iGS950 Series

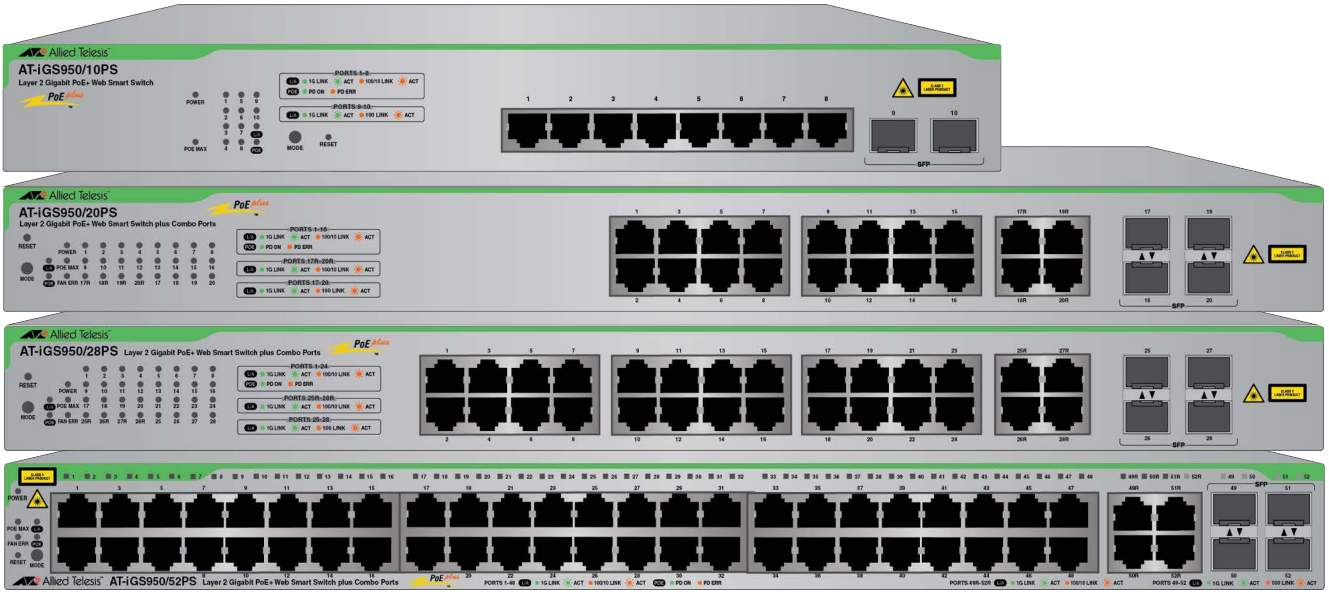
Layer 2 Gigabit Ethernet PoE+ WebSmart Switches

AT-iGS950/10PS

AT-iGS950/20PS

AT-iGS950/28PS

AT-iGS950/52PS



Web Browser User Guide

613-003432 Rev. B

Contents

Preface **23**
Document Conventions 24
Translated Safety Statements 25

Section I
Getting Started **27**

Chapter 1: Overview 29
Front and Rear Panels on the iGS950 Series 30
Hardware Features 34
Copper Ports 35
Power over Ethernet PoE+ 36
PoE+ Ports 36
Maximum PoE+ Power Budget 37
PoE+ Standards 37
Powered Device Classes 37
Mode A Power Delivery 38
PoE+ Port Priorities 38
Combo Copper Ports 40
Copper Cable Requirements 41
SFP Ports 42
LEDs 43
POWER LED 43
FAN ERR LED 43
POE MAX LED 44
Copper Port LEDs and the MODE Button 45
SFP LEDs 48
RESET Button 50
Power Supply and Fans 51
Power Supply 51
Ventilation Fans 51
Management Interfaces 52

Chapter 2: Starting a Web Browser Management Session 53
Starting a Web Browser Management Session 54
Ending a Web Browser Management Session 56
Menus 57
Dashboard View 59
CPU & Memory Utilization 59
System Information 60
Switch Information 60
Network Information 61
Switch View 62
Saving Your Changes 63
Unsupported Special Characters 65

Section II
System Menu **67**

Chapter 3: System Name, Location, and Administrator 69
Procedure 69

Chapter 4: Management IPv4 Addresses 71
IPv4 Address Overview 72
Assigning IPv4 Addresses to the VLANs on the Switch 73
Setting the ARP Aging Time 75
Managing Static IPv4 ARP Entries 76
Managing IPv4 Static/Default Route Addresses 78
Managing DNS Server IPv4 and IPv6 Addresses 80

Chapter 5: Management IPv6 Addresses 81
IPv6 Address Overview 82
Managing Static and Dynamic IPv6 Addresses 83
Setting the IPv6 Neighbor Settings 87
Assigning Static IPv6 Addresses 89

Chapter 6: System Time 91
Manually Setting the Date and Time 92
Setting the Date and Time from an SNTP Server 95

Chapter 7: Web Browser Management 97
Selecting the Web Browser Mode 98
Managing Web Browser Manager Accounts 100
Setting the Timeout for Management Sessions 102

Chapter 8: Secure Shell and Telnet Servers 103
Introduction 104
Enabling or Disabling the SSH Server 105
Configuring the Telnet Server 106

Chapter 9: DHCP Auto Configuration 107
Description and Procedure 107

Chapter 10: DHCP IPv4 Relay 109
DHCP IPv4 Relay Global Settings 110
DHCP IPv4 Relay Interface Settings 114
Adding IPv4 Addresses of DHCP Servers 114
Editing IPv4 Addresses of DHCP Servers 115
Deleting IPv4 Addresses of DHCP Servers 115

Chapter 11: DHCP IPv6 Relay 117
DHCP IPv6 Relay Global Settings 118
DHCP IPv6 Relay Interface Settings 121
Adding IPv6 Addresses of DHCP Servers 121
Editing IPv6 Addresses of DHCP Servers 122
Deleting IPv6 Addresses of DHCP Servers 122

Chapter 12: DHCP Server 123
Overview 124
Configuring Global Settings 125
Configuring DHCP IPv4 Pools 127
Configuring DHCP Server Pool Options 129
Configuring DHCP Server Hosts 131
Displaying the DHCP Server Assigned Host Table 133

Chapter 13: System Log and Syslog Client 135
Viewing the Event System Log 136
Sending System Log Events to a Syslog Server 138

Chapter 14: SNMPv1 and v2c 141
Enabling or Disabling SNMP Management 142
Changing the SNMP Engine ID 143
SNMPv1 and v2c View Names 144
Adding SNMPv1, v2c View Names 144
Modifying SNMPv1, v2c View Names 145
Deleting SNMPv1, v2c View Names 145

SNMPv1 and SNMPv2c User and Group Names....146
Adding User and Group Names....146
Modifying User and Group Names....147
Deleting User and Group Names....147
SNMP Community Strings....148
Adding SNMP Community Strings....148
Modifying SNMP Community Strings....149
Deleting SNMP Community Strings....149
SNMP Traps....150
Adding Trap Host Table Entries....150
Modifying Trap Host Table Entries....152
Deleting Trap Host Table Entries....152

Chapter 15: SNMPv3 153
SNMPv3 Overview....154
SNMPv3 Authentication Protocols....154
SNMPv3 Privacy Protocol....155
SNMPv3 MIB Views....155
SNMPv3 Configuration Process....156
SNMPv3 User and Group Names....158
Adding SNMPv3 User and Group Names....158
Modifying SNMPv3 User and Group Names....159
Deleting SNMPv3 User and Group Names....159
SNMPv3 View Names....160
Adding SNMPv3 View Names....160
Modifying SNMPv3 View Names....162
Deleting SNMPv3 View Names....162
SNMPv3 View Table....163
Adding SNMPv3 View Table Entries....163
Modifying SNMPv3 View Table Entries....164
Deleting SNMPv3 View Table Entries....164
SNMPv3 Traps....165
SNMP Engine ID....166

Chapter 16: RMON 167
RMON Overview....168
Enabling and Disabling RMON....169
RMON Port Statistics Groups....170
Adding RMON Port Statistics Groups....170
Modifying or Deleting RMON Port Statistics Groups....171
RMON Histories....172
Adding RMON History Groups....172
Modifying or Deleting RMON History Groups....174
RMON Events....175
Adding Events....175
Modifying or Deleting Events....177
RMON Alarms....179
Adding RMON Alarms....180
Modifying or Deleting Alarms....182

Chapter 17: Traffic Statistics and Charts 183
Network Statistics Overview....184
Displaying Traffic Statistics....185
Displaying Port Error Statistics....186

Chapter 18: Managing IEEE 187
Description and Procedure....187

Section III

Network Menu **189**

Chapter 19: Basic Port Settings 191
Description and Procedure 191

Chapter 20: Spanning Tree and Rapid Spanning Tree Protocols 197
STP and RSTP Overview 198
Bridge Priority and the Root Bridge 198
Forwarding Delay and Topology Changes 201
Mixed STP and RSTP Networks 203
Spanning Tree and VLANs 204
Configuring STP and RSTP Global Settings 206
Configuring STP and RSTP Port Settings 210
Configuring Topology Change Protection 214

Chapter 21: Multiple Spanning Tree Protocol Overview 217
Overview 218
Multiple Spanning Tree Instance (MSTI) 219
VLAN and MSTI Associations 219
Ports in Multiple MSTIs 219
Multiple Spanning Tree Regions 221
Region Guidelines 223
Common and Internal Spanning Tree (CIST) 224
MSTP with STP and RSTP 225
Summary of Guidelines 226
Associating VLANs to MSTIs 228
Connecting VLANs Across Different Regions 230

Chapter 22: Multiple Spanning Tree Protocol 233
Configuring MSTP Global Settings 234
Configuring MSTP Port Settings 238
Configuring MST and MSTI Settings 242
Configuring MST Port Settings 244
Displaying MST Instance Information 247

Chapter 23: Static Port Trunks 249
Static Port Trunk Overview 250
Guidelines 250
Adding Static Port Trunks 252
Modifying Static Port Trunks 254
Deleting Static Port Trunks 256

Chapter 24: LACP Trunks 257
LACP Port Trunk Overview 258
System Priority and ID Numbers 258
Port Priority Value 259
General Guidelines 260
Displaying LACP Group Status 261
Adding LACP Trunks 262
Setting LACP Port Priorities 264
Modifying LACP Trunks 265
Deleting LACP Trunks 267

Chapter 25: Port Mirroring 269
Port Mirroring Overview 270
Enabling Port Mirroring 271
Disabling Port Mirroring 273

Chapter 26: Loopback Detection 275
Configuring Loopback Detection 276
Disabling Loopback Detection 279

Chapter 27: Static Unicast MAC Addresses 281
Static MAC Addresses Overview 282
Adding Static Unicast MAC Addresses 284
Modifying Static Unicast MAC Addresses 286
Deleting Static Unicast MAC Addresses 287

Chapter 28: Static Multicast MAC Addresses 289
Adding Static Multicast MAC Addresses 290
Modifying Static Multicast MAC Addresses 292
Deleting Static Multicast Addresses 293

Chapter 29: IGMP Snooping 295
IGMP Snooping Overview 296
Configuring IGMP Snooping 298
Adding or Deleting Static Multicast Router Ports 302

Chapter 30: MLD Snooping 305
MLD Snooping Overview 306
Configuring MLD Snooping 307
Adding or Deleting Static Multicast Router Ports 311

Chapter 31: Multicast VLANs 313
Introduction 314
Managing Multicast VLANs 315
Adding Multicast VLANs 315
Editing Multicast VLANs 317
Deleting Multicast VLANs 319
Viewing Multicast VLANs 320
Managing Multicast Address Profiles 322
Adding Multicast Address Profiles 322
Editing Multicast Profiles 323
Deleting Multicast Profiles 324
Managing Associations of Multicast VLANs with Multicast Address Profiles 325
Adding Associations 325
Deleting Associations 326

Chapter 32: Multicast Filtering 327
Description and Procedure 327

Chapter 33: Bandwidth Control 329
Setting Threshold Limits for Ingress Unknown Unicast, Broadcast, and Multicast Packets 330
Setting Ingress Bandwidth Limits 332
Setting Egress Traffic Rate Limits 334

Chapter 34: 802.1Q Tagged Virtual LANs 337
802.1Q Tagged VLAN Overview 338
Tagged Ports 338
Untagged Ports 339
802.1Q Tagged VLAN Components 339
Guidelines to Adding Tagged VLANs 341
Tagged VLAN Example 342
Adding or Viewing 802.1Q Tagged VLANs 344
Configuring PVIDs and Filters for Tagged and Untagged Ports 348
Modifying 802.1Q Tagged VLANs 350
Deleting 802.1Q Tagged VLANs 351
Viewing All 802.1Q Tagged VLANs 352

Chapter 35: Private Virtual LAN 353
Private VLAN Overview 354
Source Port 354
Forwarding Ports 354
Configuring the Private VLAN 355
Disabling the Private VLAN 357

Chapter 36: VLAN Forwarding Modes 359
Description and Procedure 359

Chapter 37: GARP VLAN Registration Protocol 361
GVRP Overview 362
Guidelines 364
GVRP and Network Security 364
GVRP-inactive Intermediate Switches 365
Enabling or Disabling GVRP 366
Configuring GVRP Port Settings 367
Configuring GVRP Time Settings 369

Chapter 38: Voice VLAN 371
Voice VLAN Overview 372
802.1Q VLAN 372
Organization Unique Identifier (OUI) 372
CoS with Voice VLAN 372
Dynamic Port Auto-Detection 373
General Guidelines 374
Configuring the Voice VLAN 375
Managing the OUI Table 378

Chapter 39: Link Layer Discovery Protocol 381
LLDP Overview 382
Configuring LLDP 383
Basic TLVs Settings Table 386
Dot1 TLVs Settings Table 387
Dot3 TLVs Settings Table 389
MED Port TLV Settings 391
Statistics Information 392
LLDP Local Port Information 394
Displaying Neighbor Information 395

Chapter 40: MAC VLANs 397
Description and Procedure 397
Managing MAC VLANs 398

Chapter 41: Protocol VLANs 401
Introduction 401
Managing Protocol VLAN Profiles 402
Managing VLAN Profile Interfaces 404

Section IV
Quality of Service Menu **407**

Chapter 42: Quality of Service and Class of Service 409
QOS and COS Overview 410
Packet Priority 410
Egress Queue vs Packet Priority Mapping 411
Prioritizing Untagged Packets 412
Scheduling Algorithm 412
Mapping CoS Priorities to Egress Queues 414
Mapping CoS Priorities to Ports 416
Mapping DSCP Classes to Egress Queues 417
Setting the Queue Scheduling Algorithm 418
Mapping IPv6 Traffic Classes to Port Egress Queues 419

Section V
PoE Menu 421

Chapter 43: Power over Ethernet 423
Overview 424
PoE+ Ports 424
Maximum PoE+ Power Budget 425
PoE+ Standards 425
Powered Device Classes 425
Mode A Power Delivery 426
PoE Port Priorities 426
Managing PoE 428
Managing Time Range Power Schedules 430
Adding a Power Schedule 430
Editing a Power Schedule 432
Deleting a Power Schedule 432

Section VI
Security 433

Chapter 44: Port Security 435
Port Security Overview 436
Configuring the Global Setting for the Maximum Number of MAC Addresses 437
Configuring Port Security 438
Configuring Port and VLAN Security 441

Chapter 45: Port Authentication 443
Overview 444
Authentication Devices 445
Authentication Methods 446
802.1x Port-based Network Access Control 446
MAC Address-based Authentication 446
Authenticator Port Operational Settings 447
Authenticator Port Operating Modes 448
Single Host Mode 448
Single Host Mode with Piggy Backing 448
Multiple Host Mode 450
Supplicant and VLAN Associations 451
Single Host Mode 452
Multiple Host Mode 452
Multiple Supplicant Mode 452
Supplicant VLAN Attributes on RADIUS Servers 452
Guest VLAN 453
RADIUS Accounting 454
General Steps 455
Guidelines 456
Configuring Port Access Control 458

Chapter 46: Local Dial-in User Accounts 465
Local Dial-in User Authentication Overview 466
Adding Local Dial-in User Accounts 467
Modifying or Deleting Local Dial-in User Accounts 469

Chapter 47: RADIUS Client 471
RADIUS Client Overview 472
Managing Server IP Addresses in the RADIUS Client 473

Chapter 48: TACACS+ Client 477
TACACS+ Client Overview 478
Managing Server IP Addresses in the TACACS+ Client 479

Chapter 49: Destination MAC Address Filters 483
Destination MAC Address Filters Overview 484
Managing Destination MAC Address Filters 485

Chapter 50: Denial of Service 487
Configuring Denial of Service Protection 488

Chapter 51: DHCP Snooping 491
DHCP Snooping Overview 492
Trusted Ports 492
Untrusted Ports 492
Unauthorized DHCP Servers 492
DHCP with Option 82 493
Option 82 Pass Through 494
General Guidelines 497
Configuring DHCP Snooping 498
Adding DHCP Snooping to VLANs 501
Designating Trusted and Untrusted Ports 503
Managing the Binding Database 504

Chapter 52: Traffic Rules and Policies 507
Traffic Rules and Policies Overview 508
Policy Filters 508
Actions 508
How Ingress Packets are Compared Against Policies 509
Guidelines 509
Adding IP Rules 511
Adding L2 Rules 514
Editing, Modifying or Deleting Policies 516
Finding Policies 517

Section VII
Tools Menu 519

Chapter 53: Switch Firmware 521
Management Software Overview 522
Upgrading the Management Software with HTTP 523
Backing Up the Management Software with HTTP 525
Upgrading the Management Software with TFTP 526
Backing Up the Management Software with TFTP 528
Designating the Boot Management Software 529

Chapter 54: Configuration Files 531
Overview to Switch Configuration Files 532
Designating the Active Configuration File 533
Backing Up Configuration Files from the Switch with HTTP 535
Restoring Configuration Files to the Switch with HTTP 536
Backing Up Configuration Files from the Switch with TFTP 537
Restoring Configuration Files to the Switch with TFTP 538

Chapter 55: Troubleshooting Tools 539
Cable Diagnostics 540
Rebooting the Switch 541
Restoring the Factory Default Values 543
Pinging Network Devices 544

Figures

Chapter 1: Overview **29**
Figure 1: Front and Rear Panels on the AT-iGS950/10PS Switch 30
Figure 2: Front and Rear Panels on the AT-iGS950/20PS Switch 31
Figure 3: Front and Rear Panels on the AT-iGS950/28PS Switch 32
Figure 4: Front and Rear Panels on the AT-iGS950/52PS Switch 33
Figure 5: POWER LED 43
Figure 6: FAN ERR LED 44
Figure 7: POE MAX LED 44
Figure 8: Copper Port LEDs on the AT-iGS950/20PS Switch 45
Figure 9: Copper Port LEDs on the AT-iGS950/52PS Switch 46
Figure 10: MODE Button with L/A and POE LEDs 46
Figure 11: LEDs for SFP Ports 9 and 10 on the AT-iGS950/10PS Switch 48
Figure 12: Link/Activity (L/A) LEDs for SFP Ports 49
Figure 13: RESET Button 50
Figure 14: Ventilation Airflow of Switches with Fans 51

Chapter 2: Starting a Web Browser Management Session **53**
Figure 15: Login Window 55
Figure 16: Logout Icon 56
Figure 17: Main Menu 57
Figure 18: Security Menu Options 58
Figure 19: Example of a Sub-menu 58
Figure 20: Dashboard View 59
Figure 21: Save Settings to Flash Window 63

Chapter 3: System Name, Location, and Administrator **69**
Figure 22: Management Window 70

Chapter 4: Management IPv4 Addresses **71**
Figure 23: IPv4 Interface Window 73
Figure 24: IPv4 Interface Configuration Window 74
Figure 25: ARP Aging Time Window 75
Figure 26: Static ARP Window 77
Figure 27: IPv4 Static/Default Route Window 79
Figure 28: DNS Server Settings Window 80

Chapter 5: Management IPv6 Addresses **81**
Figure 29: IPv6 Interface Window 85
Figure 30: IPv6 Interface Configuration Window 86
Figure 31: IPv6 Neighbor Settings Window 88
Figure 32: IPv6 System Settings Window 90

Chapter 6: System Time **91**
Figure 33: System Time Window 94

Chapter 7: Web Browser Management **97**
Figure 34: SSL Settings 99
Figure 35: Administration Window 101
Figure 36: Modify Administration Window 101

Figure 37: Timeout Settings Window 102

Chapter 8: Secure Shell and Telnet Servers 103
Figure 38: SSH Settings Window 105
Figure 39: Telnet Settings Window 106

Chapter 9: DHCP Auto Configuration 107
Figure 40: DHCP Auto Configuration Window 108

Chapter 10: DHCP IPv4 Relay 109
Figure 41: DHCP IPv4 Relay Global Settings Window 113
Figure 42: DHCP IPv4 Relay Interface Settings 114

Chapter 11: DHCP IPv6 Relay 117
Figure 43: DHCP IPv6 Relay Global Settings 120
Figure 44: DHCP IPv6 Relay Interface Settings 121

Chapter 12: DHCP Server 123
Figure 45: DHCP Server Global Settings 126
Figure 46: DHCP Server Pool Settings 128
Figure 47: DHCP Server Pool Option Settings Window 130
Figure 48: DHCP Server Host Settings 132
Figure 49: DHCP Server Assigned Host Table 133

Chapter 13: System Log and Syslog Client 135
Figure 50: System Log Settings Window 137

Chapter 14: SNMPv1 and v2c 141
Figure 51: SNMP Engine ID Settings Window 142
Figure 52: SNMP Group Access Table Window 145
Figure 53: SNMP User/Group Window 147
Figure 54: SNMP Community Table Window 149
Figure 55: Trap Management Window 152

Chapter 15: SNMPv3 153
Figure 56: MIB Tree 155
Figure 57: SNMPv3 Table Relationships 157
Figure 58: SNMP Group Access Table Window 160
Figure 59: SNMP View Table Window 163

Chapter 16: RMON 167
Figure 60: RMON Basic Settings Window 169
Figure 61: Ethernet Statistics Settings Window 171
Figure 62: History Control Settings Window 174
Figure 63: RMON Event Settings Window 177
Figure 64: RMON Alarm Settings Window 182

Chapter 17: Traffic Statistics and Charts 183
Figure 65: Statisticcs Traffic Information Window 185
Figure 66: Statistics Error Information Window 186

Chapter 18: Managing IEEE 187
Figure 67: IEEE Window 187

Chapter 19: Basic Port Settings 191
Figure 68: Physical Interface Window 192

Chapter 20: Spanning Tree and Rapid Spanning Tree Protocols 197
Figure 69: Point-to-Point Ports 203
Figure 70: Edge Port 203

Figure 71: STP and VLAN Fragmentation with Untagged Ports....204
Figure 72: STP and VLAN Fragmentation....205
Figure 73: STP and VLAN Compatibility with Tagged Ports....205
Figure 74: Spanning Tree Protocol Settings Window....209
Figure 75: Port Settings Window....213
Figure 76: Spanning Tree Protocol TC Protect....215

Chapter 21: Multiple Spanning Tree Protocol Overview....217
Figure 77: Multiple Spanning Tree Region....222
Figure 78: CIST and VLAN Guideline - Example 1....228
Figure 79: CIST and VLAN Guideline - Example 2....229
Figure 80: Spanning Regions....230

Chapter 22: Multiple Spanning Tree Protocol....233
Figure 81: MST Settings Window....243
Figure 82: MST Port Settings Window....246
Figure 83: Instance Information Window....247

Chapter 23: Static Port Trunks....249
Figure 84: Static Port Trunk Example....250
Figure 85: Trunking Window....253

Chapter 24: LACP Trunks....257
Figure 86: LACP Group Status Window....261
Figure 87: Port Priority Window....264

Chapter 25: Port Mirroring....269
Figure 88: Mirroring Window....271

Chapter 26: Loopback Detection....275
Figure 89: Loopback Detection Window....278

Chapter 27: Static Unicast MAC Addresses....281
Figure 90: Static Unicast Address Table Window....285

Chapter 28: Static Multicast MAC Addresses....289
Figure 91: Static Multicast Address Table Window....291

Chapter 29: IGMP Snooping....295
Figure 92: IGMP Snooping Settings Window....301
Figure 93: IGMP Snooping Router Port Window....303
Figure 94: Modify IGS Static Router Port Window....303

