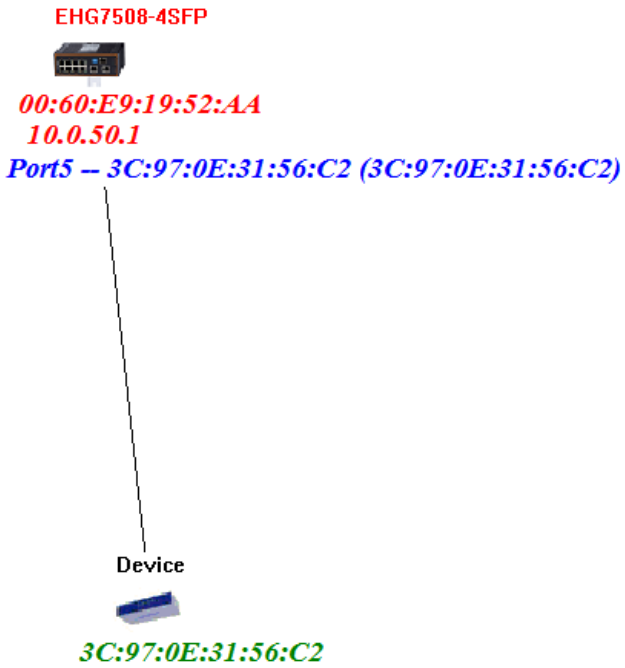


Figure 5.9 Show Information on Topology Diagram

Note that the Topology Diagram can be used to check the Ring Topology. The user can select the **RingCheck** menu from the **Advance** pulldown menu.

5.3 Firmware Update

The Device Management Utility can be used to update firmware of the switch. To perform this task, the users can click on the fifth icon on the icon bar as shown in Figure 5.10. Alternatively, the **Firmware Download…**menu under the **Firmware** pulldown menu can also perform this task.

Figure 5.10 Upgrade from Disk (Firmware Update)Icon

Figure 5.11 shows the dialog for Download Firmware from Disk. The window displays the current version of the firmware on the switch and provides the option to download either Kernel firmware or AP firmware to the switch. The users can choose a new and valid firmware (.dld extension)from the local PC and then clicking on the **Upgrade** button to perform the update.