Chapter 30: MLD Snooping....305
Figure 95: MLD Snooping Settings Window....310
Figure 96: MLD Snooping Router Port Window....312
Figure 97: Modify IGS Static Router Port Window....312

Chapter 31: Multicast VLANs....313
Figure 98: Multicast Global Settings Window....317
Figure 99: Multicast VLAN Table Window....320
Figure 100: Multicast Group Setup Window....323
Figure 101: Multicast Associate Group Setup Window....325

Chapter 32: Multicast Filtering....327
Figure 102: Multicast Filtering Window....328

Chapter 33: Bandwidth Control....329
Figure 103: Storm Control Window....331
Figure 104: Ingress Rate Limiting Window....333

Figure 105: Egress Rate Limiting Window....335

Chapter 34: 802.1Q Tagged Virtual LANs 337
Figure 106: Example of a Tagged VLAN....342
Figure 107: Tagged VLAN Window....347
Figure 108: Port Settings Window....349
Figure 109: VLAN Current Database Window....352

Chapter 35: Private Virtual LAN 353
Figure 110: Private VLAN Window....356

Chapter 36: VLAN Forwarding Modes 359
Figure 111: Forwarding Table Mode Window....360

Chapter 37: GARP VLAN Registration Protocol 361
Figure 112: GVRP Example....363
Figure 113: GVRP Global Settings Window....366
Figure 114: GVRP Port Settings Window....368
Figure 115: GVRP Time Settings Window....370

Chapter 38: Voice VLAN 371
Figure 116: Voice VLAN Settings Window....377
Figure 117: Voice VLAN OUI Settings Window....379

Chapter 39: Link Layer Discovery Protocol 381
Figure 118: Basic TLVs Setting Table....386
Figure 119: Dot1 TLVs Setting Table....387
Figure 120: Dot3 TLVs Setting Table....390
Figure 121: MED Port Settings....391
Figure 122: LLDP Statistics Information Table....393
Figure 123: LLDP Local Port Information....394
Figure 124: LLDP Neighbors Information Window....395

Chapter 40: MAC VLANs 397
Figure 125: MAC VLAN Window....399

Chapter 41: Protocol VLANs 401
Figure 126: Protocol VLAN Profile....402
Figure 127: Protocol VLAN Profile Interface....404

Chapter 42: Quality of Service and Class of Service 409
Figure 128: CoS Window....415
Figure 129: Port Priority Window....416
Figure 130: DSCP Class Mapping Window....417
Figure 131: Scheduling Algorithm Window....418
Figure 132: IPv6 Traffic Class Priority Settings Window....420

Chapter 43: Power over Ethernet 423
Figure 133: Power Over Ethernet Window....429
Figure 134: Time Range Window....432

Chapter 44: Port Security 435
Figure 135: Port Security Global Settings Window....437
Figure 136: Port Security Port Settings Window....440
Figure 137: Port Security Address Settings Window....442

Chapter 45: Port Authentication 443
Figure 138: Single Host Mode....448
Figure 139: Multiple Host Operating Mode....449
Figure 140: Multiple Supplicant Mode....450

Figure 141: Port Access Control Settings Window 459
Figure 142: Port Access Control Settings Window - Port Settings 459

Chapter 46: Local Dial-in User Accounts 465
Figure 143: Dial-In User Window 468

Chapter 47: RADIUS Client 471
Figure 144: RADIUS Window 475

Chapter 48: TACACS+ Client 477
Figure 145: TACACS+ Window 481

Chapter 49: Destination MAC Address Filters 483
Figure 146: Destination MAC Filter Window 485

Chapter 50: Denial of Service 487
Figure 147: Denial of Service Window 489

Chapter 51: DHCP Snooping 491
Figure 148: DHCP with Option 82 494
Figure 149: DHCP with Option 82 Pass Through Disabled 495
Figure 150: DHCP with Option 82 Pass Through Enabled 496
Figure 151: DHCP Snooping General Settings Window 500
Figure 152: DHCP Snooping VLAN Settings Window 502
Figure 153: DHCP Snooping Trusted Interfaces Window 503
Figure 154: DHCP Snooping Binding Database Window 506

Chapter 52: Traffic Rules and Policies 507
Figure 155: ACL Configuration Wizard Window 513
Figure 156: ACL Finder Window 517

Chapter 53: Switch Firmware 521
Figure 157: Firmware Upgrade Via HTTP Settings Window 524
Figure 158: Firmware Upgrade via TFTP Settings Window 527

Chapter 54: Configuration Files 531
Figure 159: Backup/Restore Window 534

Chapter 55: Troubleshooting Tools 539
Figure 160: Cable Diagnostics Window 540
Figure 161: Factory Default Reset/Reboot Window 541
Figure 162: Ping Test Settings Window 545

Tables

Chapter 1. Overview **29**
Table 1: Hardware Features 34
Table 2: Hardware Features of the Copper Port 35
Table 3: PoE+ Ports 36
Table 4: PoE+ Maximum Power Budgets 37
Table 5: PoE Standards 37
Table 6: IEEE Powered Device Classes Supported by the iGS950 Series 37
Table 7: Combo Copper Port Numbers 40
Table 8: POWER LED 43
Table 9: FAN ERR LED 44
Table 10: POE MAX LED 45
Table 11: MODE Button L/A and POE LEDs 46
Table 12: Copper Port LEDs in Link/Activity (L/A) Mode 47
Table 13: Copper Port LEDs in PoE+ Mode 48
Table 14: Link/Activity LEDs for the SFP Ports 49

Chapter 2. Starting a Web Browser Management Session **53**
Table 15: System Information 60
Table 16: Switch Information 60
Table 17: Network Information 61

Chapter 3. System Name, Location, and Administrator **69**
Table 18: Management Window 69

Chapter 4. Management IPv4 Addresses **71**
Table 19: IPv4 Interface Configuration Window 74
Table 20: ARP Aging Time Window 75
Table 21: Static ARP Table 76
Table 22: Static ARP Window 77
Table 23: IPv4 Static/Default Route Window 78
Table 24: DNS Server Settings Window 80

Chapter 5. Management IPv6 Addresses **81**
Table 25: IPv6 Interface Configuration Window 83
Table 26: IPv6 Router Window 90

Chapter 6. System Time **91**
Table 27: System Time Window 92
Table 28: Setting the Calender and Clock from an NTP Server 95

Chapter 7. Web Browser Management **97**

Chapter 8. Secure Shell and Telnet Servers **103**
Table 29: SSH Settings Window 105
Table 30: Telnet Settings Window 106

Chapter 9. DHCP Auto Configuration **107**

Chapter 10. DHCP IPv4 Relay **109**
Table 31: DHCP IPv4 Relay Global Settings Window 110

Chapter 11. DHCP IPv6 Relay **117**
Table 32: DHCP IPv6 Relay Global Settings Window 118

Chapter 12. DHCP Server **123**
Table 33: DHCP Server Global Settings Window 125
Table 34: DHCP Server Pool Settings Window 127
Table 35: DHCP Server Pool Option Settings Window 129

Table 36: DHCP Server Host Settings Window 131
Table 37: DHCP Server Assigned Host Table Window 133

Chapter 13. System Log and Syslog Client 135
Table 38: System Log Settings Window - Syslog Client 139

Chapter 14. SNMPv1 and v2c 141
Table 39: SNMP Group Access Table Window for v1 and v2c 144
Table 40: SNMP User/Group Window for v1/v2c 146
Table 41: SNMP Community Table Window 148
Table 42: Trap Management Window 150

Chapter 15. SNMPv3 153
Table 43: SNMP User/Group Window for v3 158
Table 44: SNMP Group Access Table Window for v3 161
Table 45: SNMP View Table Window for v3 164

Chapter 16. RMON 167
Table 46: Ethernet Statistics Settings Window 170
Table 47: History Control Settings Window 172
Table 48: RMON Event Settings Window 175
Table 49: RMON Alarm Settings Window 180

Chapter 17. Traffic Statistics and Charts 183
Table 50: Port Traffic Statistics 185
Table 51: Error Statistics 186

Chapter 18. Managing IEEE 187

Chapter 19. Basic Port Settings 191
Table 52: Physical Interface (Port) Settings 192

Chapter 20. Spanning Tree and Rapid Spanning Tree Protocols 197
Table 53: Valid Port Priority Values 200
Table 54: Spanning Tree Protocol Settings Window for STP and RSTP 206
Table 55: STP and RSTP Port Settings Window 210
Table 56: Spanning Tree Protool TC Protect Window 214

Chapter 21. Multiple Spanning Tree Protocol Overview 217

Chapter 22. Multiple Spanning Tree Protocol 233
Table 57: Spanning Tree Protocol Settings Window for MSTP 234
Table 58: MSTP Port Settings 238
Table 59: MST Settings Window - MST Configuration Identification Settings 242
Table 60: MST Settings Window - MST Instance Settings 242
Table 61: MST Port Settings Window 244
Table 62: Instance Information Window 247

Chapter 23. Static Port Trunks 249

Chapter 24. LACP Trunks 257
Table 63: LACP Group Status Window 261

Chapter 25. Port Mirroring 269

Chapter 26. Loopback Detection 275
Table 64: Loopback Detection Window 276

Chapter 27. Static Unicast MAC Addresses 281
Table 65: Static Unicast Table 284

Chapter 28. Static Multicast MAC Addresses 289
Table 66: Static Multicast Address Table 291

Chapter 29. IGMP Snooping 295
Table 67: IGMP Snooping Settings Window 298
Table 68: Multicast Group Entries Table in the IGMP Snooping Settings Window 300
Table 69: IGMP Snooping Router Port Window 302

Chapter 30. MLD Snooping 305
Table 70: MLD Snooping Settings Window 307
Table 71: Multicast Group Entries Table in the MLD Snooping Settings Window 309
Table 72: MLD Snooping Router Port Window 311

Chapter 31. Multicast VLANs 313
Table 73: Multicast VLAN Table Window 320

Chapter 32. Multicast Filtering 327
Table 74: Multicast Filtering Window 327

Chapter 33. Bandwidth Control 329
Table 75: Storm Control Window 330
Table 76: Ingress Rate Limiting Window 332
Table 77: Egress Rate Limiting Window 334

Chapter 34. 802.1Q Tagged Virtual LANs 337
Table 78: Components of 802.1Q Tagged VLANs 339
Table 79: Example of Tagged VLANs 343
Table 80: Tagged VLAN Window 345
Table 81: Tagged VLAN Window Buttons 346
Table 82: Port Settings Window 348
Table 83: VLAN Current Database Window 352

Chapter 35. Private Virtual LAN 353
Table 84: Private VLAN Window 355

Chapter 36. VLAN Forwarding Modes 359

Chapter 37. GARP VLAN Registration Protocol 361
Table 85: GVRP Port Settings Window 367
Table 86: GVRP Time Settings Window 369

Chapter 38. Voice VLAN 371
Table 87: Voice VLAN Settings Window 375
Table 88: Voice VLAN OUI Settings Window 378

Chapter 39. Link Layer Discovery Protocol 381
Table 89: LLDP Global Settings 383
Table 90: Basic TLVs Settings Window 386
Table 91: Dot1 TLVs Setting Window 387
Table 92: Dot3 TLVs Settings Table Window 389
Table 93: MED Port TLV Settings Window 391
Table 94: LLDP Statistics Information Window 392
Table 95: LLDP Statistics Ports Window 392
Table 96: LLDP Local Port Information Window 394
Table 97: LLDP Neighbors Information Window 395

Chapter 40. MAC VLANs 397
Table 98: MAC VLAN Window 398

Chapter 41. Protocol VLANs 401
Table 99: Protocol VLAN Profile Window 403
Table 100: Protocol VLAN Profile Interface Window 405

Chapter 42. Quality of Service and Class of Service 409
Table 101: Default Mappings Priority Levels to Priority Queues 411
Table 102: Example of Customized Mappings Priority Levels to Priority Queues 411
Table 103: Weighted Round Robin Priority 413

Chapter 43. Power over Ethernet 423
Table 104: PoE+ Ports 424
Table 105: PoE+ Maximum Power Budgets 425
Table 106: PoE Standards 425
Table 107: IEEE Powered Device Classes Supported by the iGS950 Series 425
Table 108: Power over Ethernet Settings 428
Table 109: Power over Ethernet Table 428
Table 110: Time Range Window 430

Chapter 44. Port Security 435
Table 111: Port Security Port Settings Window 438
Table 112: Port Security Address Settings Window 441

Chapter 45. Port Authentication 443
Table 113: Port Access Control Settings Window 458
Table 114: Port Access Control Settings Window - Advanced Settings 460

Chapter 46. Local Dial-in User Accounts 465
Table 115: Dial-In User Window 467

Chapter 47. RADIUS Client 471
Table 116: RADIUS Window 473

Chapter 48. TACACS+ Client 477
Table 117: TACACS+ Window 479

Chapter 49. Destination MAC Address Filters 483

Chapter 50. Denial of Service 487
Table 118: Denial of Service Filters 488

Chapter 51. DHCP Snooping 491
Table 119: DHCP Snooping General Settings Window 498
Table 120: DHCP Snooping Binding Database Window 504
Table 121: DHCP Snooping Binding Database Window 505

Chapter 52. Traffic Rules and Policies 507
Table 122: IP Rule Policy Window for IP Rules and MAC Addresses 511
Table 123: IP Rule Policy Window for L2 Rules and IP Addresses 514

Chapter 53. Switch Firmware 521

Chapter 54. Configuration Files 531

Chapter 55. Troubleshooting Tools 539
Table 124: Ping Test Settings Window 544
Table 125: Ping Test Results Window 545

Electrical Safety and Emissions Standards

This product meets the following standards.

U.S. Federal Communications Commission
Radiated Energy Note: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. Note: Modifications or changes not expressly approved of by the manufacturer or the FCC, can void your right to operate this equipment.

Industry Canada
This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Warning: In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Laser Safety IEC/EN 60825-1:2014 & IEC/EN 60825-2:2004/A2:2010

Note
For safety and regulatory compliance certificates, refer to the *iGS950 Series Installation Guide*.

Note
For electromagnetic certificates, refer to *the iGS950 Series Installation Guide*.

Preface

This guide contains instructions on how to monitor and manage the features of the iGS950 Series of Layer 2 Gigabit Ethernet PoE+ WebSmart Switches with their onboard web browser management interface. This preface contains the following sections:

- ❒ “Document Conventions” on page 24
- ❒ “Translated Safety Statements” on page 25

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

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

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

Warning
Laser warnings inform you that an eye or skin hazard exists due to the presence of a Class 1 laser device.

Translated Safety Statements

Important: Safety statements with ✍ symbols are translated in the PDF document **Translated Safety Statements** on the Allied Telesis website at **alliedtelesis.com/library/search**.

Übersetzte Sicherheitserklärungen:

Wichtig: Das ✍ zeigt an, dass Übersetzungen der Sicherheitserklärung in den PDF-**Translated Safety Statements** auf der Allied Telesis-Website unter **alliedtelesis.com/us/en/library/search** verfügbar sind.

Declaraciones de seguridad traducidas:

Importante: El ✍ indica que las traducciones de la declaración de seguridad están disponibles en las **Translated Safety Statements** en PDF publicadas en el sitio web de Allied Telesis en **alliedtelesis.com/us/en/library/search**.

Consignes de sécurité traduites:

Important: Le symbole ✍ indique que les traductions de la déclaration de sécurité sont disponibles dans le PDF **Translated Safety Statements** publiées sur le site Web de Allied Telesis à l'adresse **alliedtelesis.com/us/en/library/search**.

Dichiarazioni di sicurezza tradotte:

Importante: ✍ indica che le traduzioni della dichiarazione di sicurezza sono disponibili nelle **Translated Safety Statements** in PDF pubblicate sul sito Web di Allied Telesis all'indirizzo **alliedtelesis.com/us/en/library/search**.

Översatta säkerhetsförklaringar:

Viktig: ✍ anger att översättningar av säkerhetsförklaringen finns tillgängliga i PDF-dokumentet **Translated Safety Statements** som publicerats på Allied Telesis webbplats på **alliedtelesis.com/us/en/library/search**.

Section I

Getting Started

This section contains the following chapters:

- Chapter 1, “Overview” on page 29
- Chapter 2, “Starting a Web Browser Management Session” on page 53

Chapter 1
Overview

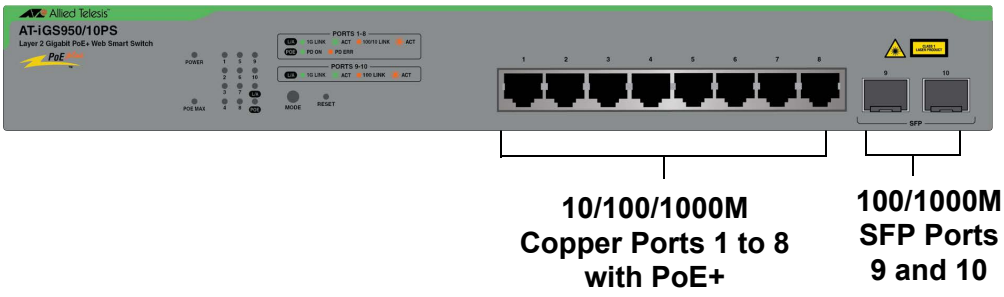
This chapter describes the hardware features of the iGS950 Series of Layer 2 Gigabit Ethernet PoE+ WebSmart Switches:

- ❒ “Front and Rear Panels on the iGS950 Series” on page 30
- ❒ “Hardware Features” on page 34
- ❒ “Copper Ports” on page 35
- ❒ “Power over Ethernet PoE+” on page 36
- ❒ “Combo Copper Ports” on page 40
- ❒ “Copper Cable Requirements” on page 41
- ❒ “SFP Ports” on page 42
- ❒ “LEDs” on page 43
- ❒ “RESET Button” on page 50
- ❒ “Power Supply and Fans” on page 51
- ❒ “Management Interfaces” on page 52

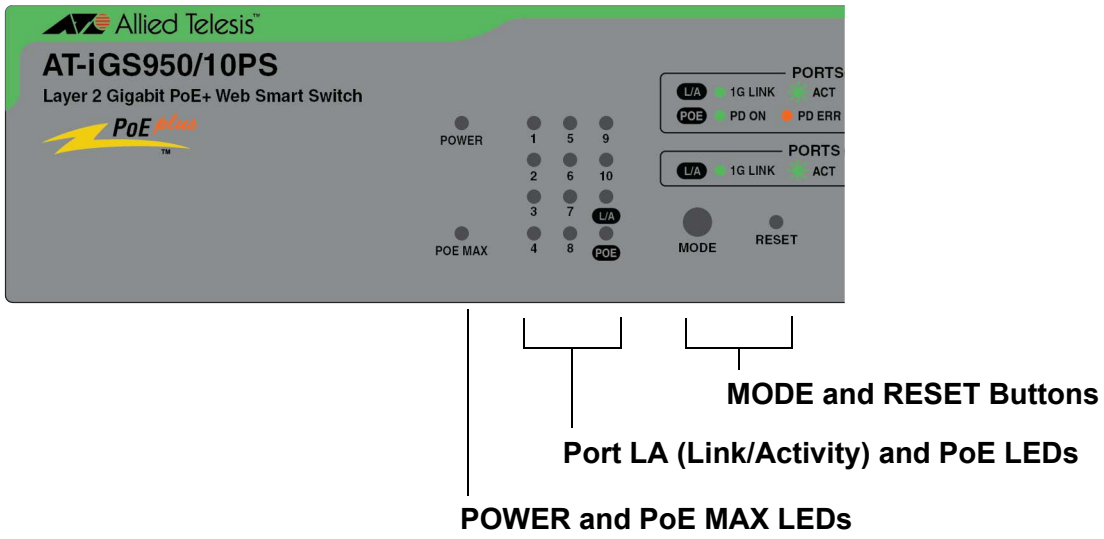
Front and Rear Panels on the iGS950 Series

Figure 1 illustrates the front and rear panels of the AT-iGS950/10PS Switch.

Front Panel - Ports



System and Port LEDs



Rear Panel

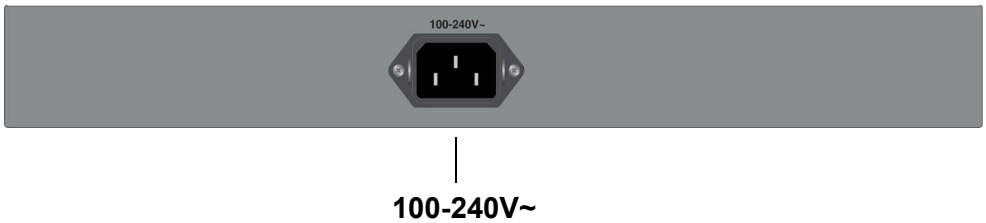
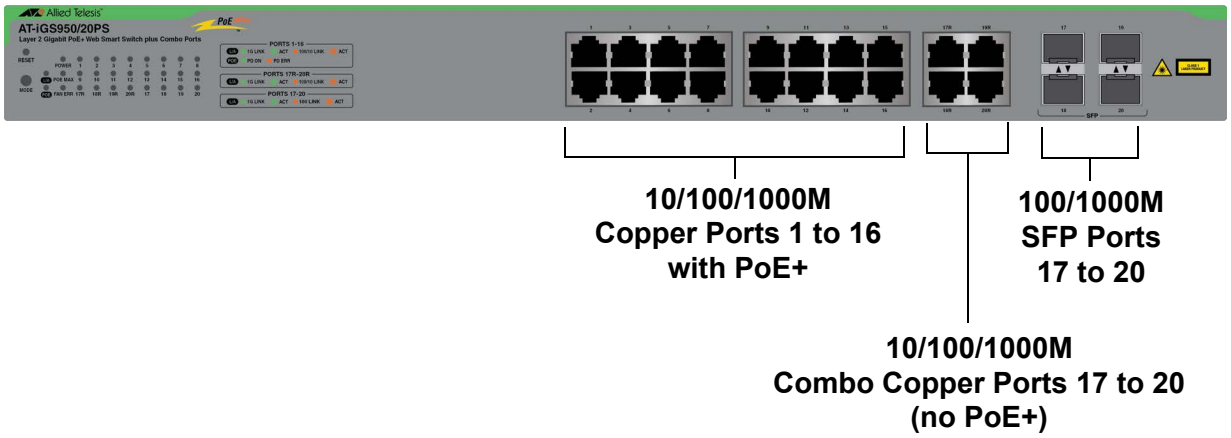


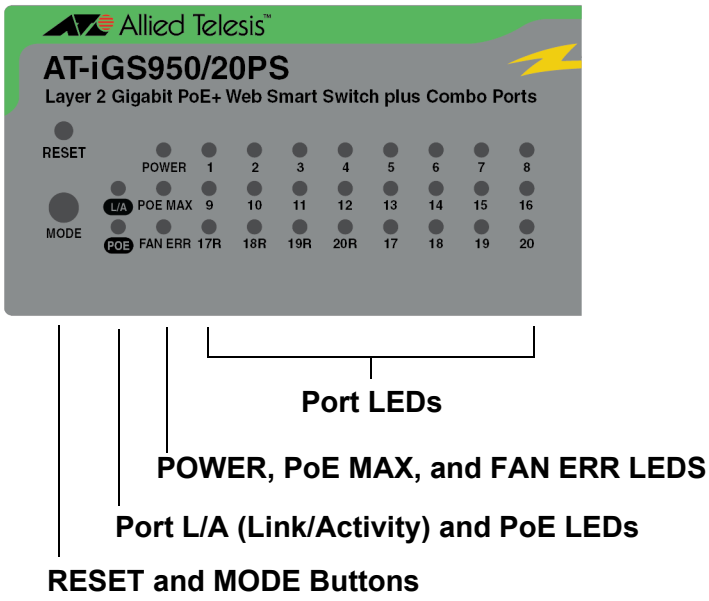
Figure 1. Front and Rear Panels on the AT-iGS950/10PS Switch

Figure 2 illustrates the front and rear panels of the AT-iGS950/20PS Switch.