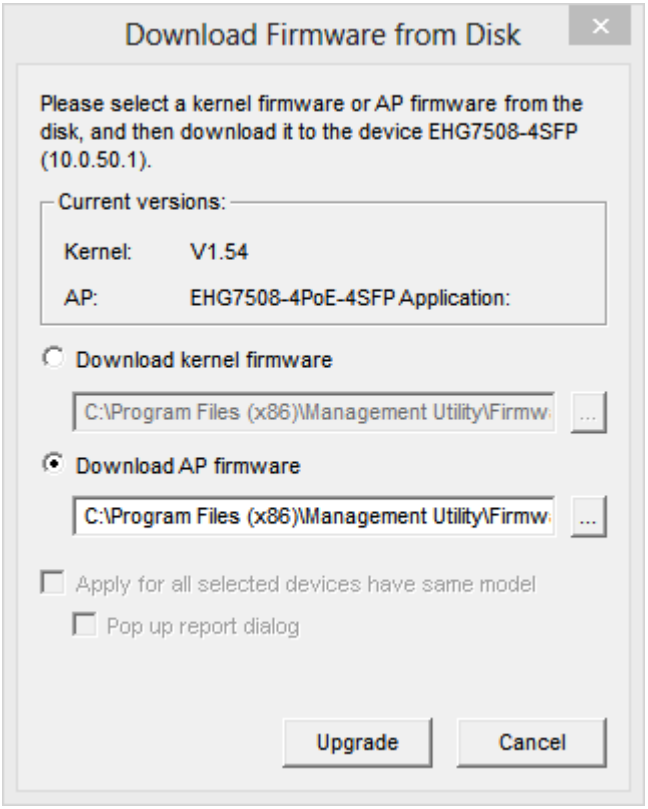


Figure 5.11 Dialog Window for Download Firmware from Disk

6 Glossary

Term	Description
802.1	A working group of IEEE standards dealing with Local Area Network.
802.1p	Provide mechanism for implementing Quality of Service (QoS)at the Media Access Control Level (MAC).
802.1x	IEEE standard for port- xbased Network-Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN
Broadcast	Broadcastpackets to all stations of a local network.
Client	Device that use services provided by other participants in the network.
DES	Data Encryption Standard is a block cipher that uses shared secret encryption. It's based on a symmetric-key algorithm that uses a 56-bit key.
DHCP	Dynamic Host Configuration Protocol allows a computer to be configured automatically, eliminating the need for intervention by a network administrator.It also prevents two computers from being configured with the same IP address automatically.There are two versions of DHCP; one for IPv4 and one for IPv6.
DNS	Domain Name System is a hierarchical naming system built for any computers or resources connected to the Internet. It maps domain names into the numerical identifiers. For example, the domain name www.google.com is translatedinto the address 74.125.153.104.
EAP	Extensible Authentication Protocol is an authentication framework widely used by IEEE.
Ethernet	In star-formed physical transport medium, all stations can send data simultaneously.Collisions are detected and corrected through network protocols.
Gateway	Provide access to other network components on the OSI layer model. Packets which are not going to a local partner are sent to the gateway. The gateway takes care of communication with the remote network.
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol is used on IPv4 networks for establishing multicast group memberships.
IP	Internet Protocol
IPv4	Internet Protocol version 4 is the fourth revision of the Internet Protocol. Together with IPv6, it is the core of internet network.It uses 32-bit addresses, which means there are only 2^32 possible unique addresses. Because of this limitation, an IPv4 addresses became scarce resource.This has stimulated the development of IPv6, which is still in its early stage of development.
LAN	Local Area Network is the network that connects devices in a limited geographical area such as company or computer lab.
MAC	Media Access Control is a sub-layer of the Data Link Layer specified in the OSI model. It provides addressing and channel access control mechanisms to allow network nodes to communicate within a LAN.

MAC Address	A unique identifier assigned to network interfaces for communications on a network segment. It is formed according to the rules of numbering name space managed by IEEE.
MD5	Message-Digest algorithm 5 is a widely used cryptographic which has a function with a 128-bit hash value.
Multicast	This type of transmission sends messages from one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. Also, networks that support multicast send only one copy of the information across the network until the delivery path that reaches group members diverges. At these diverges points, multicast packets will be copied and forwarded. This method can manage high volume of traffic with different destinations while using network bandwidth efficiently.
OSI Model	**O**pen **S**ystem **I**nterconnection mode is a way of sub-dividing a communication system into smaller parts called layers. A layer is a collection of conceptually similar functions that provide services to the layer above it and receives services from the layer below it.
QoS	Quality of Service
RADIUS	**R**emote **A**uthentication **D**ial **I**n **U**ser **S**ervice is an authentication and monitoring protocol on the application level for authentication, integrity protection and accounting for network access.
Server	Devices that provide services over the network.
SMTP	**S**imple **M**ail **T**ransfer **P**rotocol(**SMTP**) is an internet standard for email transmission across IP network.
SNMP	**S**imple **N**etwork **M**anagement **P**rotocol 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.

7 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 EH7510” 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 ='7' Word 9 Hi byte ='5' Word 9 Lo byte ='1' Word 10 Hi byte ='0' 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
0x0102 (258)	1 word	W	Clear All Warning Events 0x0001:Do clear action
Warning Events Information			
0x0200 (512)	64 words	R	1st Warning Event Information
0x0300 (768)	64 words	R	2st Warning Event Information
0x0400 (1024)	64 words	R	3st Warning Event Information
0x0500 (1280)	64 words	R	4st Warning Event Information
0x0600 (1536)	64 words	R	5st Warning Event Information
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
0x1200(4608)	20 words	R	Port TX rate Ex.Port 1 runs at TX Rate(1024 Kbps = 0x400). Word 0 of Port 1 =0x0000 Word 1 of Port 1 =0x0400 Word 0,1 =Port 1 TX Rate Word 2,3 =Port 2 TX Rate Word 4,5 =Port 3 TX Rate Word 6,7 =Port 4 TX Rate Word 8,9 =Port 5 TX Rate Word 10,11 =Port 6 TX Rate Word 12,13 =Port 7 TX Rate Word 14,15 =Port 8 TX Rate