Front Panel - Ports



System and Port LEDs

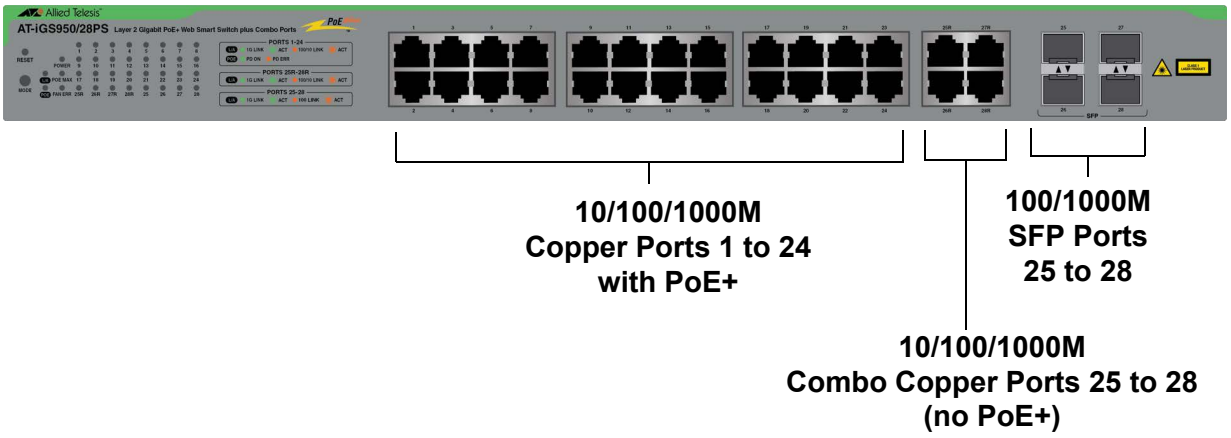


Rear Panel

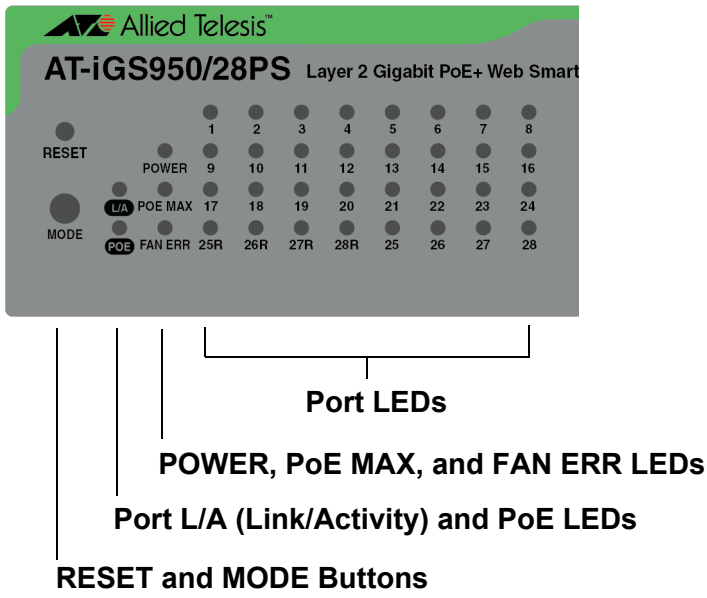
Figure 2. Front and Rear Panels on the AT-iGS950/20PS Switch

Figure 3 illustrates the front and rear panels of the AT-iGS950/28PS Switch.

Front Panel - Ports



System and Port LEDs

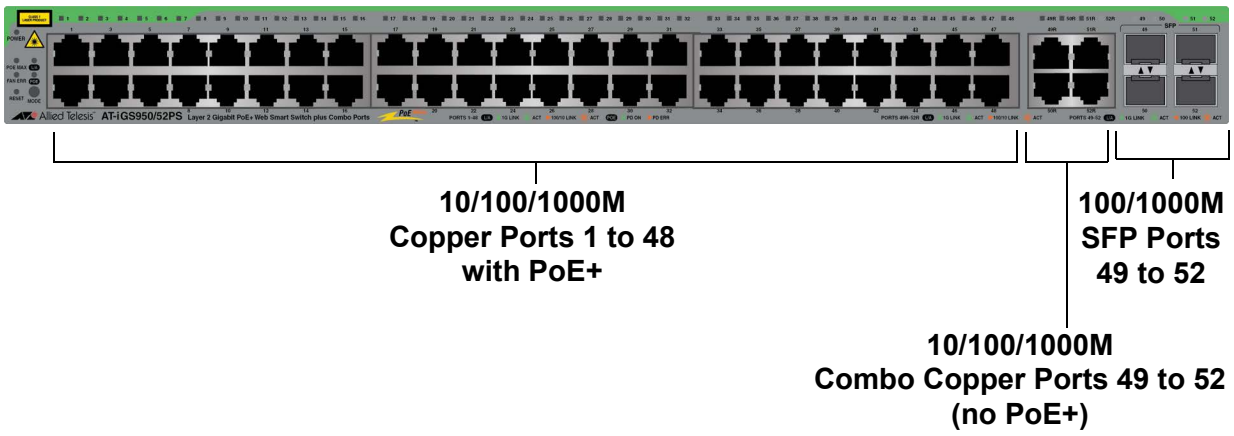


Rear Panel

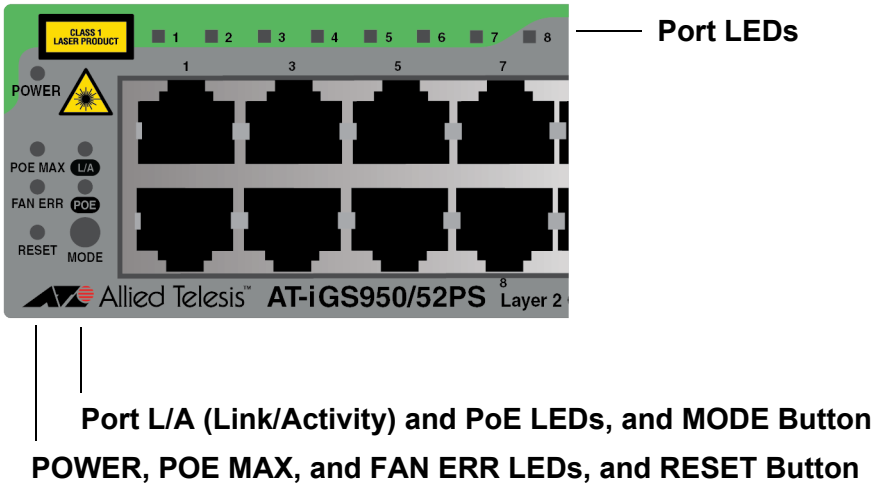
Figure 3. Front and Rear Panels on the AT-iGS950/28PS Switch

Figure 4 illustrates the front and rear panels of the AT-iGS950/52PS Switch.

Front Panel - Ports



System and Port LEDs



Rear Panel

Figure 4. Front and Rear Panels on the AT-iGS950/52PS Switch

Hardware Features

Table 1 lists the hardware features of the switches.

Table 1. Hardware Features

Feature	10PS	20PS	28PS	52PS
Port numbers of 10/100/1000M copper ports with PoE+	1 - 8	1 - 16	1 - 24	1 - 48
Port numbers of 10/100/1000M combo copper ports without PoE+	-	17R - 20R	25R - 28R	49R - 52R
Port numbers of 1000M SFP ports	9 - 10	17-20	25-28	49-52
Maximum PoE+ power	130W	370W	370W	740W
Supported PoE+ device classes	0 to 4	0 to 4	0 to 4	0 to 4
PoE+ power range at the switch ports	15.4W to 30.0W	15.4W to 30.0W	15.4W to 30.0W	15.4W to 30.0W
Auto-negotiation for speed and duplex mode on copper ports	Yes	Yes	Yes	Yes
MODE button	Yes	Yes	Yes	Yes
RESET button	Yes	Yes	Yes	Yes
MAC address table	8 Kbytes	8 Kbytes	8 Kbytes	16Kbytes
Maximum jumbo frames	10 Kbytes	10 Kbytes	10 Kbytes	12 Kbytes
Packet buffer	4.1 Mbit	4.1 Mbit	4.1 Mbit	12 Mbit
Tabletop and 19-inch equipment rack mountable	Yes	Yes	Yes	Yes

Copper Ports

Table 2 lists the hardware features of the copper ports.

Table 2. Hardware Features of the Copper Port

Feature	Description
Port speeds	Copper port speeds are listed here: - 10M (IEEE802.3 10Base-T) - 100M (IEEE802.3u 100Base-TX) - 1000M (IEEE802.3ab 1000Base-T) Speeds can be set manually or with IEEE 802.3u Auto-Negotiation.
Duplex modes	- Supports half or full duplex mode at 10/100M - Supports full duplex mode at 1000M Duplex modes can be set manually or automatically with IEEE 802.3u Auto-Negotiation.
Connector hardware	8-pin RJ-45
Connector wiring	- 10/100M Auto-MDI/MDIX. Refer to Appendix A, Technical Specifications, in the *iGS950 Series Installation Guide*. - 1000M. Refer to Appendix A, Technical Specifications, in the *iGS950 Series Installation Guide*.
Maximum distance	100 meters (328 feet)
Minimum cable requirements	- 10/100M - Standard TIA/EIA 568-B-compliant Category 3 unshielded cable. - 1000M - Standard TIA/EIA 568-B-compliant Category 5 or Category 5e unshielded cable.
Additional features	- IEEE 802.3x Back Pressure in 10/100M half-duplex mode - IEEE 802.3x Flow Control in 10/100M full-duplex mode - IEEE802.3z 1000Base-T Flow Control - Non-blocking, wire speed supported at all speeds.

Note

Copper ports that are connected to devices that do not support Auto-Negotiation should not use Auto-Negotiation to set speed and duplex mode. A speed or duplex mode mismatch may occur between the devices, resulting in reduced performance. Speed and duplex mode should be set manually on ports connected to devices that do not support Auto-Negotiation.

Power over Ethernet PoE+

The iGS950 Series of Layer 2 Gigabit Ethernet Switches features PoE+ on the copper ports. This feature enables the switches to supply power to network devices over the same cables that carry the network traffic. The value of PoE+ is that it can make it easier to install networks. Selecting locations for network devices are often limited by whether there are power sources nearby. This often limits equipment placement or requires the added time and cost of having additional electrical sources installed. But with PoE+, you can install PoE-compatible devices wherever they are needed without having to worry about whether there are adjacent power sources.

A device that provides PoE+ to other network devices is referred to as *power sourcing equipment* (PSE). The switches in the iGS950 Series act as PSE units by adding DC power on the network cables connected to its ports, thus functioning as a power source for other network devices.

Devices that receive their power from a PSE are called *powered devices* (PD). Examples include wireless access points, IP telephones, webcams, and even other Ethernet switches.

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

PoE+ Ports

Table 3 lists the ports that support PoE+ on the switches.

Table 3. PoE+ Ports

Switch	PoE+ Ports
AT-iGS950/10PS	1 to 8
AT-iGS950/20PS	1 to 16
AT-iGS950/28PS	1 to 24
AT-iGS950/52PS	1 to 48

Note

PoE+ is not supported on the combo copper ports on the AT-iGS950/20PS, AT-iGS950/28PS, and AT-iGS950/52PS Switches. Refer to Table 1 on page 34 for the combo port numbers.

Maximum PoE+ Power Budget

The maximum PoE+ power budget is the maximum amount of power the switches have for powered devices on their ports. Table 4 lists the maximum PoE+ power budgets for the switches.

Table 4. PoE+ Maximum Power Budgets

Switch	PoE+ Maximum Power Budget
AT-iGS950/10PS	130W
AT-iGS950/20PS	370W
AT-iGS950/28PS	370W
AT-iGS950/52PS	740W

PoE+ Standards

The iGS950 Series supports the PoE standards listed in Table 5.

Table 5. PoE Standards

PoE Standard	IEEE Standard	Definition
PoE	IEEE 802.3af, IEEE 802.3at Type 1	Supplies up to 15.4 watts at switch ports for powered devices requiring up to 12.95 watts.
PoE+	IEEE 802.3at Type 2	Supplies up to 30.0 watts at switch ports for powered devices requiring up to 25.5 watts.

Powered Device Classes

Powered devices are grouped into classes, based on their power requirements. The iGS950 Series supports the five classes in Table 6.

Table 6. IEEE Powered Device Classes Supported by the iGS950 Series

Class	Maximum Power Output at the Switch Port	Powered Device Power Range
0	15.4W	0.44W to 12.95W
1	4.0W	0.44W to 3.84W
2	7.0W	3.84W to 6.49W
3	15.4W	6.49W to 12.95W
4	30.0W	12.95W to 25.5W

Note

The iGS950 Series can support any combination of powered devices, up to the maximum PoE+ power budgets. Refer to Table 4 on page 37.

Mode A Power Delivery

The PoE IEEE 802.3at standard defines two modes for delivering power over copper cables from a PSE, such as the iGS950 Series, to PDs. The two modes define the pins on the RJ-45 copper ports of the PSE that supply power to the PDs.

The modes are called Mode A and Mode B, In Mode A, the PSE use pins 1, 2, 3, and 6 on its copper ports to supply power over the copper cables to the PDs. In Mode B, the PSE uses pins 4, 5, 7, and 8 on its copper ports as the power output.

The iGS950 Series supports Mode A of the IEEE 802.3at standard. The switches use pins 1, 2, 3, and 6 on copper ports to deliver power to PDs.

Most PDs are designed to support both modes. However, older PDs might support only one mode. You should review the documentation included with your PDs before connecting them to the switches to confirm that they support both modes. If they are older units that support only one mode, they must support Mode A to be compatible with the iGS950 Series

Note

Older PDs that only support Mode B are not compatible with the iGS950 Series.

PoE+ Port Priorities

If the power requirements of the powered devices exceed the switch's power budget, the switch will deny power to some ports based on a system called PoE+ port priorities. You can use this feature to ensure that powered devices critical to the operations of your network or business are given preferential treatment by the switch in the allocation of power should the demands of the devices exceed the available power.

There are three priority levels:

- Critical
- High
- Low

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

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

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

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

Combo Copper Ports

The AT-iGS950/20PS, AT-iGS950/28PS, and AT-iGS950/52PS Switches have four combo ports. These ports are identified with the letter “R” in their port numbers. Refer to Table 7.

Table 7. Combo Copper Port Numbers

Switch	Combo Copper Port Numbers
AT-iGS950/10PS	None
AT-iGS950/20PS	17R, 18R, 19R, and 20R
AT-iGS950/28PS	25R, 26R, 27R, 28R
AT-iGS950/52PS	49R, 50R, 51R, 52R

Note

The AT-iGS950/10PS Switch does not have combo ports.

Each combo copper port is paired with an SFP port. Using the AT-iGS950/20PS Switch as an example, the 17R combo copper port is paired with the 17 SFP port, the 18R combo copper port is paired with the 18 SFP port, and so forth. Only one port in a pair, either the copper port or the corresponding SFP port, can be active at a time. Here are the rules and guidelines to using the combo copper ports:

- Combo copper ports do not support PoE+.
- Other than not supporting PoE+, these ports support the same operating properties and features as the other copper ports in the switches. Refer to Table 2 on page 35.
- The copper port is the active port of a pair when there is no transceiver in the corresponding SFP port or the SFP transceiver does not have an active connection to a network device.
- If both the combo copper port and SFP port of a pair are connected to active network devices, the SFP port becomes the active port and the combo copper port automatically transitions to a redundant status.
- In nearly all cases, the copper and SFP ports of a pair share the same configuration settings, including port settings, VLAN assignments, access control lists, and spanning tree.
- One exception to the shared settings of paired ports is port speed. If you disable Auto-Negotiation on a copper port and set the speed and duplex mode manually, the speed reverts to Auto-Negotiation when the SFP port in the port pair establishes a link to an end node.

Copper Cable Requirements

The minimum copper cable requirements for non-PoE devices are listed here:

- 10/100M - Standard TIA/EIA, 568-B-compliant cable, Category 5, 100 ohm, shielded or unshielded cabling, complying with IEEE 802.3u 100Base-TX specifications
- 1000M - Standard TIA/EIA, 568-B-compliant cable, Category 5, 100 ohm, 4-pair, shielded or unshielded cabling, complying with IEEE 802.3ab 1000Base-T specifications. Category 5e is recommended.

The minimum copper cable requirements for PoE devices are listed here:

- Category 5 unshielded or better is recommended for ITE immunity levels (i.e., EN 55035)
- Category 6 or 6a shielded twisted pair cable or shielded foil twisted pair cable is required to meet immunity levels in high RF noise environments, such as industrial Ethernet sites, electric power utility stations, electric power substations, and rail yards.

Note

Shielded or unshielded Category 5 or better cable is required to meet EN55035 immunity levels.

SFP Ports

The SFP ports support 100M and 1000M fiber optic transceivers and copper connector transceivers. The ports support the following types of 100M fiber optic transceivers:

- 100M SFP multi-mode fiber (MMF) optic transceivers with operating distances up to 2 kilometers
- 100M SFP single-mode fiber (SMF) optic transceivers with operating distances up to fifteen kilometers

The SFP ports the following types of 1000M fiber optic and copper connector transceivers:

- 1000M SFP SMF and MMF fiber optic transceivers
- 1000M SFP SMF and MMF fiber optic transceivers with extended operating temperature ranges
- 1000M SFP SMF single core, bi-directional fiber optic transceivers
- 1000M copper cable transceivers

Fiber optic transceivers are available with operating distances over 40 kilometers and wide industrial temperature ranges.

Transceivers are hot-swappable. You can install or remove them while the switch is powered on.

Note

Transceivers are purchased separately. For a list of supported transceivers, refer to the product's data sheet on the Allied Telesis web site at **www.alliedtelesis.com**.

Note

To ensure compatibility, use only transceivers that have been approved by Allied Telesis for use with this product.

LEDs

The following sections describe the LEDs:

- “POWER LED” next
- “FAN ERR LED” on page 43
- “POE MAX LED” on page 44
- “Copper Port LEDs and the MODE Button” on page 45
- “SFP LEDs” on page 48

POWER LED

The switches have a POWER LED. An example is shown in Figure 5.

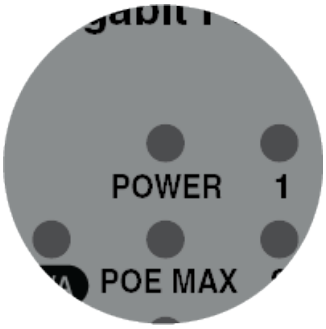


Figure 5. POWER LED

The LED is defined in Table 8.

Table 8. POWER LED

State	Description
Solid Green	The switch is operating normally.
Off	Possible sources of this condition are: - The AC power cord is disconnected. - The AC power source is powered off or has failed. - The switch experienced a hardware or software failure. - The switch shutdown from a power surge. - The power supply failed. For troubleshooting suggestions, refer to the *iGS950 Series Installation Guide*..

FAN ERR LED

AT-iGS950/20PS, AT-iGS950/28PS, and AT-iGS950/52PS Switches have FAN ERR LEDs. The LED displays the status of the internal ventilation fans. (The AT-iGS950/10PS Switch does not have this LED.) An example of the LED is shown in Figure 6 on page 44.

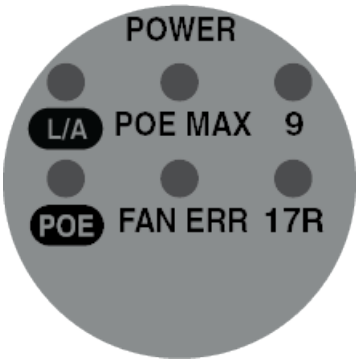


Figure 6. FAN ERR LED

Table 9 describes the states of the LED.

Table 9. FAN ERR LED

State	Description
Off	The internal fans are operating properly or the switch is powered off.
Red	One or more fans are experiencing a problem. Use the management software to view fan status. If necessary, replace the switch.

POE MAX LED

Switches have a POE MAX LED on the front panels. An example is shown in Figure 7.

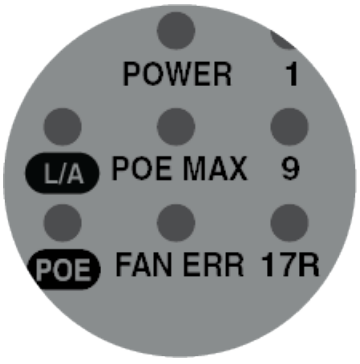


Figure 7. POE MAX LED

Table 10 details the states of the POE MAX LED.

Table 10. POE MAX LED

State	Description
Off	Possible causes of this state are: ❒ The switch is not connected to any powered devices. ❒ The switch is supplying power to one or more powered devices, and has sufficient PoE power to support additional powered devices.
Amber	The switch is nearing or has reached its maximum PoE budget from supporting the power requirements of the powered devices on its copper ports. The switch will not support additional powered devices and may be denying power to some ports.

Copper Port LEDs and the MODE Button

Each copper port on the switch has an LED that displays link and activity status, or PoE+ status information. The copper port LEDs on the AT-iGS950/10PS, AT-iGS950/20PS, and AT-iGS950/28PS Switches are grouped on the left sides of the front panels. An example is shown in Figure 8.

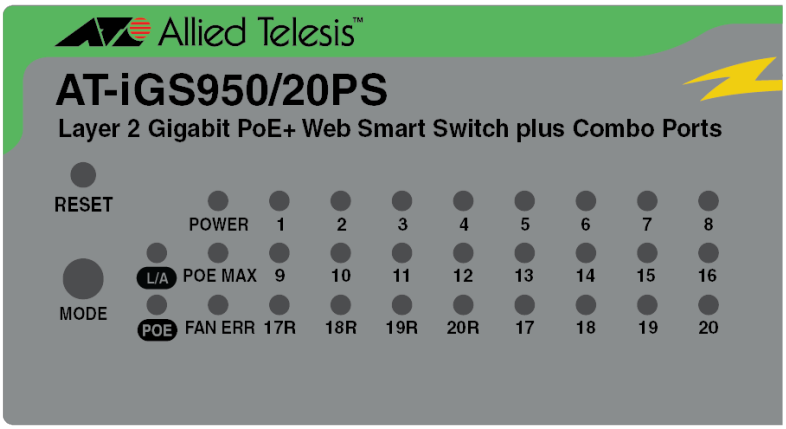


Figure 8. Copper Port LEDs on the AT-iGS950/20PS Switch

The copper port LEDs on the AT-iGS950/52PS Switch are located in a row across the top of the front panel. Refer to Figure 9 on page 46.

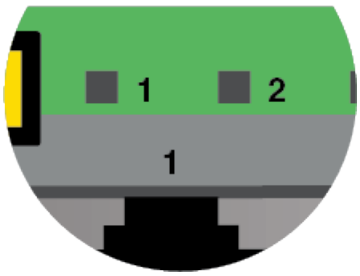


Figure 9. Copper Port LEDs on the AT-iGS950/52PS Switch

The copper port LEDs display the following information:

- Link/Activity (L/A) status
- PoE+ status

The switches have a MODE button that controls the status of the port LEDs. Refer to Figure 10. The button toggles the copper port LEDs between displaying link/activity information or PoE+ status. The status of the copper port LEDs is displayed by the L/A and POE LEDs next to the MODE button.

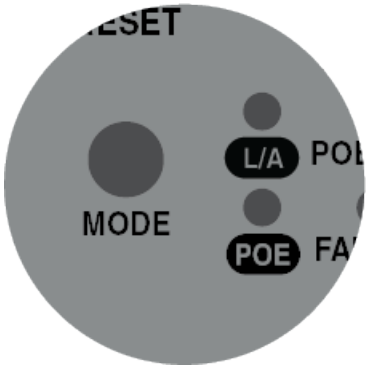


Figure 10. MODE Button with L/A and POE LEDs

Table 11. MODE Button L/A and POE LEDs

LED	State	Description
L/A	Green	The copper port LEDs are displaying link/activity status.
POE	Green	The copper port LEDs are displaying PoE+ status.

Note
The MODE button does not control the LEDs on the combo copper ports or SFP ports. Those port LEDs always display link/activity status.

Table 12 defines the states of the copper port LEDs when displaying link/activity status.

Table 12. Copper Port LEDs in Link/Activity (L/A) Mode

State	Description
Off	Possible causes of this state: ❒ The port is not connected to a network device or the network device is powered off. ❒ The port is connected to a network device but the switch is unable to establish a connection to it. ❒ If the copper port is a combo port, its corresponding SFP port may have a link to a network device, in which case the copper port is disabled.
Steady Green	The copper port has established a 1000M connection to a network device.
Flashing Green	The copper port is transmitting or receiving network traffic from a network device at 1000M.
Steady Amber	The port has established a 10M or 100M link to a network device.
Blinking Amber	The port is receiving or transmitting network traffic at 10M or 100M.

Table 13 defines the states of the copper port LEDs when displaying PoE+ status.

Table 13. Copper Port LEDs in PoE+ Mode

State	Description
Off	This state has the following possible causes: - The port is not connected to a network device. - The port is connected to a non-PoE device. - The port is connected to a older powered device that does not support the Mode A power delivery on pins 1, 2, 3, and 6 on the RJ-45 port.
Green	The copper port is delivering power to a PoE or PoE+ device.
Amber	The switch has detected an error condition on the port. Examples include the following: - The powered device is requiring more power than its device class. - There is a terminal short in the network cable or connector. For troubleshooting suggestions, refer to the *iGS950 Series Installation Guide*.

SFP LEDs

The SFP ports have Link/Activity (L/A) LEDs. The LEDs for SFP ports 9 and 10 on the AT-iGS950/10PS Switch are located on the left side of the faceplate, with the copper port LEDs. Refer to Figure 11.

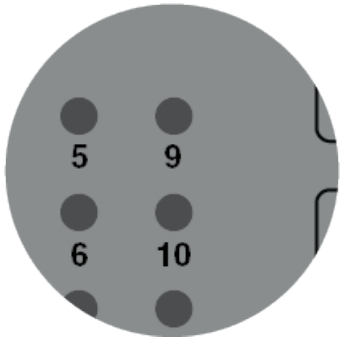


Figure 11. LEDs for SFP Ports 9 and 10 on the AT-iGS950/10PS Switch

The SFP port LEDs for all other switches in the iGS950 Series are located between the SFP ports. An example is shown in Figure 12 on page 49.

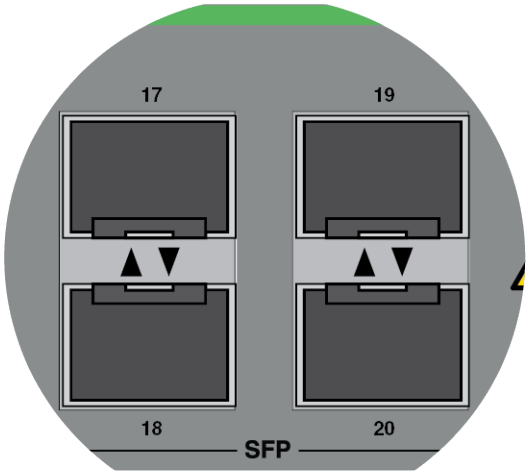


Figure 12. Link/Activity (L/A) LEDs for SFP Ports

The states of the SFP port LEDs are defined in Table 14.

Table 14. Link/Activity LEDs for the SFP Ports

State	Description
Off	Possible causes of this state are: ❒ The SFP slot is empty. ❒ The SFP transceiver has not established a link with a remote network device. ❒ The remote network device is powered off.
Steady Green	The port has established a 1000M link to a remote network device.
Blinking Green	The port is receiving and transmitting network traffic at 1000M.
Steady Amber	The port has established a 100M link to a remote network device.
Blinking Amber	The port is transmitting or receiving network packets at 100M.

RESET Button

The RESET button, shown in Figure 13, has these two functions:

- Reboots the switch so that it initializes its management software and reloads its saved configuration. To reboot the switch, press the RESET button for one to five seconds.
- Restores the default configuration settings on the switch. You might perform this action to discard the switch's current configuration or if you lost the management login password. To restore the default configuration settings on the switch, press the RESET button for more than six seconds. The switch turns off all the port LEDs to indicate that the configuration reset has started.

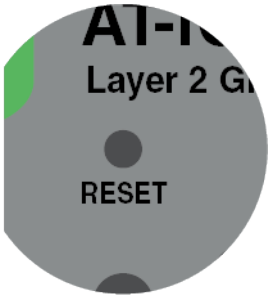


Figure 13. RESET Button

Note

Restoring the default settings returns the management IP address to the default 192.168.1.1. You may need to change the IP address on your workstation to manage the switch again. Refer to "Starting a Web Browser Management Session" on page 54.

Caution

The switch temporarily stops forwarding network traffic when you reboot it or restore the default settings. Some network traffic may be lost. E113

Note

You can disable the RESET button with the management software. For instructions, refer to the *iGS950 Series Web Browser User Guide.*

Power Supply and Fans

Power Supply

The switches have one internal power supply with a single AC power supply socket on the rear panel. You power the switch on or off by connecting and disconnecting the power cord. The power cord is supplied with the switch.

Note

For power requirements, refer to Appendix A, Technical Specificatons, in the *iGS950 Series Installation Guide*..

Ventilation Fans

Three of the switches come with two or three internal ventilation fans:

- AT-iGS950/10PS - none
- AT-iGS950/20PS - 2 fans
- AT-iGS950/28PS - 2 fans
- AT-iGS950/52PS - 3 fans

The fans are located on the right sides of the switches, when facing the front of the units. They draw air out of the switches, with airflow direction from left to right. Refer to Figure 14.

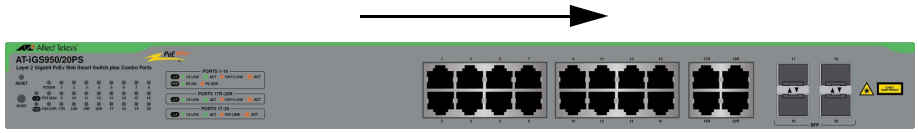


Figure 14. Ventilation Airflow of Switches with Fans

Review the following:

- Fans are not field replaceable.
- Fan status is indicated with the FAN ERR LED. Refer to “FAN ERR LED” on page 43.
- The AT-iGS950/10PS Switch does not have internal ventilation fans. It relies on surrounding airflow for cooling.

Note

Be sure the installation site provides adequate airflow to prevent switches from overheating and shutting down.

Management Interfaces

The iGS950 Series has three management interfaces that are accessed over your network from your workstation:

- Web browser interface: This interface consists of a series of web browser windows that support non-secure HTTP and secure HTTPS. The default is HTTP. This interface allows you to configure all the features and functions of the switches. The default setting for this interface is enabled.
- Command line Interface: This interface is accessed with a Telnet or Secure Shell (SSH) client from your workstation. It has a series of command line commands that configure a subset of the software features, such as the IPv4 and IPv6 addresses.

  The default setting for the Telnet server is enabled. The default setting for the SSH server is disabled. To enable the server, you have to use the SSH Settings option under the System menu in the web browser management interface.
- SNMPv1, v2c, and v3: This interface consists of SNMP MIBs and objects. Only experienced technicians should manage devices with SNMP.

Note

Allied Telesis may periodically release updates to the management software for our products and provide them on our public web site for customers to download. For instructions, see the product's management guide.

Chapter 2

Starting a Web Browser Management Session

This chapter contains the following sections:

- “Starting a Web Browser Management Session” on page 54
- “Ending a Web Browser Management Session” on page 56
- “Menus” on page 57
- “Dashboard View” on page 59
- “Switch View” on page 62
- “Saving Your Changes” on page 63
- “Unsupported Special Characters” on page 65

Starting a Web Browser Management Session

Please review the following information before starting a management session on the switch:

- The switch comes with the default IPv4 address 192.168.1.1 and subnet mask 255.255.255.0. If you have not yet assigned a new address to the switch, you must use the default address to establish your first management session.
- The switch does not have a default IPv6 address.
- If you have already assigned the switch a new IPv4 or IPv6 address either manually or with a DHCP server, use that address to establish your management sessions with the unit.
- If the switch still has the default IPv4 address, you will need to change the IP address of your workstation to the same subnet as the switch's default address. For example, you might change the workstation's IP address to 192.168.1.4. Refer to the computer's documentation of instructions on how to set its IP address.
- The switch has IPv4 and IPv6 DHCP clients. Their default status is disabled. You can enable them during the initial management session so that the switch receives its IP address configuration from a DHCP server on your network the next time you reboot or power on the unit.

Note
The switch does not support BOOTP.

Here is the procedure for starting a web browser management session with the switch:

Note
If the switch has its default IPv4 address 192.168.1.1, start with step 1. If you already assigned the switch a new address, start with step 3.

1. Change the IPv4 address of your computer to 192.168.1.*n*, where n is any number from 2 to 254. Refer to the computer's documentation for instructions.
2. Connect the Ethernet network port on your computer to any Ethernet port on the switch.
3. Power on the switch and wait several minutes for it to start the management firmware.

4. Start the web browser on your computer.

5. Enter the IP address of the switch in the URL field of the web browser. The default address is 192.168.1.1 with the subnet mask 255.255.255.0.

   The switch displays the login window. Refer to Figure 15.

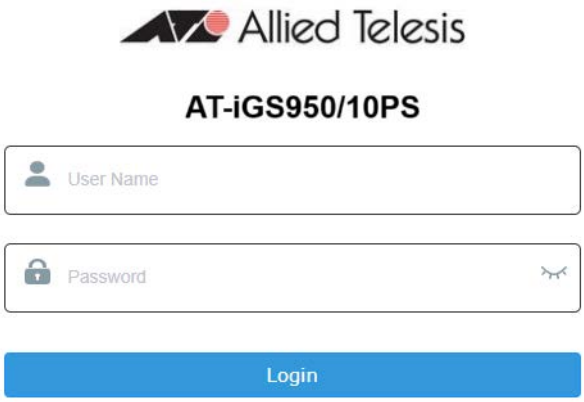


Figure 15. Login Window

6. Enter the username and password for the switch. The default settings are “manager” and “friend”, respectively. The username and password are case sensitive. (The password appears in the Password field as a series of asterisks.)

7. Click the **Login** button.

   The switch displays the Dashboard view. Refer to “Dashboard View” on page 59.

Ending a Web Browser Management Session

To end a web browser management session, click the Logout icon in the upper right corner of the window and, for added security, close your web browser. Refer to Figure 16.

Figure 16. Logout Icon

Menus

Figure 17 shows the main menu of the web browser management interface. The menu is displayed on the left side of the window.

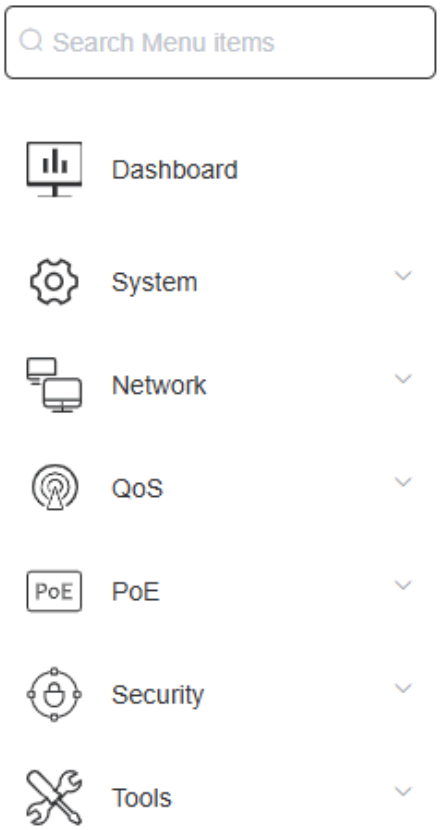


Figure 17. Main Menu

Clicking on a main menu selection displays its options. The example in Figure 18 on page 58 shows the Security menu options.

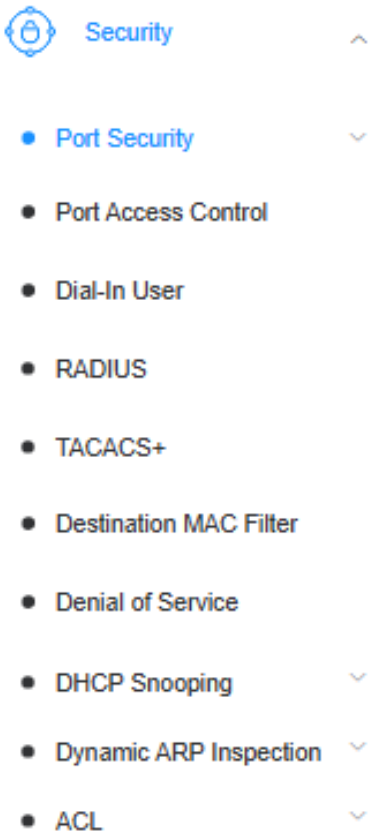


Figure 18. Security Menu Options

Menu selections with the “V” symbol to the right have sub-menus that you display by clicking the selections. Figure 19 shows part of the Port Security sub-menu.

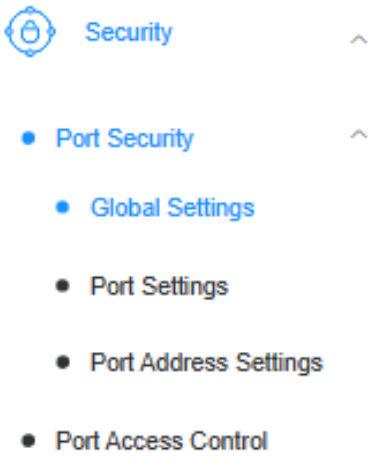


Figure 19. Example of a Sub-menu

Dashboard View

The first window displayed after starting a management session is the Dashboard View. An example is shown in Figure 20.

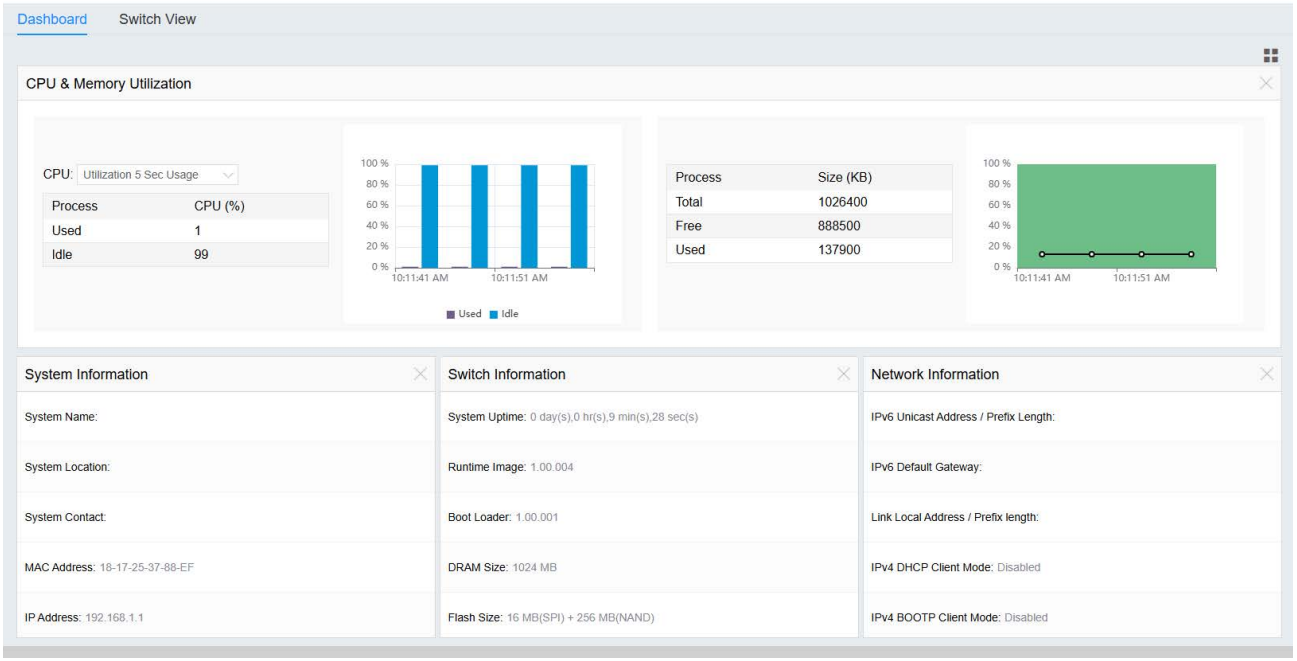


Figure 20. Dashboard View

The sections in the Dashboard view are explained in the following sections.

CPU & Memory Utilization

The CPU & Memory Utilization section consists of the following four sections:

CPU Table

The CPU table displays the numerical percentages of used and idle CPU processes of the switch, up to a total of 100%. The CPU pull-down menu allows you to select the sampling interval. The available intervals are:

- 5 seconds (default)
- 1 minute
- 5 minutes

CPU Bar Chart

The blue bars in the chart represent the percentages of unused processes and the orange bars represent the percentage of used processes, up to a total of 100%.

Process Table (Memory Utilization)

The process table displays the total, free, and used portions of system memory, in kilobytes.

Process Graphic

The graph charts the amount of used memory as a percentage of total memory.

System Information

The fields in the System Information section are described in Table 15.

Table 15. System Information

Field	Description
System Name	Displays the name assigned to the switch. Refer to Chapter 3, “System Name, Location, and Administrator” on page 69.
System Location	Displays the physical location of the switch. Refer to Chapter 3, “System Name, Location, and Administrator” on page 69.
System Contact	Displays the name of the contact person responsible for managing the switch. Refer to Chapter 3, “System Name, Location, and Administrator” on page 69.
MAC Address	Displays the MAC address of the switch. This value is not adjustable.
IP Address	Displays the switch’s IPv4 address. Refer to Refer to “Assigning IPv4 Addresses to the VLANs on the Switch” on page 73.

Switch Information

The options in the Switch Information section are explained in Table 16.

Table 16. Switch Information

Field	Description
System Uptime	Displays the number of days, hours, minutes, and seconds the switch has been running since the last reboot.
Runtime Image	Displays the version number of the runtime firmware.
Boot Loader	Displays the version number of the bootloader firmware.

Table 16. Switch Information (Continued)

Field	Description
DRAM Size	Displays the size of the DRAM, in megabytes.
Flash Size	Displays the size of the flash memory, in megabytes.

Network Information

The Network Information section is described in Table 17.

Table 17. Network Information

Field	Description
IPv6 Unicast Address/Prefix Length	Displays the switch's IPv6 address and prefix length. Refer to Chapter 5, "Management IPv6 Addresses" on page 81.
IPv6 Default Gateway	Displays the IPv6 default gateway address. Refer to Chapter 5, "Management IPv6 Addresses" on page 81.
Link Local Address/ Prefix Length	Displays the IPv6 link local address. Refer to Chapter 5, "Management IPv6 Addresses" on page 81.
IPv4 DHCP Client Mode	Displays the status of the IPv4 DHCP client on the switch. Refer to "Assigning IPv4 Addresses to the VLANs on the Switch" on page 73.
IPv4 BOOTP Client Mode	Displays the status of the IPv4 BOOTP client on the switch. The switch does not support BOOTP.

Switch View

The Switch View option in the upper left corner of the window displays port status. The colors represent port speeds. Review the following:

- The legend above the graphic defines the colors.
- The selectable options Status, PoE, Mirror, and Uplink below the graphic allow you to customize the view to display specific port functions. You can select only one function at a time, The default is Status.
- Clicking on a port displays traffic statistics below the switch graphic.

Saving Your Changes

The switch immediately implements your changes to its parameter settings as soon you enter them in the web browser interface and click Apply. However, you must save the settings in a configuration files in flash memory. Otherwise, your changes will be discarded if you reboot or power cycle the switch.

The switch has two configuration files. They are labeled Config 1 and Config 2. One file is active and the other is inactive. The switch uses the active file to store its configuration settings and to restore them when rebooted or powered on.

You can use the inactive file for several functions. For instance, you can use it as a backup to the active file so that if the latter becomes damaged or corrupted, you can quickly restore the switch settings. You can also use the inactive file to return the switch to an earlier configuration.

By default, Config 1 is the active configuration file and Config 2 is the inactive file. For instructions on designating the inactive file as the active file, refer to “Saving Your Changes” on page 63.

Perform the following procedure to save the switch’s configuration to the Config 1 or Config 2 configuration file:

1. Select **Save** at the bottom of the menu. Refer to Figure 17 on page 57. The switch displays the Save Settings to Flash window in Figure 21.

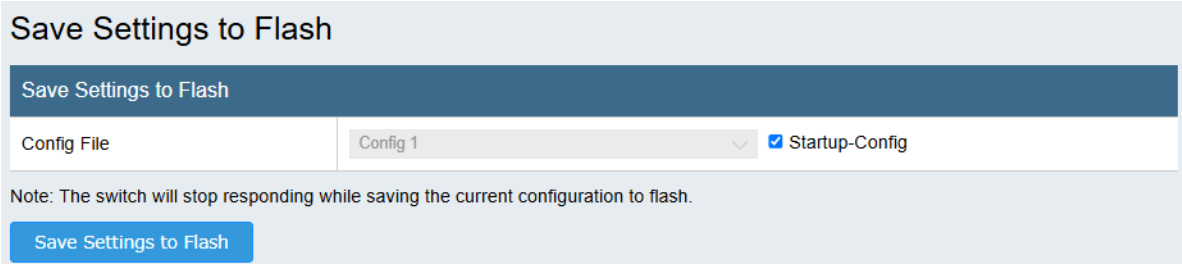


Figure 21. Save Settings to Flash Window

2. To save your changes to the active configuration file, click the **Save Settings to Flash** button. You do not need to change the window to save to the active file. The default active file is Config 1.

3. To save your changes to the inactive configuration file, do the following:

   a. Click the **Startup-Config** option to remove the check mark from the dialog box.

b. Select the inactive configuration file from the menu. The default inactive file is Config 2.

c. Click the **Save Settings to Flash** button. The switch's configuration is save in the inactive file.

d. To designate the inactive configuration file as the active file, click the **Startup-Config** to add a check mark.

Unsupported Special Characters

The following special characters not support in the text fields in the management interfaces:

- Vertical bar (|)
- Comma (,)
- Forward slash and backslash (\ /)
- Angle brackets (< >)
- Question mark (?)
- Colon (:)
- Semicolon (;)
- Single quote (‘)
- Double quotes (“)

Section II

System Menu

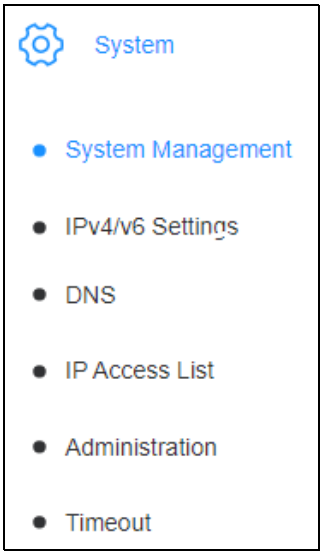
This section contains the following chapters:

- Chapter 3, “System Name, Location, and Administrator” on page 69
- Chapter 4, “Management IPv4 Addresses” on page 71
- Chapter 5, “Management IPv6 Addresses” on page 81
- Chapter 6, “System Time” on page 91
- Chapter 7, “Web Browser Management” on page 97
- Chapter 8, “Secure Shell and Telnet Servers” on page 103
- Chapter 9, “DHCP Auto Configuration” on page 107
- Chapter 10, “DHCP IPv4 Relay” on page 109
- Chapter 11, “DHCP IPv6 Relay” on page 117
- Chapter 13, “System Log and Syslog Client” on page 135
- Chapter 14, “SNMPv1 and v2c” on page 141
- Chapter 15, “SNMPv3” on page 153
- Chapter 16, “RMON” on page 167
- Chapter 17, “Traffic Statistics and Charts” on page 183
- Chapter 18, “Managing IEEE” on page 187

Chapter 3

System Name, Location, and Administrator

Procedure



To set the name, location, and administrator of the switch:

1. Select **System** > **System Management** from the menu. The Management window is shown in Figure 22 on page 70.
2. Configure the parameters in Table 18.
3. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

Table 18. Management Window

Field	Description
System Description	Displays the Allied Telesis switch model. You cannot change this value.
System Object ID	Displays the SNMP MIB object identifier of the switch model. You cannot change this value.
System Name	Enter a name of up to 50 characters for the switch, for example Sales. The name is optional. Spaces and most special characters are allowed. Refer to “Unsupported Special Characters” on page 48.
System Location	Enter the physical location of up to 30 characters for the switch. The location is optional. Spaces and most special characters are allowed.

Table 18. Management Window (Continued)

Field	Description
System Contact	Enter the name of the network administrator responsible for maintaining the switch. The system contact can have up to 30 characters. The system contact is optional. Spaces and most special characters are allowed.