			Word 16,17 =Port 9 TX Rate Word 18,19 =Port 10 TX Rate
0x1280 (4736)	20 words	R	Port RX rate Ex. Port 1 runs at RX Rate(1024 Kbps =0x400). Word 0 of Port 1 =0x0000 Word 1 of Port 1 = 0x0400 Word 0,1 =Port 1 RX Rate Word 2,3 =Port 2 RX Rate Word 4,5 =Port 3 RX Rate Word 6,7 =Port 4 RX Rate Word 8,9 =Port 5 RX Rate Word 10,11 =Port 6 RX Rate Word 12,13 =Port 7 RX Rate Word 14,15 =Port 8 RX Rate Word 16,17 =Port 9 RX Rate Word 18,19 = Port 10 RX Rate
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
Redundancy Information			
0x2000 (8192)	1 word	R	Redundancy Protocol 0x0000:None 0x0001:STP 0x0002:RSTP 0x0004:ERPS 0x0008:iA-Ring 0x0010:Compatible-Ring
0x2100 (8448)	1 word	R	STP Root 0x0000:Not Root 0x0001:Root 0xFFFF:RSTP not enable
0x2101 (8449)	5 words	R	STP Port Status 0x00: Disabled 0x01: Listening 0x02: Learning 0x03: Forwarding 0x04: Blocking 0x05: Discarding 0xFF: RSTP Not Enable 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
0x2200 (8704)	5 words	R	ERPS R-APS VLAN ID of the ring Ex: 3st VLAN ID =1, Word 2 =0x0001 1~4094:ID Value range 0x0000:VLAN ID Not Setup Word 0 =1st VLAN ID Word 1 =2st VLAN ID Word 2 =3st VLAN ID Word 3 =4st VLAN ID Word 4 =5st VLAN ID
0x2230 (8752)	5 words	R	ERPS West Port Ex:3st West Port =Port 2, Word 2 =0x0002 0x0001:Port 1 0x0002:Port 2 ... 0x000A:Port 10 0x000C:Trk1 0x000D:Trk2 0x000E: Trk3 0x000F:Virtual Channel 0x00FF:VLAN ID exist but no West Port be Selected 0xFFFF:ERPS Not Enable Word 0 =1st VLAN ID West Port Word 1 =2st VLAN ID West Port Word 2 =3st VLAN ID West Port Word 3 =4st VLAN ID West Port Word 4 =5st VLAN ID West Port
0x2240 (8768)	5 words	R	ERPS East Port Ex:3st West Port =Port 3, Word 2 =0x0003 0x0001: Port 1 0x0002: Port 2 ... 0x000A:Port 10 0x000C:Trk1 0x000D: Trk2 0x000E: Trk3 0x000F:Virtual Channel 0x00FF: VLAN ID exist but no East Port be Selected 0xFFFF: ERPS Not Enable Word 0 =1st VLAN ID East Port Word 1 =2st VLAN ID East Port Word 2 =3st VLAN ID East Port Word 3 =4st VLAN ID East Port Word 4 =5st VLAN ID East Port
0x2250 (8784)	5 words	R	ERPS West Port Status Ex:3st West Port Status = Forwarding, Word 2 = 0x0001 0x0001:Forwarding 0x0002:Blocking 0x0003:Signal Fail Blocking 0x000F:Virtual Channel 0x00FF:VLAN ID exist but no West Port be Selected 0xFFFF:ERPS Not Enable Word 0 =1st VLAN ID West Port Status

			Word 1 =2st VLAN ID West Port Status Word 2 =3st VLAN ID West Port Status Word 3 =4st VLAN ID West Port Status Word 4 =5st VLAN ID West Port Status
0x2260 (8800)	5 words	R	ERPS East Port Status Ex:3st East Port Status =Blocking, Word 2 =0x0002 0x0001:Forwarding 0x0002:Blocking 0x0003:Signal Fail Blocking 0x000F:Virtual Channel 0x00FF:VLAN ID exist but no Eest Port be Selected 0xFFFF:ERPS Not Enable Word 0 =1st VLAN ID East Port Status Word 1 =2st VLAN ID East Port Status Word 2 =3st VLAN ID East Port Status Word 3 =4st VLAN ID East Port Status Word 4 =5st VLAN ID East Port Status
0x2270 (8816)	5 words	R	ERPS Node State Ex: 3st Node State = Protection, Word 2 =0x0002 0x0001: None 0x0002: Idle 0x0003: Protection 0xFFFF: ERPS Not Enable Word 0 = 1st VLAN ID Node State Word 1 = 2st VLAN ID Node State Word 2 = 3st VLAN ID Node State Word 3 = 4st VLAN ID Node State Word 4 = 5st VLAN ID Node State
0x2280 (8832)	5 word	R	ERPS RPL Owner 0x0000: Disabled 0x0001: Enabled
0x2300 (8960)	1 word	R	iA-Ring Master Status 0x0000: Disabled 0x0001: Enabled 0xFFFF: iA-Ring not enable
0x2301 (8961)	1 word	R	1st Ring Port Ex: 1st Ring Port = Port 2, Word 0 = 0x0002 0x0001:Port 1 0x0002 :Port 2 … 0x000A:Port 10 0xFFFF:iA-Ring not enable
0x2302 (8962)	1 word	R	2st Ring Port Ex: 2st Ring Port =Port 3, Word 0 =0x0003 0x0001: Port 1 0x0002: Port 2 … 0x000A: Port 10 0xFFFF: iA-Ring not enable

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