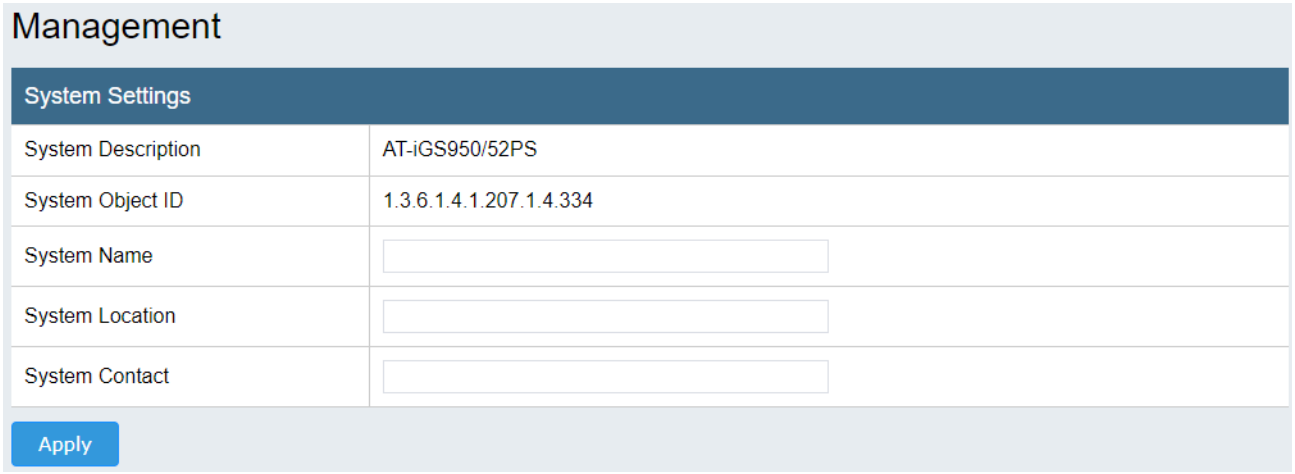


Figure 22. Management Window

Chapter 4

Management IPv4 Addresses

This chapter contains the following procedures:

- “Assigning IPv4 Addresses to the VLANs on the Switch” on page 73
- “Setting the ARP Aging Time” on page 75
- “Managing Static IPv4 ARP Entries” on page 76
- “Managing IPv4 Static/Default Route Addresses” on page 78
- “Managing DNS Server IPv4 and IPv6 Addresses” on page 80

IPv4 Address Overview

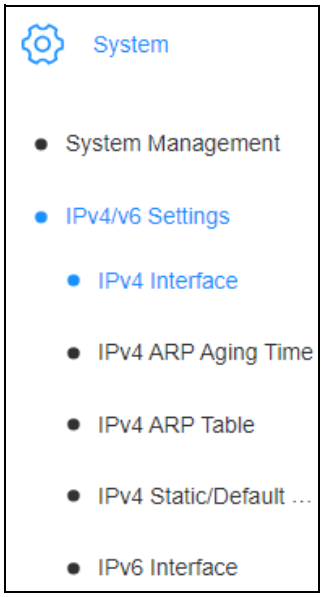
This chapter explains how to assign IP4 addresses to the VLANs on the switch. The addresses can be assigned manually or from a DHCP or BOOTP server. The switch must have IP addresses to support the following features:

- Web browser management
- Command line management with a Telnet or Secure Shell client
- Syslog server
- RADIUS authentication
- TACACS+ authentication
- RMON
- SNMPv1, v2c, or v3
- HTTP software updates
- TFTP software updates
- Ping tests

The switch has the following default static IPv4 address settings:

- IPv4 address 192.168.1.1
- Subnet mask 255.255.255.0
- Gateway address: null

Assigning IPv4 Addresses to the VLANs on the Switch



This section contains instructions on how to assign management IPv4 addresses to the VLANs on the switch. Here are the guidelines:

- IPv4 addresses are used to manage the switch and for other management functions.
- A VLAN must already exist on the switch before you can assign it an IPv4 address. For instructions, refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.
- The switch has the default IPv4 address 192.168.1.1 assigned to the Default_VLAN. In its default configuration, the Default_VLAN contains all ports on the switch.
- You can management the switch only through VLANs that have either an IPv4 or IPv6 address.

To assign an IPv4 management address to a VLAN on the switch:

1. Select **System** > **IPv4/IPv6 Settings** > **IPv4 Interface** from the menu. The IPv4 Interface window is shown in Figure 23.

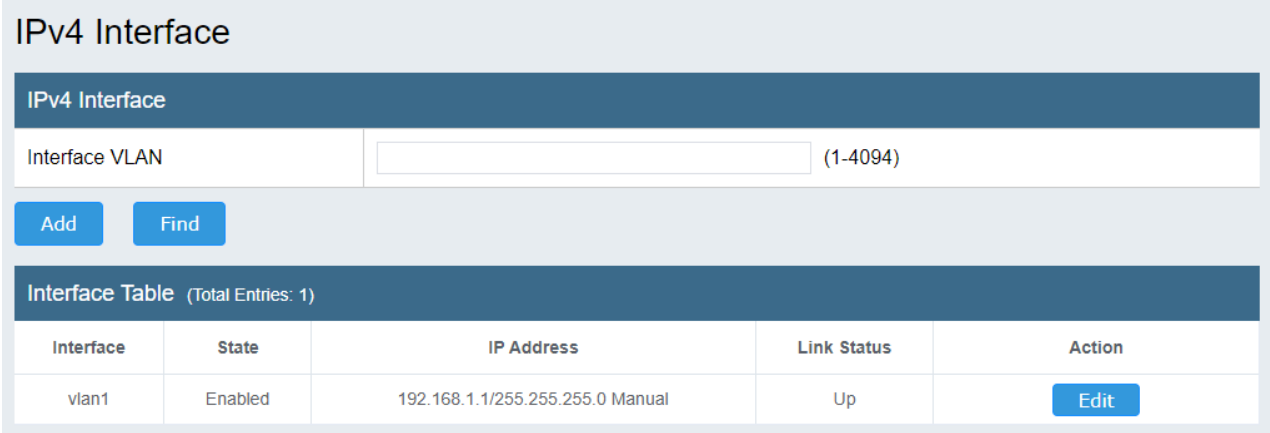


Figure 23. IPv4 Interface Window

2. In the **Interface VLAN** field, enter the VID number of the VLAN to be assigned an IPv4 address. You can enter only one VID.
3. Click **Add**. The VLAN is added to the Interface Table, without an IP address.
4. Click the new entry’s **Edit** button. The IPv4 Interface Configuration window in Figure 24 on page 74 is displayed.

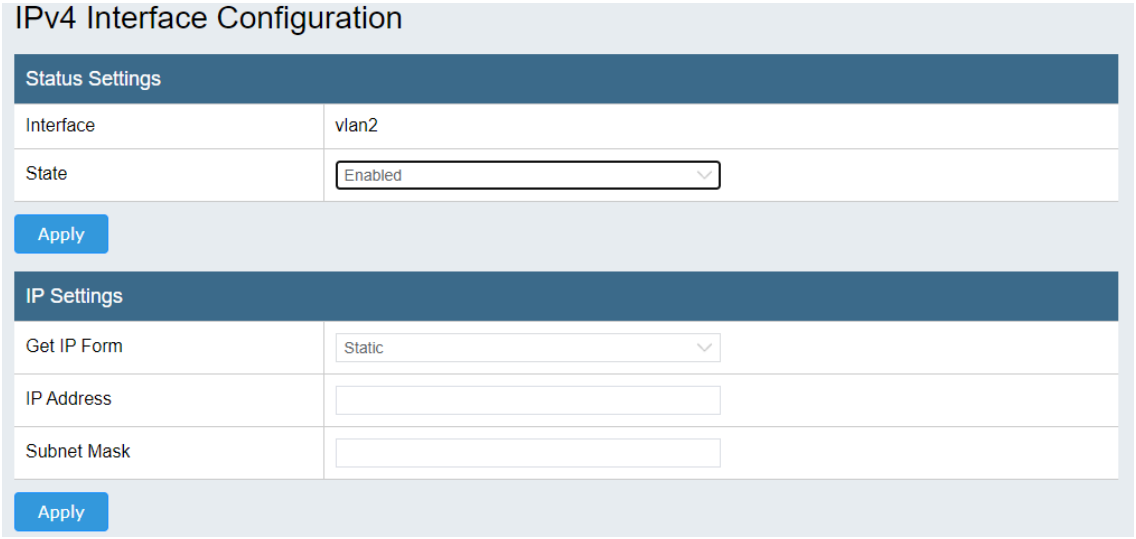


Figure 24. IPv4 Interface Configuration Window

5. Configure the parameters in Table 19.

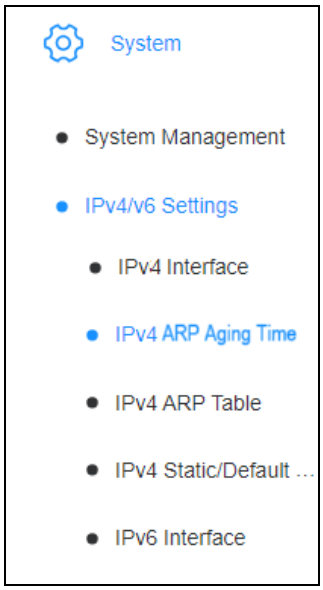
Table 19. IPv4 Interface Configuration Window

Field	Description
Status Settings	
Interface	Displays the VLAN name.
State	Controls the state of the IP address on the VLAN: - **Enabled**: Enables the IP address. - **Disabled**: Disables the IP address and those management functions that use the address.
IP Settings	
Get IP From	Select either **Static** to enter a static address or **Dynamic** to assign the address from a DHCP server. If you select Static, enter the address and subnet mask in the follopwing fields.
IP Address	Enter the static IPv4 address for the VLAN.
Subnet Mask	Enter the static IPv4 subnet mask for the VLAN.

6. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

Setting the ARP Aging Time



The switch times out dynamic IPv4 ARP entries to prevent the cache from filling up with entries for hosts that are inactive. If the switch stops receiving traffic for a device specified in a dynamic ARP entry, it deletes the entry after a timeout period, referred to as the ARP aging time, expires. Static ARP entries are not aged or automatically deleted. To set the IPv4 ARP aging time:

1. Select **System** > **IPv4/v6 Settings > IPv4 ARP Aging Time** from the menu. The Management window is shown in Figure 23 on page 73. The columns are defined in Table 20.
2. Click the **Edit** button of the VLAN whose ARP aging time you want to change. You can change the aging time of only one VLAN at a time.
3. Enter the new ARP aging time. in the Timeout field.
4. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

Table 20. ARP Aging Time Window

Field	Description
Internet Name	Lists the names of VLANs on the switch with IPv4 addresses.
Timeout	Displays the ARP aging time.

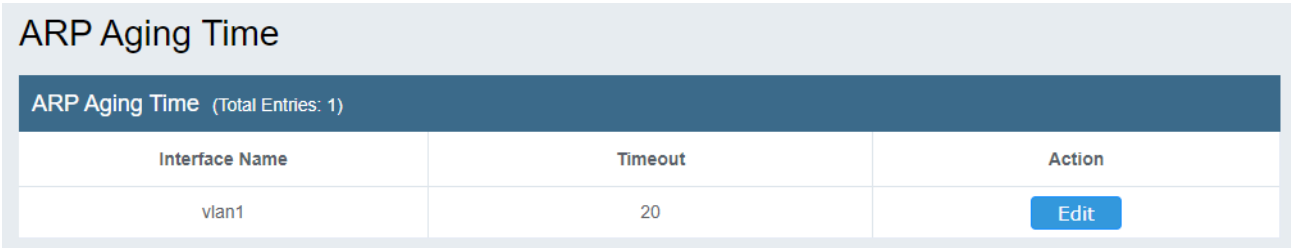


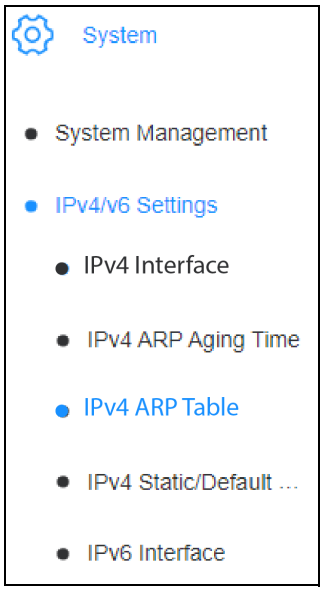
Figure 25. ARP Aging Time Window

Managing Static IPv4 ARP Entries

Address Resolution Protocol (ARP) is used by network devices to dynamically learn the Layer 2 addresses of other devices in their networks. Most hosts also have a MAC physical address in addition to an assigned IP address, which for Ethernet is a 6-byte, globally unique number. ARP enables network devices to learn the physical address of the host that has a given IP address.

When a network device needs to forward packets to a destination with an unknown Layer 2 address, it broadcasts an ARP request with the target IP address to determine where to send the packet. All stations on the LAN receive this broadcast but only the device with the specified IP address responds, giving the device its physical address.

If your LAN includes hosts that do not support ARP, you can add static ARP entries to the cache. However, it is rarely necessary to add an ARP entry this way.



To manage static IPv4 ARP entries:

1. Select **System** > **IPv4/v6 Settings** > **IPv4 ARP Table** from the menu. The Static ARP window is shown in Figure 23 on page 73. The Static ARP Table in the window lists the existing dynamic and static ARP entries. The table columns are defined in Table 21.

Table 21. Static ARP Table

Column	Description
Interface Nane	Displays the name of the VLAN where the device resides.
IP Address	Displays the IP address of the device.
Hardware Address	Displays the hardware MAC address of the device.
Aging Time	Displays the amount of time remaining until the switch deletes the ARP entry. Restricted to dynamic entries only.
Type	Lists whether the entry is dynamic or static.

2. To add a new static entry, enter values in the two fields under Static ARP. Refer to Table 22 on page 77.

Table 22. Static ARP Window

Field	Description
IP Address	Enter the IPv4 address of the host device. You can enter only one address at a time.
Hardware Address	Enter the MAC address of the device.

3. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

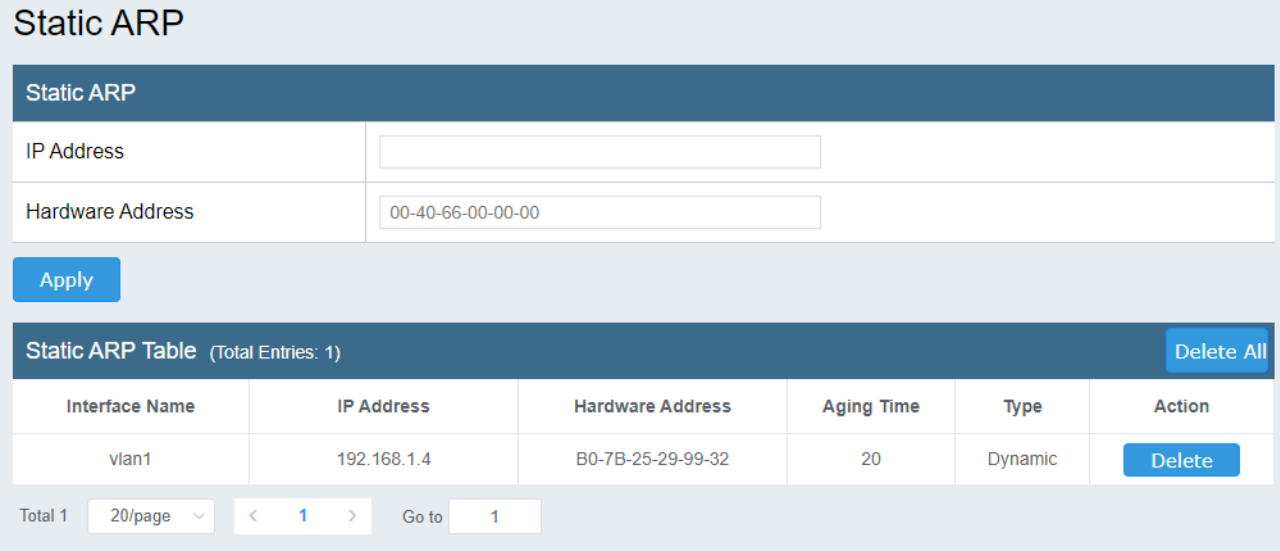
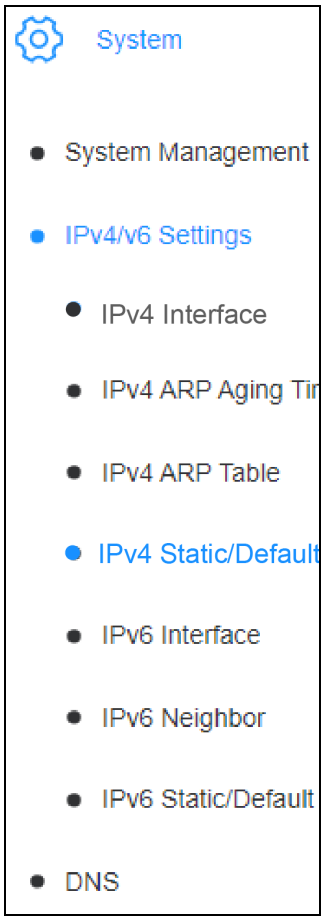


Figure 26. Static ARP Window

Note
You cannot edit an entry. To change an entry, you must delete it and reenter it.

Managing IPv4 Static/Default Route Addresses



Static routes are routes that you enter manually into the switch. Static routes are useful in designating a default route, which the switch uses if it does not have a route to a specific packet destination. Static routes are also useful in setting up multiple networks or subnets, where you define multiple routes for a particular interface, usually a LAN port.

To manage IPv4 static routes:

1. Select **System** > **IPv4/v6 Settings** > **IPv4 Static/ Default Route** from the menu. The IPv4 Static/ Default Route window is shown in Figure 23 on page 73.

2. Configure the parameters in Table 23.

Table 23. IPv4 Static/Default Route Window

Field	Description
IP Address	Enter the IPv4 of the default static route.
Default Route check box	Check this box if the IP address is the default route. Remove the check mark if it is not the default route.
Mask	Enter the subnet mask of the IP address.
Next Hop IP Address	Enter the IPv4 of the next hop.

3. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

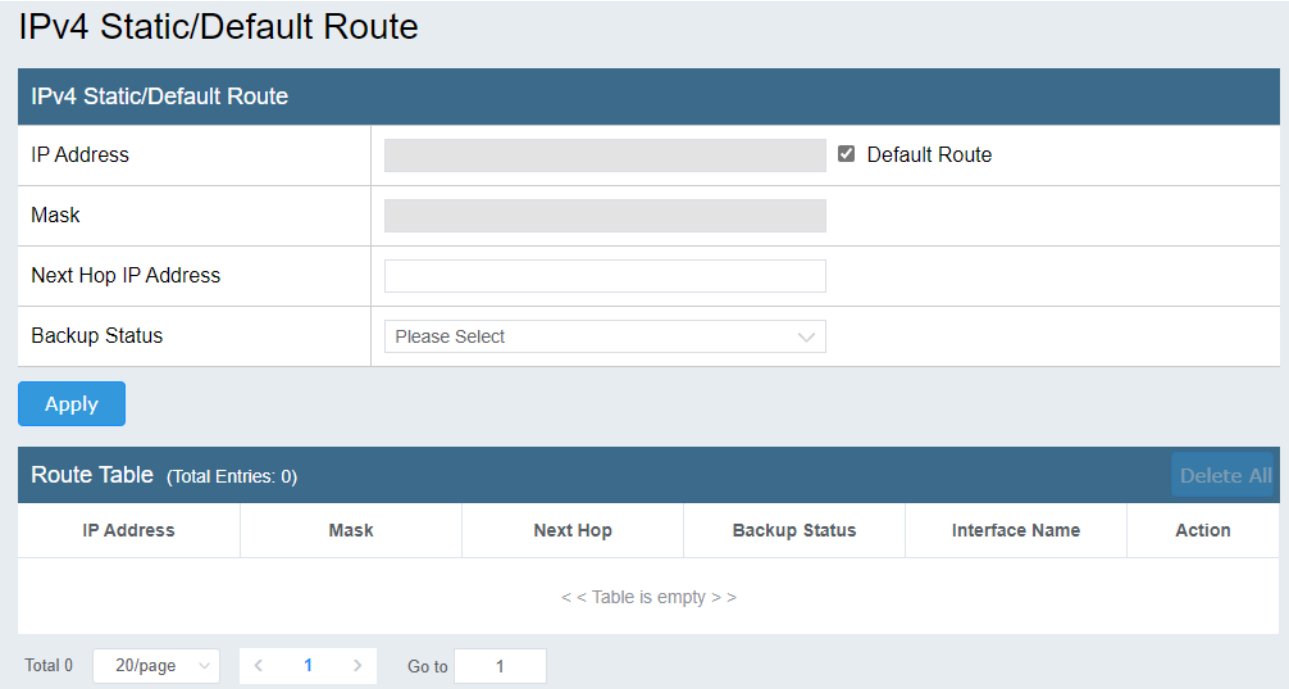
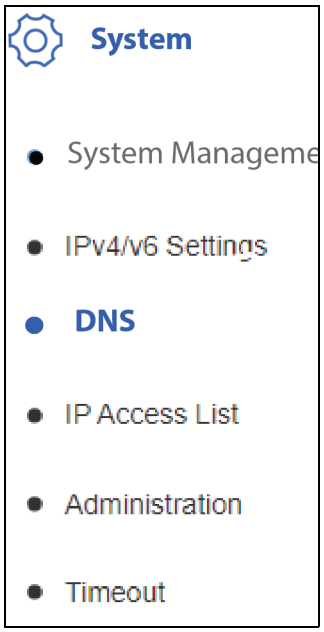


Figure 27. IPv4 Static/Default Route Window

Managing DNS Server IPv4 and IPv6 Addresses



The switch cannot resolve hostname requests itself. It needs the IP address of either an IPv4 or iPv6 hostname server where it can direct requests for resolution. To set the IPv4 or IPv6 address of a hostname server:

1. Select **System** > **DNS** from the menu. The **DNS Server Setting** window is shown in Figure 28.
2. Configure the parameters in Table 24.
3. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

Table 24. DNS Server Settings Window

Field	Description
DNS IPv4 Server	Enter the IPv4 address of the DNS server. You can enter only one IPv4 address.
DNS IPv6 Server	Enter the IPv6 address of the DNS server. You can enter only one IPv6 address.

Figure 28. DNS Server Settings Window

Chapter 5

Management IPv6 Addresses

This chapter contains the following sections:

- “IPv6 Address Overview” on page 82
- “Managing Static and Dynamic IPv6 Addresses” on page 83
- “Setting the IPv6 Neighbor Settings” on page 87
- “Assigning Static IPv6 Addresses” on page 89

IPv6 Address Overview

The sections in this chapter explain how to assign IPv6 addresses to the VLANs on the switch. The IPv6 addresses can be static addresses that you assign yourself or dynamic addresses from a DHCP IPv6 server on the network. The switch uses IPv6 addresses to support the following management functions:

- Web browser management
- Command line management with a Telnet or Secure Shell client
- Syslog server
- RADIUS authentication
- TACACS+ authentication
- RMON
- SNMPv1, v2c, or v3
- HTTP software updates
- TFTP software updates
- Ping tests

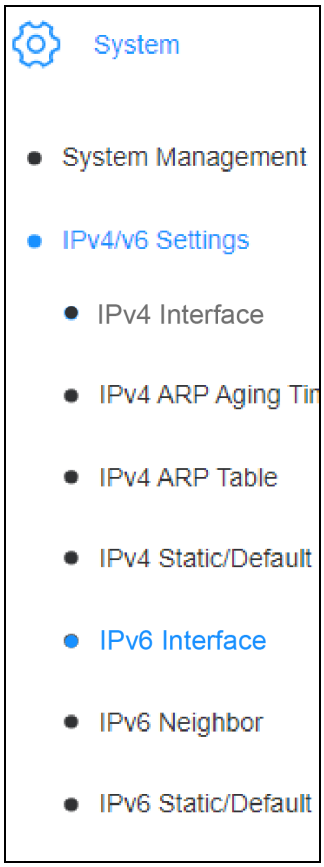
Note
The switch does not have a default IPv6 address configuration.

Here are the basic steps to assigning IPv6 addresses to the VLANs on the switch:

1. Add the VLANs. For instructions, refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.
2. Designate the VLANs as IPv6 interfaces. Refer to “Managing Static and Dynamic IPv6 Addresses” on page 83.
3. Add the IPv6 addresses to the VLANs. Refer to “Managing Static and Dynamic IPv6 Addresses” on page 83. A VLAN can have more than one address.

Note
In its default configuration the switch has no IPv6 interfaces or IPv6 addresses.

Managing Static and Dynamic IPv6 Addresses



To designate VLANs as IPv6 interfaces and add or modify IPv6 addresses on the interfaces for management functions:

1. Select **System** > **IPv4/IPv6 Settings** > **IPv6 Interface** from the menu. The IPv6 Interface window is shown in Figure 29 on page 85. The Interface Table portion of the window lists VLANs that are already designated as IPv6 interfaces on the switch. Review the following:
   - ❒ A VLAN has to exist on the switch before you can designate it as an IPv6 interface. For instructions, refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.
   - ❒ A VLAN has to be designated as an IPv6 interface before you can assign it an IPv6 address. The next step explains how to designate VLANs as IPv6 interfaces.
2. To designate a VLAN as an IPv6 interface, enter its VLAN ID in the **Interface VLAN** field and click **Add**. You can enter only one VLAN ID at a time. (If you do not know the VLAN ID, refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.). The switch adds the VLAN to the Interface Table.
3. To add or modify an IPv6 address on an IPv6 interface, click its **Detail** button in the Interface Table. (If you cannot find the VLAN in the Interface Table, enter its number in the **Interface VLAN** field and click **Find**.) You can configure only one IPv6 interface at a time. The IPv6 Interface Configuration window is displayed. Refer to Figure 30 on page 86.
4. Configure the parameters in Table 25.
5. Click **Apply** for all adjusted parameter settings.

Note
Click **Save** in the menu to save your changes.

Table 25. IPv6 Interface Configuration Window

Field	Description
Status Settings	
Interface	Displays the name of the IPv6 interface as “VLAN*id”,* where “id” is the VLAN ID. The name cannot be change. To select a different VLAN, repeat this procedure.

Table 25. IPv6 Interface Configuration Window (Continued)

Field	Description
State	Select one of the following: - **Disabled**: Disables the IPv6 interface on the VLAN. This is the default setting. - **Enabled**: Enables the IPv6 interface.
IP Settings	
DHCPv6 Client State	Select one of the following: - **Disabled**: Disables the DHCPv6 client on the interface. Select this option to assign a static IPv6 address to the interface. This is the default setting. - **Enabled**: Enables the DHCPv6 client on the interface. Select this option to assign a dynamic IPv6 address from a DHCPv6 server to the interface.
Rapid Commit	Enables or disables the DHCPv6 Rapid Commit option (DHCPv6 option 14) on the interface. This feature can result in faster assignments of IPv6 addresses to clients by DHCPv6 servers. Note the following: - The option is disabled when there is no check mark in the check box. This is the default setting. - The DHCPv6 Client State must be enabled to activate Rapid Commit.

Table 25. IPv6 Interface Configuration Window (Continued)

Field	Description
IPv6 Address	Enter a static IPv6 address and prefix length for the IPv6 interface. The default is no address. The DHCPv6 Client State must be disabled to enter a static address. The address is entered in this format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/prefix Each x is a hexadecimal digit representing 4 bits. The eight groups of digits have to be separated by colons. Groups where all four digits are '0' can be omitted. Leading '0's in groups can also be omitted. As an example, the following IPv6 addresses are equivalent: 3710:421e:09a8:0000:0000:0000:00a4:1c50/56 3710:421e:9a8::a4:1c50/56 The switch permits only one unicast address per IPv6 interface.
NS Retransmit Time	
NS Interval	Specifies the amount of time in seconds that the client waits for a response to its Neighbor Solicitation before retransmitting the solicitation. The range is 1 to 3600 seconds. The default is 1 second.

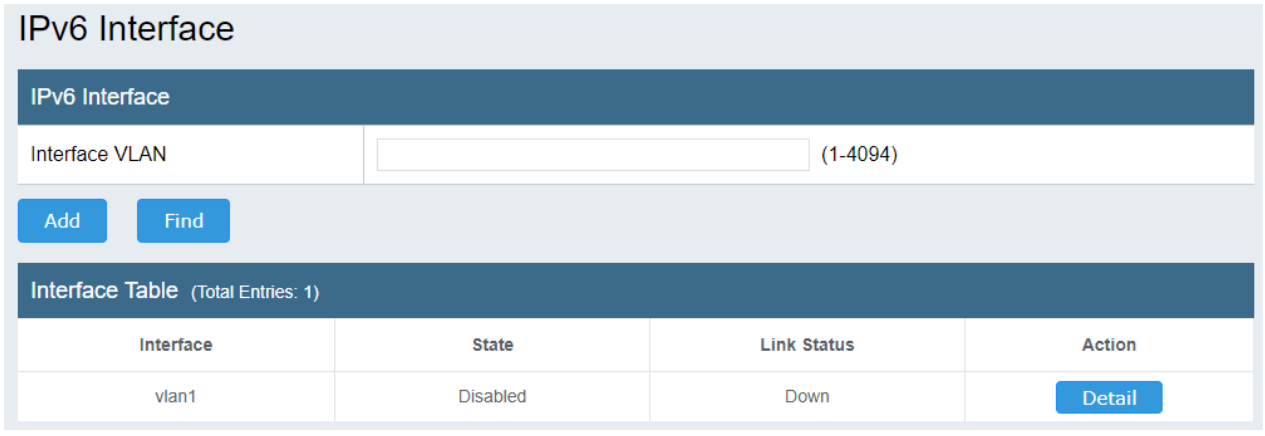


Figure 29. IPv6 Interface Window

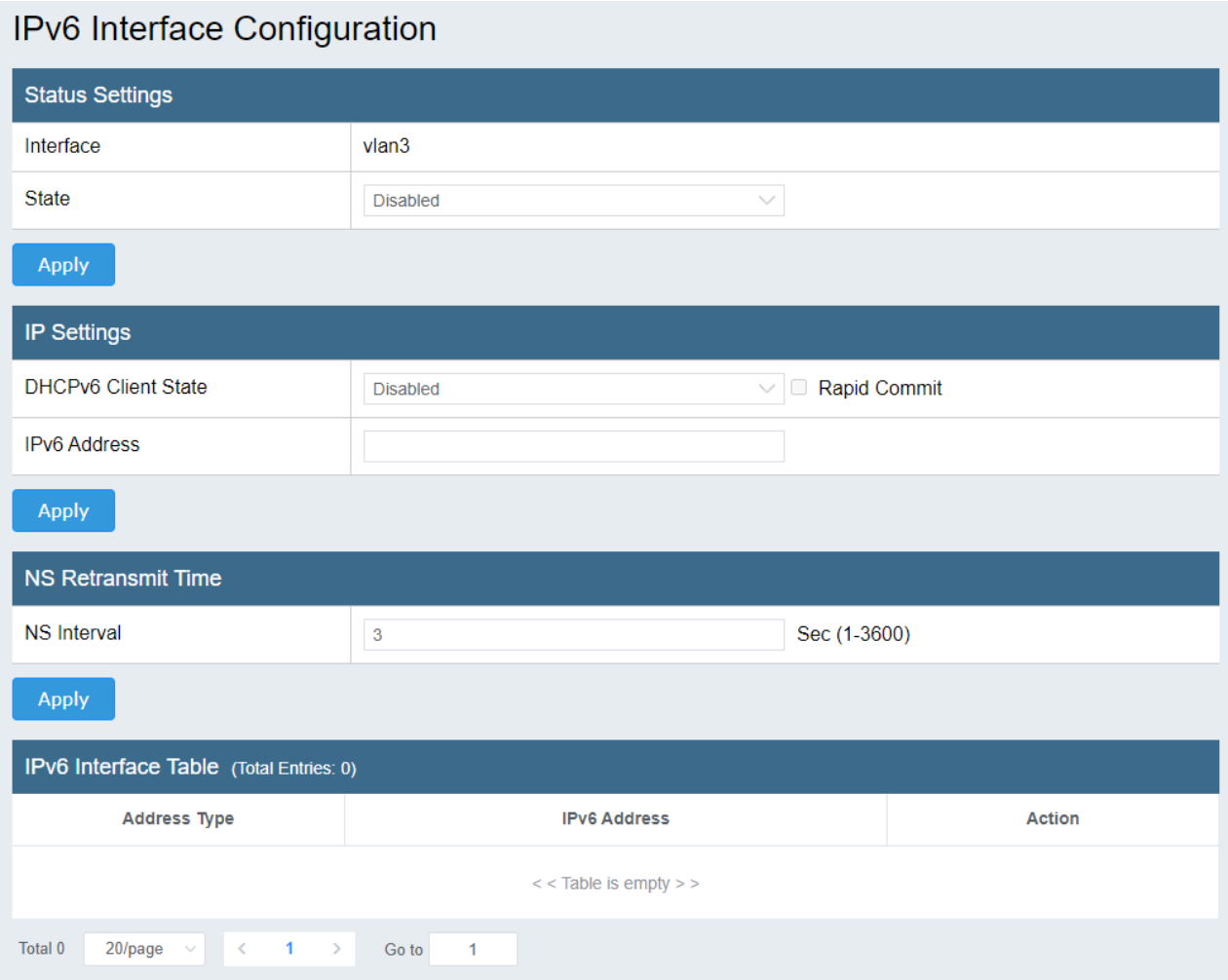
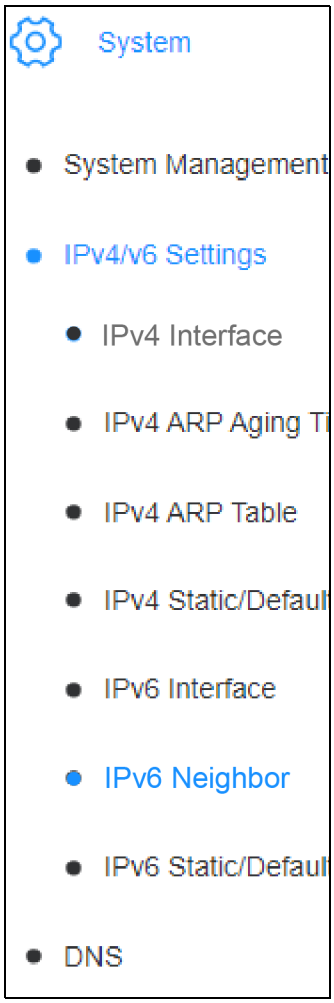


Figure 30. IPv6 Interface Configuration Window

Setting the IPv6 Neighbor Settings



To manage the list of IPv6 neighbors, select **System** > **IP Settings** > **IPv6 Neighbor** from the menu. The IPv6 Neighbor Settings window is shown in Figure 31 on page 88.

To add a new address, do the following:

1. Enter an IPv6 address in the **Neighbor IPv6 Address** field in this format:

   xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

   Each x is a hexadecimal digit representing 4 bits. The eight groups of digits have to be separated by colons. Groups where all four digits are '0' can be omitted. Leading '0's in groups can also be omitted. For example, the following IPv6 addresses are equivalent:

   3710:421e:09a8:0000:0000:0000:00a4:1c50

   3710:421e:9a8::a4:1c50

2. Enter a link layer MAC address in the **Link Layer MAC Address** field.
3. Click the **Add** button.

To delete addresses, do one of the following:

- ❒ To delete a single entry, click its **Delete** button in the Action column.
- ❒ To delete all the entries, select **All** from the Status drop-down menu and click the **Delete** button in the Action column.
- ❒ To delete all static entries, select **Static** from the Status drop-down menu and click the **Delete** button in the Action column.
- ❒ To delete all dynamic entries, select **Dynamic** from the Status drop-down menu and click the **Delete** button in the Action column.

To find an address in the table, do one of the following:

- ❒ To view all static or dynamic IPv6 neighbors, type asterisks in the **Neighbor IPv6 Address** and **Link Layer MAC Address** fields, then select **Static** or **Dynamic** from the Status drop-down menu.
- ❒ To find a neighbor by its IPv6 address, enter the neighbor address in the **Neighbor IPv6 Address** field and an asterisk in the **Link Layer MAC Address** field. The asterisk serves as a wildcard character.

- To find a specific IPv6 neighbor by its MAC address, enter an asterisk in the **Neighbor IPv6 Address** field and the MAC address in the **Link Layer MAC Address** field.
- To find an address by both its IPv6 address and MAC address, enter the values in the **Neighbor IPv6 Address** field and **Link Layer MAC Address** fields.

Note
Select **Save** from the menu to save your changes.

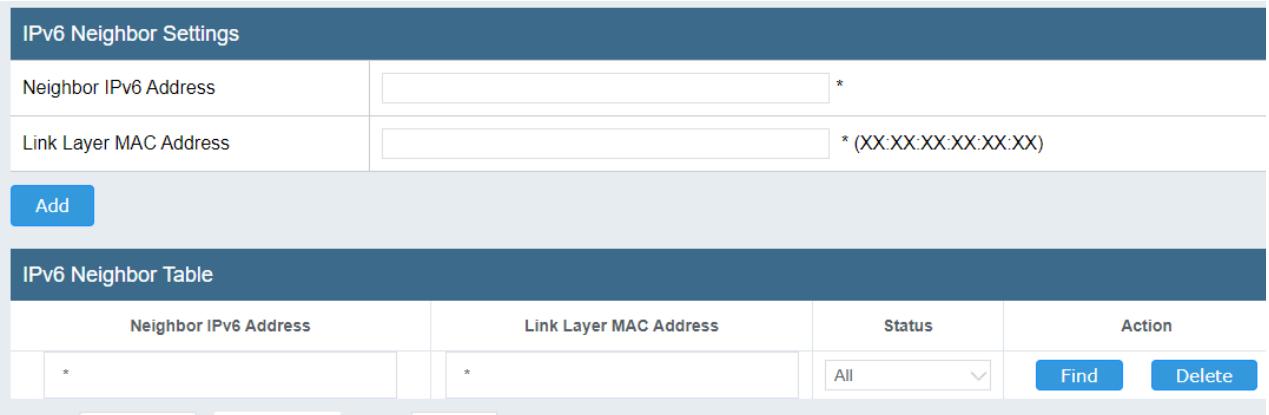
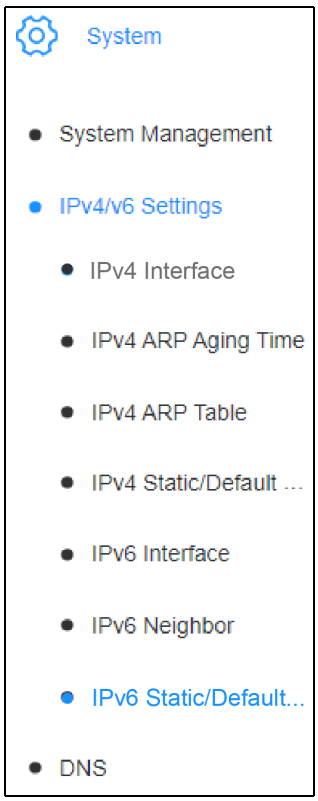


Figure 31. IPv6 Neighbor Settings Window

Assigning Static IPv6 Addresses

This section contains the procedure for assigning static IPv6 addresses to the VLANs on the switch to support management functions.

Note
VLANs to be assigned IPv6 addresses must already exist on the switch. For instructions, refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.



To assign a static IPv6 address to a VLAN on the switch:

1. Select **System** > **IPv4/v6 Settings** > **IPv6 Static/Default Router** from the menu. The IPv6 System Settings window is shown in Figure 32 on page 90.
2. Configure the settings in Table 26.
3. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

Note
Changing the switch’s iGS950 address will interrupt your management session if you are using the address to manage the switch. To resume managing the unit, start a new management session using the new IPv6 address or a different management IP address.

Table 26. IPv6 Router Window

Field	Description
IPv6 Address/Prefix Length	Enter a static IPv6 unicast address and prefix length for the switch. The default is no address. The address is entered in this format: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/prefix Each x is a hexadecimal digit representing 4 bits. The eight groups of digits have to be separated by colons. Groups where all four digits are '0' can be omitted. Leading '0's in groups can also be omitted. As an example, the following IPv6 addresses are equivalent: 3710:421e:09a8:0000:0000:0000:00a4:1c50/56 3710:421e:9a8::a4:1c50/56 If the DHCP IPv6 client is enabled on the switch, this field displays the IPv6 address assigned by the DHCP server.
Interface VLAN	Enter the VLAN ID of the VLAN to be assigned the new IPv6 address. You can specify only one VLAN ID.
Next Hop IPv6 Address	Enter the IPv6 address of the next hop.

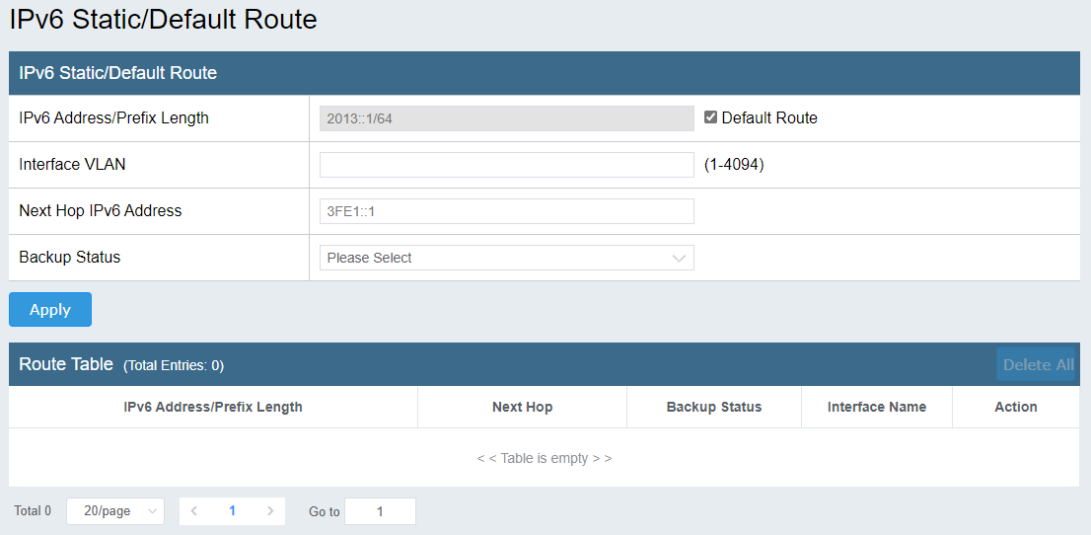


Figure 32. IPv6 System Settings Window

Chapter 6

System Time

This chapter contains the following sections:

- “Manually Setting the Date and Time” on page 92
- “Setting the Date and Time from an SNTP Server” on page 95

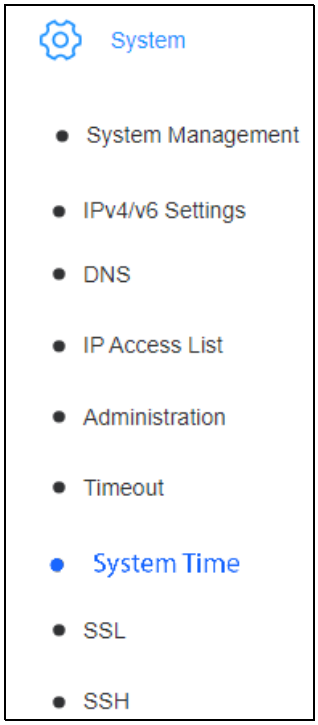
Manually Setting the Date and Time

The switch generates event messages when performing specific functions or after encountering network errors. The messages, which the switch tags with the times and dates so that you know when they occurred, can be useful in monitoring system operations and troubleshooting network problems.

The switch has an internal clock and calender that can be set two ways:

- ❒ You can manually set the clock and calender yourself.
- ❒ The switch can automatically obtain the time and date from a Network Time Protocol (NTP) server on your network or the internet.

Note
If the time and date are set manually, the switch maintains them with its internal battery when powered off.



To manually set the date and time or specify an NTP server:

1. Select **System** > **System Time** from the menu. The System Time window is shown in Figure 33 on page 94.
2. Configure the window fields in Table 27.
3. Click **Apply** to activate your changes.

Note
Click **Save** in the menu to save your changes.

Table 27. System Time Window

Field	Description
Current Time Settings	
Clock Mode	Displays either of the following: - Local Time: The switch uses its internal clock and calender to maintain its time and date. - SNTP: The switch uses an NTP server on the network or internet to set its time and date.
Current Time	Displays the switch's current date and time.
Time Zone	Displays its time zone, if required.

Table 27. System Time Window (Continued)

Field	Description
Date/Time Settings	
Clock Mode	Select one of the following: - **Local** - The switch uses its internal clock and calender to maintain its time and date.This is the default setting. - **NTP**: The switch uses an NTP server on the network or Internet to maintain its time and date
Local Time Settings (Local Setting)	
Date Settings	Enter the current year, month, and date.
Time Settings	Enter the current hour, minutes, and seconds. The hour is set in 24-hour format.
Addition Time Parameters Set these fields if the switch's location observes Daylight Savings Time.	
Time Zone	Select the time zone of the location of the switch.
Daylight Savings Time Status	Choose one of the following: - **Enabled**: Select this if the switch's location observes Daylight Savings Time. - **Disabled**: Select this if the switch's location does not observe Daylight Savings Time. This is the default setting.
From	Set the month, weekday, hour, and minute of the start of Daylight Savings Time.
To	Set the month, weekday, hour, and minute of the end of Daylight Savings Time.
DST Offset	Set the Daylight Savings Time offset from the menu. The choices are 1 hour, the default, and 30 minutes.

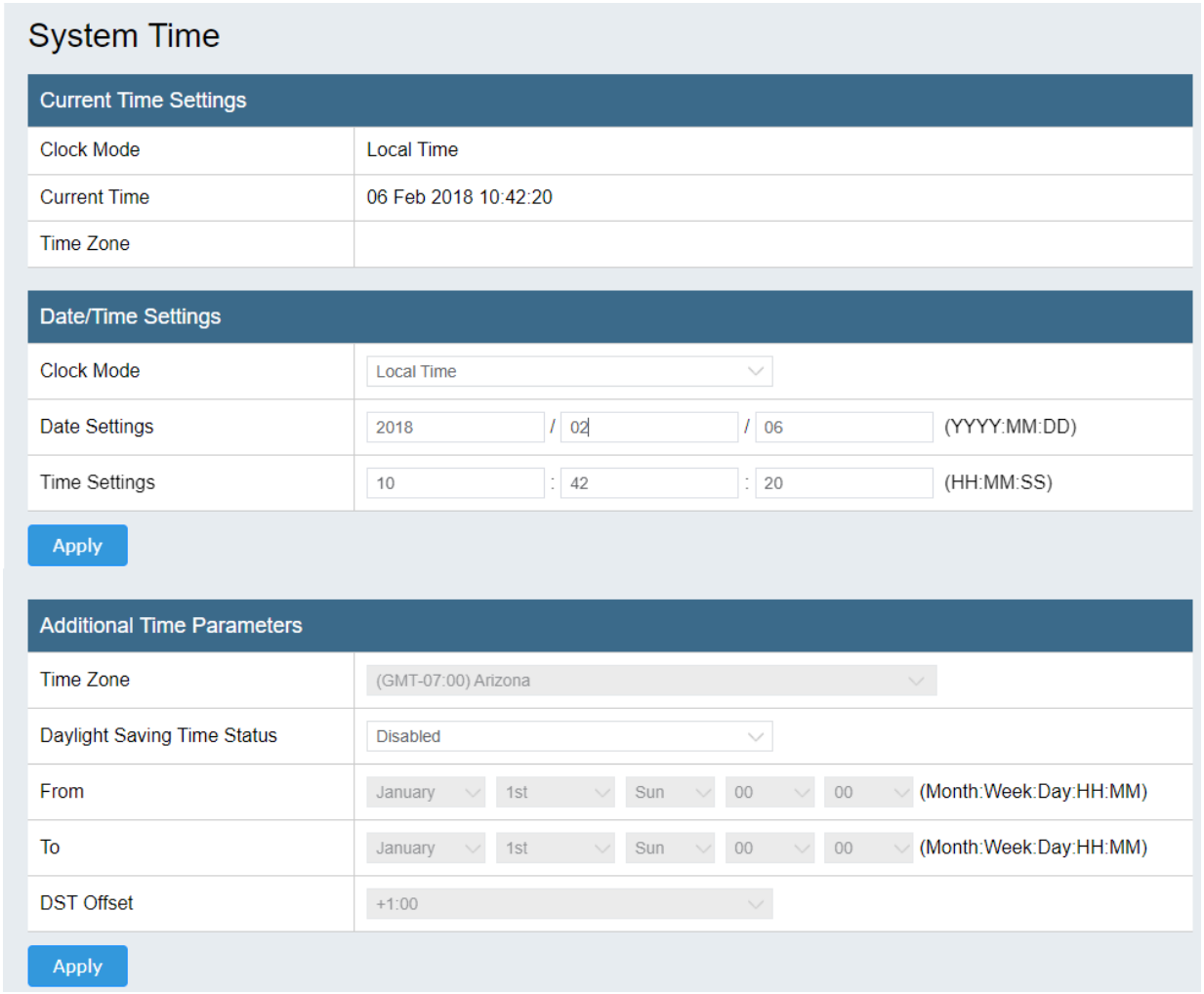
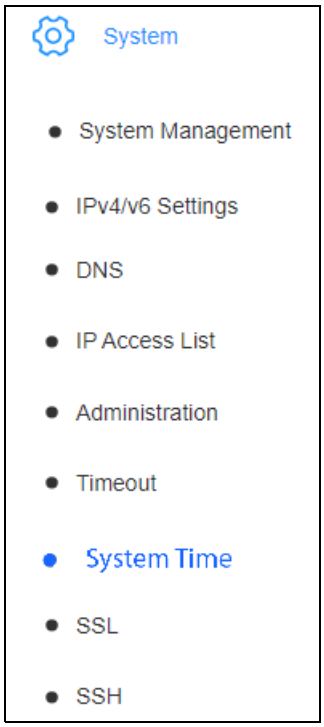


Figure 33. System Time Window

Setting the Date and Time from an SNTP Server



To configure the switch to set its date and time from an SNTP server on your network or the Internet:

1. Select **System** > **System Time** from the menu. The System Time window is shown in Figure 33 on page 94.
2. Configure the fields in Table 28.
3. Click the **Apply** button to activate your changes.

Note
Click **Save** in menu to save your changes.

Table 28. Setting the Calender and Clock from an NTP Server

Field	Description
Date/Time Settings	
Clock Mode	Set to **SNTP**.
Simple Network Time Protocol (SNTP) Settings	
SNTP Primary Server	Select **IPv4** or **IPv6** from the menu and enter the IP address of the primary SNTP server. The default is IPv4. This field is required. The format for an IPv4 address is shown here: nnn nnn nnn nnn Each N is a decimal number from 0 to 255. The format for an IPv6 address is shown here: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx Each x is a hexadecimal digit representing four bits. The eight groups of digits have to be separated by colons. Groups where all four digits are '0' can be omitted. Leading '0's in groups can also be omitted. As an example, the following IPv6 addresses are equivalent: 3710:421e:09a8:0000:0000:0000:00a4:1c50 3710:421e:9a8::a4:1c50

Table 28. Setting the Calender and Clock from an NTP Server (Continued)

Field	Description
SNTP Secondary Server	Select **IPv4** or **IPv6** from the menu and enter the IP address of a secondary SNTP server. The default is IPv4. This field is optional.
SNTP Poll Interval	Enter the number of minutes the switch waits to poll the NTP server. The range is 1 to 60 minutes. The default is 1 minute.
Time Zone	Select the time zone of the location of the switch from the pull-down menu.
Addition Time Parameters Set these fields if the location of the switch observes Daylight Savings Time.	
Daylight Savings Time Status	Select one of the following: - **Enabled**: Select this if the switch's location observes Daylight Savings Time. - **Disabled**: Select this if the switch's location does not observe Daylight Savings Time. This is the default setting.
From	Set the month, weekday, hour, and minute of the start of Daylight Savings Time.
To	Set the month, weekday, hour, and minute of the end of Daylight Savings Time.
DST Offset	Set the Daylight Savings Time offset from the menu. The choices are 1 hour, the default, and 30 minutes.

Chapter 7

Web Browser Management

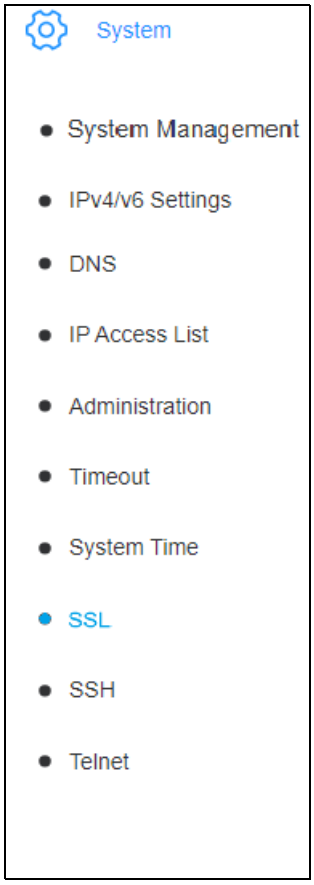
This chapter contains the following sections:

- “Selecting the Web Browser Mode” on page 98
- “Managing Web Browser Manager Accounts” on page 100
- “Setting the Timeout for Management Sessions” on page 102

Selecting the Web Browser Mode

The switch has a web browser server for remote management from your management workstation with a web browser. The server has two modes:

- HTTP
- HTTPS (SSL)



Although HTTP is the default active mode for the web server, it is not recommended that you use it to manage the switch because it is not secure. The packets exchanged by the switch and your workstation during HTTP management sessions are transmitted in plain text. This makes them vulnerable to snooping from network intruders and may compromise the security of the switch and your network. In contrast, HTTPS management sessions are secure because the transmitted packets are encrypted.

Here are the guidelines:

- The default active mode is HTTP.
- Both HTTP and HTTPS cannot be active on the switch at the same time.
- Changing the web server mode interrupts your management session. You will have to log on again.
- If you enable the HTTPS (SSL) mode, remember to include the prefix “HTTPS://” in the URL field of your web browser when specifying the IP address of the switch at the start of your management sessions.

To enable or disable HTTP or HTTPS on the switch:

1. Select **System** > **SSL** from the menu. The SSL Settings window is shown in Figure 34 on page 99.
2. Select one of the following options:
   - **Enabled**: Enables the SSL mode for encrypted HTTPS management sessions, and disables non-secure HTTP management.
   - **Disabled**: Disables the SSL mode and HTTPS management, and activates non-secure HTTP management. This is the default setting.
3. Click **Apply**. The switch displays a confirmation prompt.
4. Click **OK** to implement the change or **Cancel** to cancel the change.

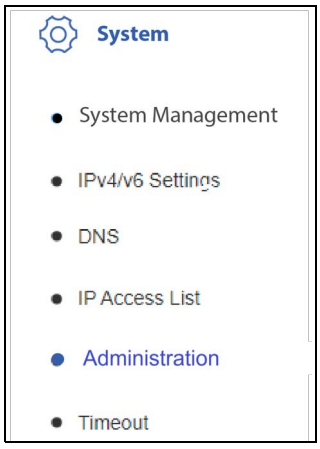
Note
If you click OK, your management session is interrupted.

5. To resume managing the switch, start a new management session. When specifying the IP address of the switch in the URL field of the web browser, include the prefix “HTTPS://” if you enabled SSL or “HTTP://” if you disabled it.

Note
Select **Save** from the menu to save your changes.

Figure 34. SSL Settings

Managing Web Browser Manager Accounts



You must have a user name and password of a manager account to log on and manage the switch. The switch has one default manager account, with the user name “manager” and default password “friend”. If more than one manager will be managing the switch, you can add more accounts so that the administrators do not have to share the same account.

To set the authentication method and add or delete local manager accounts:

1. Select **System** > **Administrator** from the menu. The Administration window is shown in Figure 35 on page 101.

2. To add a new local manager account, do the following:

   a. Enter a user name in the **User Name** field. Here are the guidelines.

   - ❒ The name is case sensitive.
   - ❒ It can be up to 20 characters.
   - ❒ Spaces and special characters are not recommended.

   b. Enter a password for the manager account in the **Password** field. The password has the same guidelines as the user name.

   c. Confirm the password by entering it again in the **Confirm Password** field.

   d. Click **Add**.

   e. Go to step 6.

3. To modify the password of a local manager account, do the following:

   a. Click **Modify** of the account to be changed. You can modify only one account at a time.

   The switch displays the Modify Administration window in Figure 36 on page 101.

   b. Change the password of the account.

   You cannot change the entry numbers or user names of accounts.

   c. Go to step 6.

4. To delete a local account, do one of the following:

   - ❒ To delete a specific account, click **Delete** in the Action column.
   - ❒ To delete all the accounts, click **Delete All**.

   You cannot delete the default manager account. Your management session is not interrupted if you delete the account you are currently using to manage the switch.

Note
Select **Save** from the menu to save your changes.

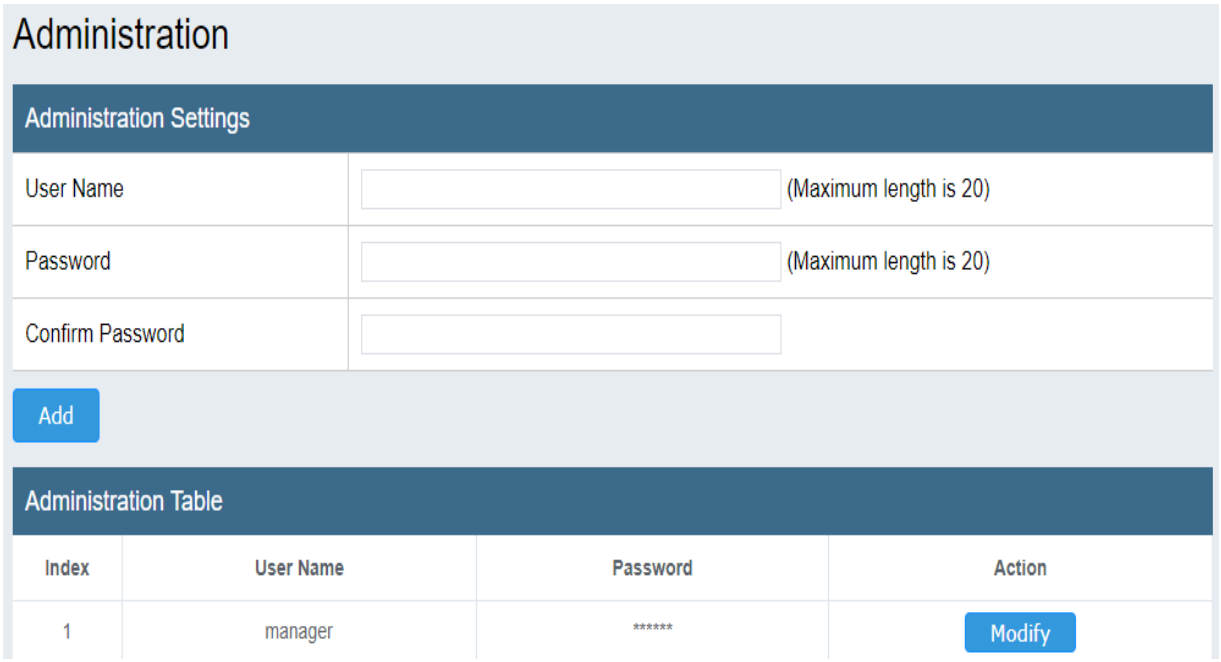


Figure 35. Administration Window

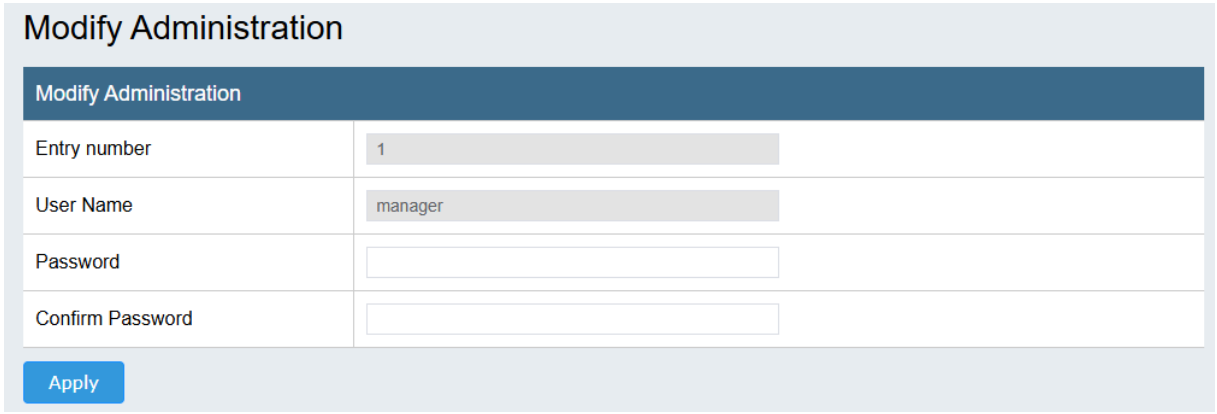
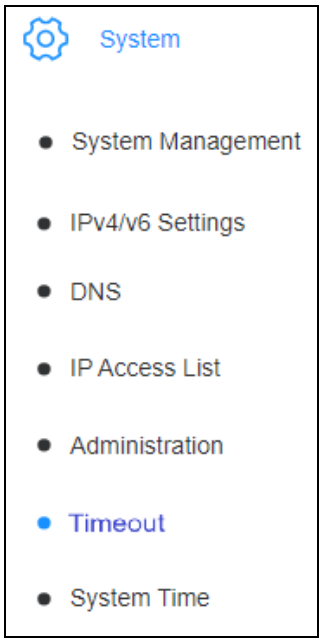


Figure 36. Modify Administration Window

Setting the Timeout for Management Sessions



The switch has a timeout value for inactive management sessions. The timeout value is the maximum amount of time the switch waits before automatically ending inactive web browser management sessions.

To configure the timeout for web browser management sessions:

1. Select **System** > **Timeout** from the menu. The Timeout Settings window is shown in Figure 37.
2. In the **Web Idle Timeout** field, enter the new timeout value for inactive web browser management sessions. The range is 3 to 60 minutes. The default is 10 minutes.
3. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

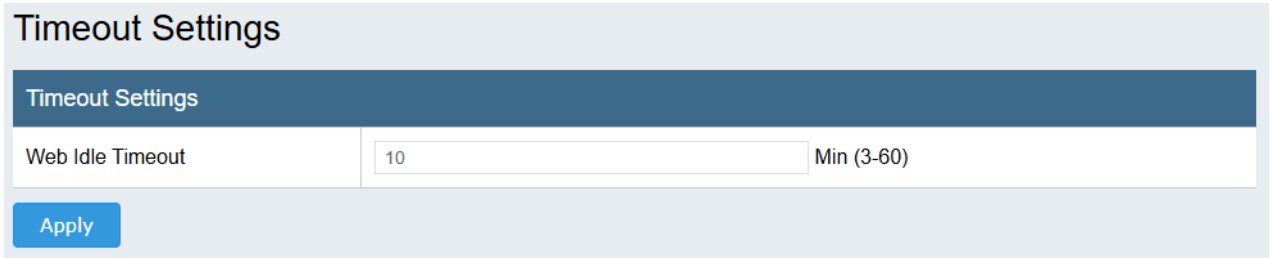


Figure 37. Timeout Settings Window

Chapter 8

Secure Shell and Telnet Servers

This chapter contains the following sections:

- “Introduction” on page 104
- “Enabling or Disabling the SSH Server” on page 105
- “Configuring the Telnet Server” on page 106

Introduction

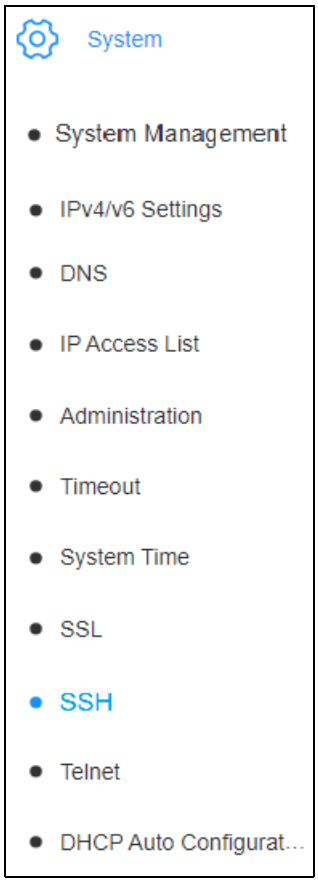
The switch has two management interfaces. The primary interface is the web browser interface. You can configure all the features and functions of the switch from the web browser interface.

The switch also has a command line management interface that has a series of commands you enter at a command line prompt. You can configure only a limited number of features of the switch with the command line interface.

You can access the command line interface with either Telnet or Secure Shell (SSH). You need to have a Telnet or SSH client on your management workstation. SSH is recommended because it protects your management sessions from snooping by encrypting the packets. In contrast, management sessions conducted with Telnet are conducted in clear text, meaning packets are not encrypted, leaving your switch and network vulnerable to network intruders. The default settings are the Telnet server is enabled and the SSH server is disabled.

Note
You cannot disable the Telnet server on the switch.

Enabling or Disabling the SSH Server



To enable or disable the SSH server:

1. Select **System** > **SSH** from the menu. The SSH Settings window is shown in Figure 38 on page 105.
2. Configure the settings in Table 29.

Table 29. SSH Settings Window

State	Description
SSH Status	Select one of the following: - **Enabled**: Enables the SSH server. - **Disabled**: Disables the SSH server. This is the default setting.
Port	Enter the SSH protocol port number. The range is 1 to 65535. The default is 22.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

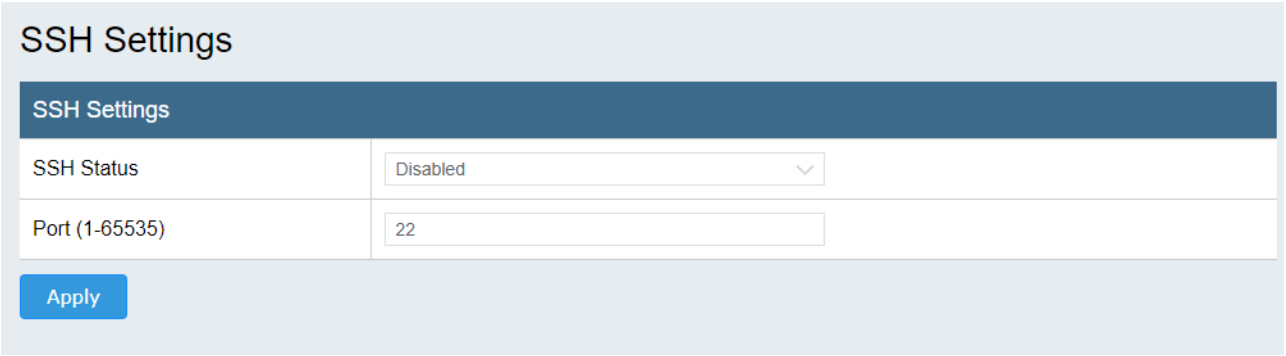


Figure 38. SSH Settings Window

Configuring the Telnet Server

The switch has a Telnet server for remote management with a Telnet client. These instructions explains how to enable or disable the Telnet server. When the server is enabled, you can configure the switch with the command line interface using a Telnet client.

To enable or disable the Telnet server:

1. Select **System** > **Telnet** from the menu. The Telnet Settings window is shown in Figure 39 on page 106.
2. Configure the settings in Table 30.
3. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

Table 30. Telnet Settings Window

State	Description
Telnet Status	Select one of the following from the pull-down menu: - **Enabled**: Enables the Telnet server. This is the default setting. - **Disabled**: Disables the Telnet server.
Port (1-65535)	Enter the Telnet protocol port number. The range is 1 to 65535. The default is 23.

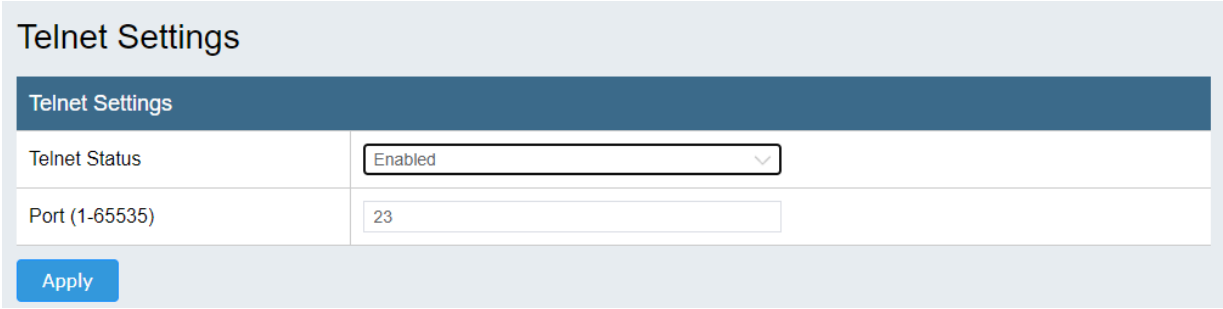
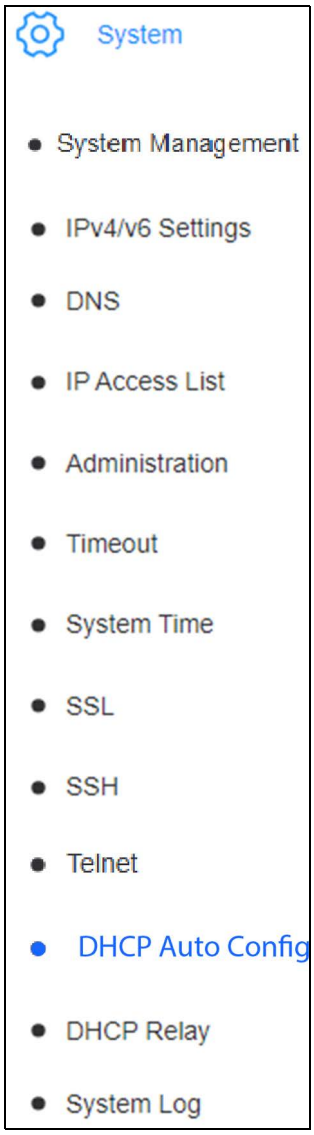


Figure 39. Telnet Settings Window

Chapter 9

DHCP Auto Configuration

Description and Procedure



The switch stores its parameter settings in a configuration file in flash memory, which it updates with the latest settings whenever you select the Save option in the menu. It is good network practice to maintain backup copies of the configuration files on a server on your network, so that you can restore the files to the devices or to configure replacement devices, if needed. Refer to “Backing Up Configuration Files from the Switch with HTTP” on page 535 or “Backing Up Configuration Files from the Switch with TFTP” on page 537.

The switch has a DHCP auto configuration feature that can make adding or replacing switches easier. With DHCP auto configuration, the switch automatically obtains its configuration file from a DHCP server, along with its IP address, when booted or powered on. Here are the guidelines:

- ❒ You have to enable the DHCP client on the switch. Refer to Chapter 4, “Management IPv4 Addresses” on page 71 or Chapter 5, “Management IPv6 Addresses” on page 81.
- ❒ The DHCP server has to support option 54 (server address). Use the option to specify the IP address of a TFTP server.
- ❒ The DHCP server also has to support option 67 (filename). Use this option to specify the filename of the configuration file for the switch.
- ❒ The TFTP and DHCP servers have to reside on the same device.
- ❒ The switch configuration files have to reside on the DHCP server.

To enable or disable DHCP auto configuration:

1. Select **System** > **DHCP Auto Configuration** from the menu. The DHCP Auto Config window is shown in Figure 40 on page 108.
2. Select one of the following options from the pull-down menu and click **Apply**.
   - ❒ **Enabled**: Enables the feature. The switch queries the DHCP server for both its IP address and configuration file the next time it is booted or powered on.
   - ❒ **Disabled**: Disables the feature. This is the default setting.

Note
Select **Save** from the menu to save your changes.

Review the following guidelines:

- If you enabled the feature and want the switch to obtain its configuration file from the DHCP server now, reboot the switch. Refer to “Rebooting the Switch” on page 541.
- After the switch obtains its configuration file from the DHCP server, you should disable the DHCP Auto Configuration feature. That way, any additional configuration changes you make to the switch will not be overwritten by the configuration file on the DHCP server the next time you reboot or power cycle the device.

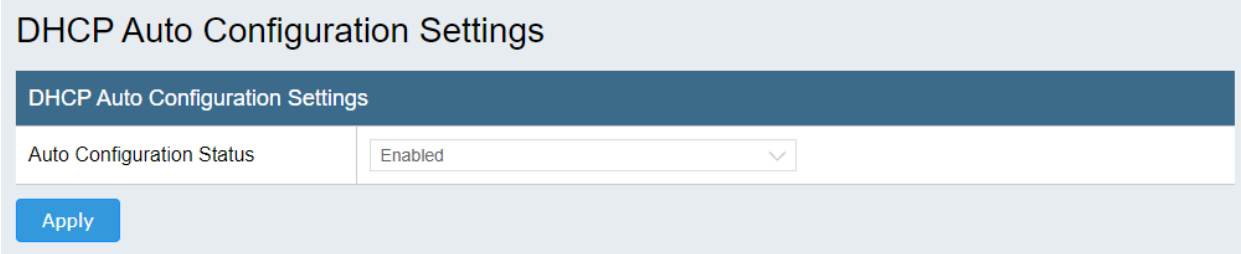


Figure 40. DHCP Auto Configuration Window

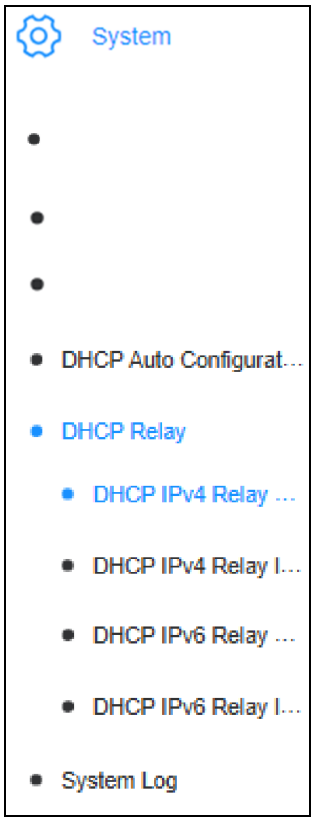
Chapter 10

DHCP IPv4 Relay

This chapter contains the following sections:

- “DHCP IPv4 Relay Global Settings” on page 110
- “DHCP IPv4 Relay Interface Settings” on page 114

DHCP IPv4 Relay Global Settings



The switches in the iGS950 Series feature DHCP IPv4 relay agents that forward BOOTP and DHCP messages between DHCP servers and IPv4 clients. Relay agents are required when DHCP servers and their clients reside on different IP subnets. The switch's DHCP relay agent can relay BOOTREQUEST messages, which are messages from clients to a DHCP server, and BOOTREPLY messages, which are responses from the DHCP server.

To configure the DHCP IPv4 relay agent:

1. Select **System** > **DHCP Relay** > **DHCP IPv4 Relay Global Settings**. The switch displays the DHCP IPv4 Relay Global Settings window. Refer to Figure 41 on page 113.
2. Configure the settings in Table 31.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 31. DHCP IPv4 Relay Global Settings Window

Setting	Description
State	Enables or disables the DHCP relay agent. The settings are: - Enabled: Enables the agent. - Disabled: Disables the agent. This is the default setting.
Hop Count Limit	Controls whether the switch forwards or discards ingress DHCP messages, based on their hop count. The hop count is the number of hops (routers) that messages pass through to reach the switch. The switch discards ingress DHCP messages that exceed the hop count limit. The range is 1 to 16 hops. The default is 4 hops. For example, at the default, the switch discards ingress DHCP messages that have passed through five or more routers.

Table 31. DHCP IPv4 Relay Global Settings Window (Continued)

Setting	Description
Time Threshold	Enter the maximum length of existence, in seconds, of ingress BOOTP messages. The switch uses this parameter to determine whether to forward or discard ingress BOOTP messages. The switch discards ingress BOOTP messages whose timestamps exceed the defined value. The range is 0 to 65535 seconds. The default value is 0, which disables the time threshold.
Port List	Enter the ports on the switch with IPv4 clients of the DHCP server. The ports can be identified individually (e.g., 1,4,7), as ranges (1-5,19-24), or both (e.g., 1-12,15,18).
VLAN Settings State	Enter the VLAN IDs of tagged VLANs with ports connected to clients and servers of the DHCP relay agent. Refer to “Viewing All 802.1Q Tagged VLANs” on page 352.
Agent Information Option 82 State	Specify whether the DHCP relay agent on the switch is to insert additional Option 82 information into the DHCP packets that it forwards from DHCP clients to the DHCP server. Examples of the information may include: - Identification information about the relay agent. - Client’s connection to the switch. Possible settings are: - Enabled: The DHCP relay agent inserts additional information into the DHCP packets. - Disabled: The DHCP relay agent does not insert additional information into the DHCP packets. This is the default setting.

Table 31. DHCP IPv4 Relay Global Settings Window (Continued)

Setting	Description
Agent Information Option 82 Check	Specify whether the switch is to check the validity of Option 82 fields in ingress packets from clients. The settings are: - Enabled: The switch checks the validity of Option 82 fields and drops their packets if it determines the fields are invalid or contain errors. - Disabled: The DHCP relay agent does not check the validity of ingress packets for Option 82 fields. This is the default setting. Although clients themselves do not insert Option 82 fields when transmitting DHCP messages, it is possible for DHCP requests received by the switch from clients to contain Option 82 fields. The two possible scenarios are listed here: - The fields are being added by a trusted device, such as a DHCP snooping switch, that exists between clients and the switch. - A malicious device adds bogus Option 82 fields to client packets. This option can be used to screen for and block packets from the latter
Agent Information Option 82 Policy	Specify the action of the switch when the following two conditions are met: - Option 82 Check is set to Disabled. - Ingress packets from clients already contain Option 82 fields. Available settings are: - Replace: The switch replaces the Option 82 fields in packets from DHCP clients. This is the default value. - Drop: The switch deletes the Option 82 fields. - Keep: The switch retains the Option 82 fields. As mentioned previously, it is possible for ingress packets from clients to contain Option 82 fields. This option determines the action of the switch in handling those Option 82 fields.

Table 31. DHCP IPv4 Relay Global Settings Window (Continued)

Setting	Description
Agent Information Option 82 Remote ID	Description or other identifier of the switch that inserts the Option 82 information into the relayed DHCP messages from clients to the server. Possible settings are: - Default: The MAC address of the switch. - User Define: A description of up to 32 alphanumeric characters. The description can include special characters and spaces.

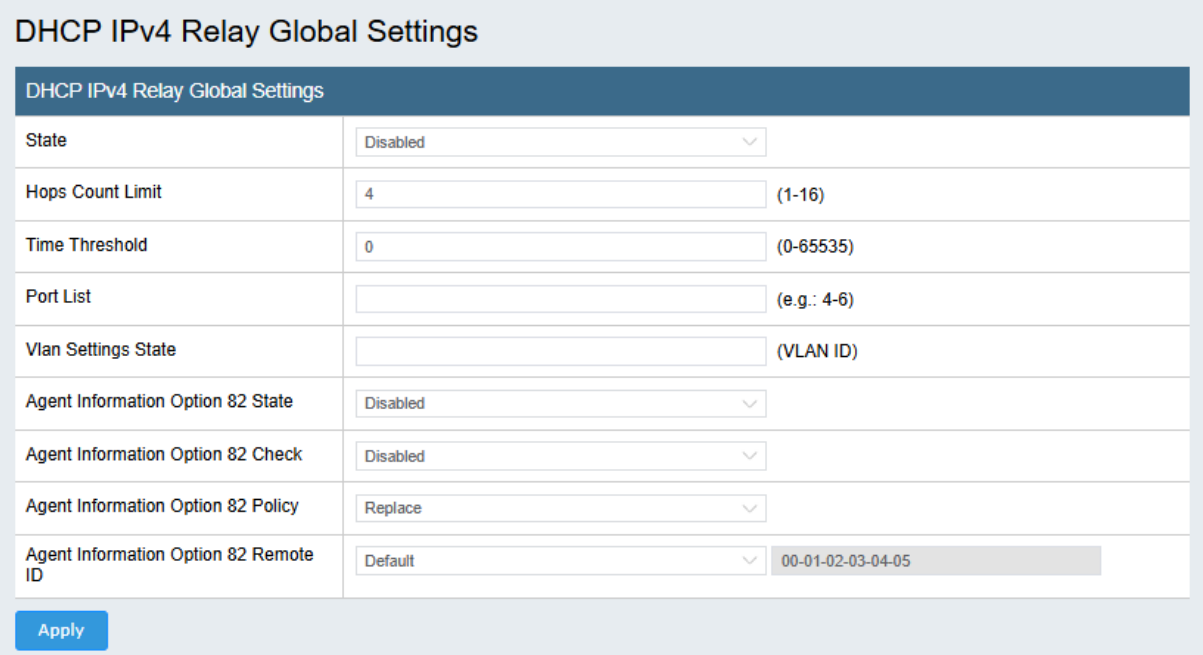
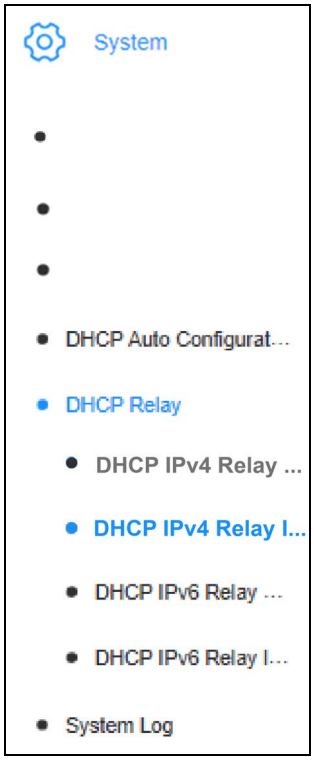


Figure 41. DHCP IPv4 Relay Global Settings Window

DHCP IPv4 Relay Interface Settings

Adding IPv4 Addresses of DHCP Servers



This procedure adds the IPv4 addresses of DHCP servers to the switch for the DHCP relay agent. To add server IPv4 addresses:

1. Select **System** > **DHCP Relay** > **DHCP IPv4 Relay Interface Settings**. The switch displays the DHCP IPv4 Relay Interface Settings window. Refer to Figure 42.

   Note
   The Interface System parameter cannot be changed.

2. In the **Server IP** field, enter the IPv4 address of a DHCP server. You can enter only one address at a time. The switch supports a maximum of four IP addresses.

3. Click **Apply**. The address is added to the DHCP IPv4 Relay Interface Table.

   Note
   Select **Save** from the menu to save your changes.

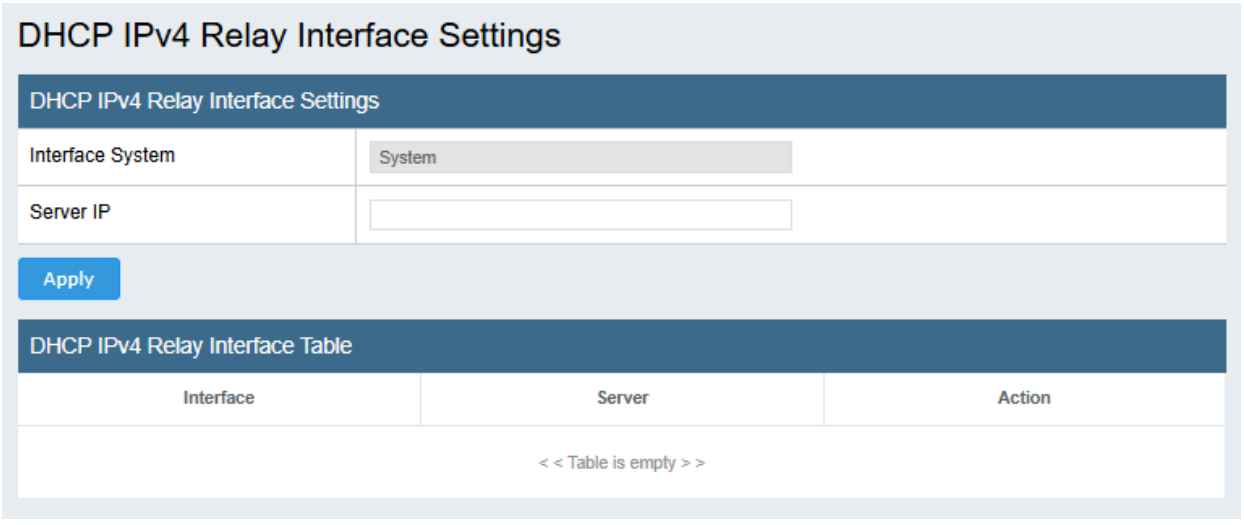


Figure 42. DHCP IPv4 Relay Interface Settings

Editing IPv4 Addresses of DHCP Servers

You cannot edit the IPv4 addresses of DHCP servers. To change an address, you must delete it and reenter it.

Deleting IPv4 Addresses of DHCP Servers

To delete IPv4 addresses of DHCP servers:

1. Select **System** > **DHCP Relay** > **DHCP IPv4 Relay Interface Settings**. The switch displays the DHCP IPv4 Relay Interface Settings window. Refer to Figure 42 on page 114.

2. In the Action column of the DHCP IPv4 Relay Interface Table, click the **Delete** button of the address you want to delete. The switch deletes the address. The switch immediately stops forwarding DHCP requests from client to the address.

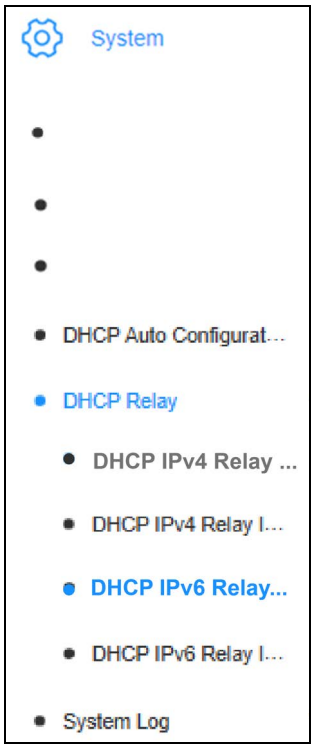
Chapter 11

DHCP IPv6 Relay

This chapter contains the following sections:

- “DHCP IPv6 Relay Global Settings” on page 118
- “DHCP IPv6 Relay Interface Settings” on page 121

DHCP IPv6 Relay Global Settings



The switches in the iGS950 Series feature DHCP IPv6 relay agents for forwarding DHCP messages between DHCP servers and IPv6 clients in networks where the servers and clients reside on different IP subnets.

To configure the DHCP IPv6 relay agent:

1. Select **System** > **DHCP Relay** > **DHCP IPv6 Relay Global Settings**. The switch displays the DHCP IPv6 Relay Global Settings window. Refer to Figure 43 on page 120.
2. Configure the settings in Table 32.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 32. DHCP IPv6 Relay Global Settings Window

Setting	Description
State	Enables or disables the DHCP IPv6 relay agent. The settings are: - Enabled: Enables the agent. - Disabled: Disables the agent. This is the default setting.
Hop Count Limit	Controls whether the switch forwards or discards ingress DHCP messages, based on their hop count. The hop count is the number of hops (routers) that the messages pass through to reach the switch. The switch discards ingress DHCP messages that exceed the hop count limit. The range is 1 to 32 hops. The default is 4 hops. For example, at the default value the switch discards ingress DHCP messages that have passed through five or more routers.

Table 32. DHCP IPv6 Relay Global Settings Window (Continued)

Setting	Description
Option 37 State	Controls whether the DHCP relay agent on the switch inserts Option 37 information into the DHCP packets that it forwards from DHCP clients to the DHCP server. Examples of the information are: - Identification information about the relay agent. - Client's connection to the switch. Possible settings are: - Enabled: The DHCP relay agent inserts information into the DHCP packets. - Disabled: The DHCP relay agent does not insert information into DHCP packets. This is the default setting.
Option 37 Check	Specify whether the switch is to check the validity of Option 37 fields in ingress packets. The settings are: - Enabled: The switch checks the validity of Option 37 fields and drops their packets if it determines the fields are invalid or contain errors. - Disabled: The DHCP relay agent does not check the validity of ingress packets for Option 82 fields. This is the default setting. Although clients themselves do not insert Option 37 fields when transmitting DHCP messages, it is possible for DHCP requests received by the switch from clients to contain Option 37 fields. The two possible scenarios are listed here: - The fields are being added by a trusted device, such as a DHCP snooping switch, that exists between clients and the switch. - A malicious device adds bogus Option 37 fields to client packets. - This option can be used to screen for and block packets from the latter

Table 32. DHCP IPv6 Relay Global Settings Window (Continued)

Setting	Description
Option 37 Remote ID Type	Description or other identifier of the switch that inserts the Option 37 information into the relayed DHCP messages from clients to the server. Possible settings are: - Default: The MAC address of the switch. - CID with User Defined - User Define: A description of up to 32 alphanumeric characters. The description can include special characters and spaces.

Note
Select **Save** from the menu to save your changes.

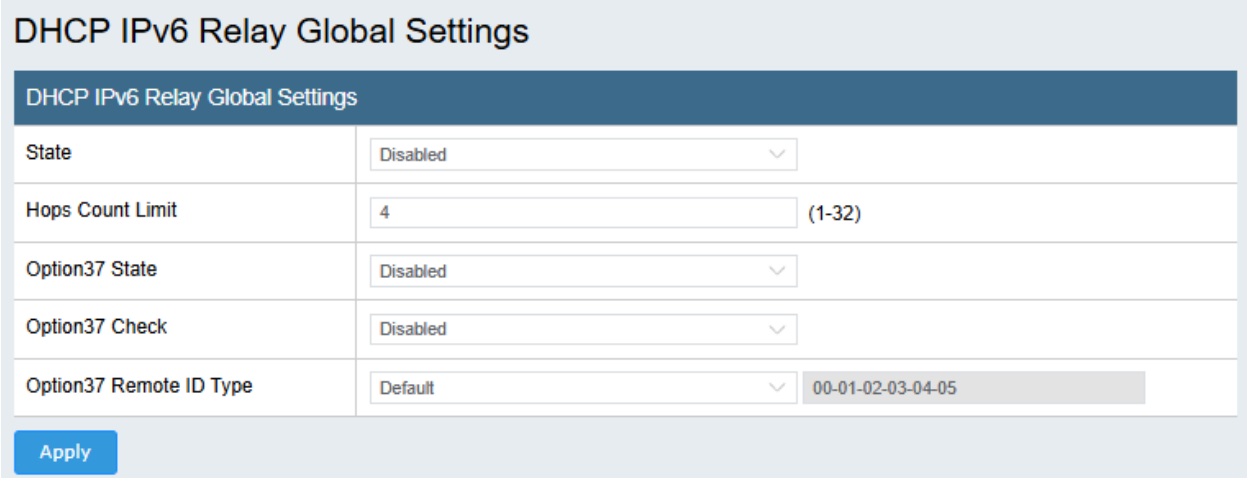
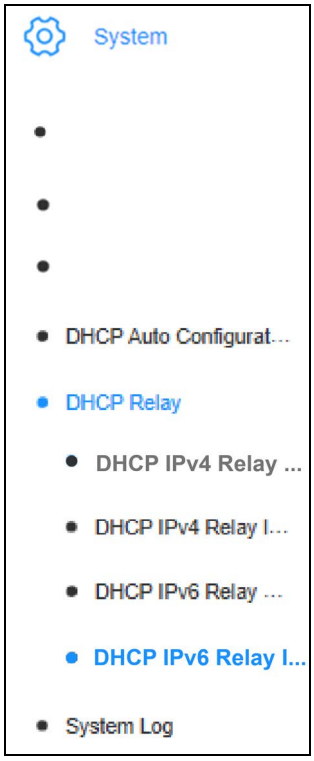


Figure 43. DHCP IPv6 Relay Global Settings

DHCP IPv6 Relay Interface Settings

Adding IPv6 Addresses of DHCP Servers



This procedure adds the IPv6 addresses of DHCP servers to the switch for the DHCP relay agent. To add server IPv6 addresses:

1. Select **System** > **DHCP Relay** > **DHCP IPv6 Relay Interface Settings**. The switch displays the DHCP IPv6 Relay Interface Settings window. Refer to Figure 44.

   Note
   The Interface System parameter cannot be changed.

2. In the **Server IP** field, enter the IPv6 address of a DHCP server. You can enter only one address at a time. The switch supports a maximum of four IP addresses.

3. Click **Apply**. The address is added to the DHCP IPv6 Relay Interface Table in the window.

   Note
   Select **Save** from the menu to save your changes.

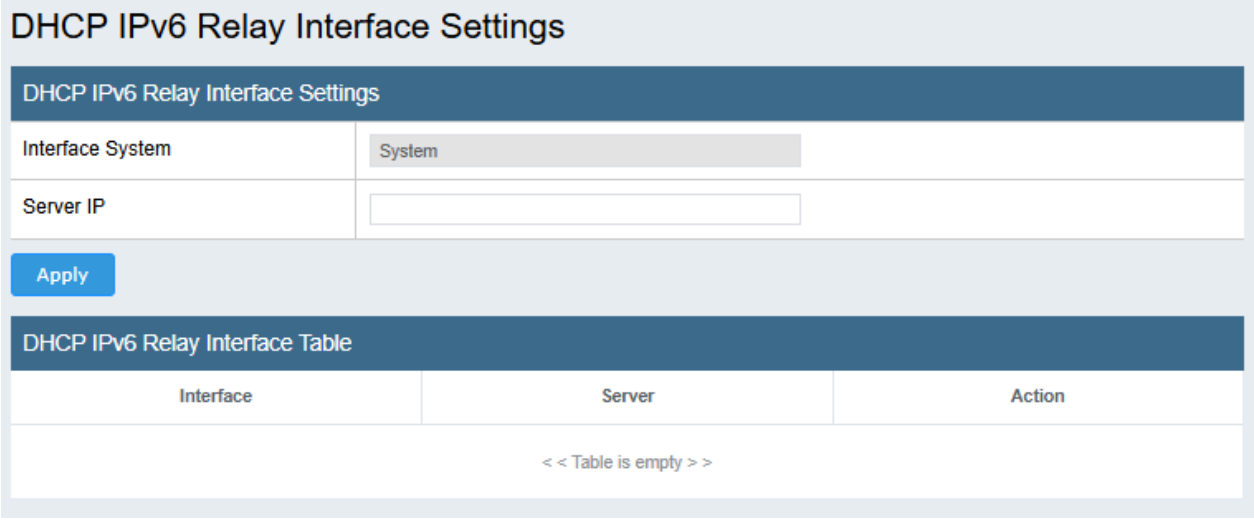


Figure 44. DHCP IPv6 Relay Interface Settings

Editing IPv6 Addresses of DHCP Servers

You cannot edit the IPv6 addresses of DHCP servers. To change an address, you must delete it and reenter it.

Deleting IPv6 Addresses of DHCP Servers

To delete IPv6 addresses of DHCP servers:

1. Select **System** > **DHCP Relay** > **DHCP IPv6 Relay Interface Settings**. The switch displays the DHCP IPv6 Relay Interface Settings window. Refer to Figure 44 on page 121.

2. In the Action column of the DHCP IPv6 Relay Interface Table, click the **Delete** button of the address you want to delete. The switch deletes the address. The switch immediately stops forwarding DHCP requests from client to the address.

Chapter 12

DHCP Server

This chapter describes the DHCP server:

- “Overview” on page 124
- “Configuring Global Settings” on page 125
- “Configuring DHCP IPv4 Pools” on page 127
- “Configuring DHCP Server Pool Options” on page 129
- “Configuring DHCP Server Hosts” on page 131
- “Displaying the DHCP Server Assigned Host Table” on page 133

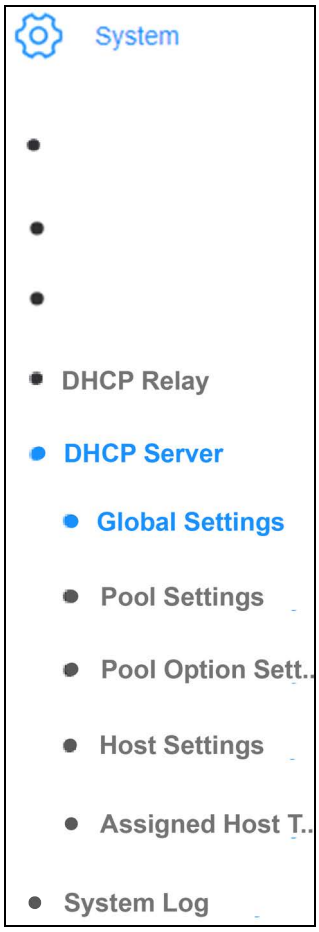
Overview

Dynamic Host Configuration Protocol (DHCP) is a standardized client/server network protocol that dynamically assigns IP addresses and other related configuration information to network devices. Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses for new computers or computers that are moved from one subnet to another must be configured manually.

The key thing to understand about DHCP is that it dynamically assigns IP addresses. This is in contrast with its alternative, static addressing. With static addressing, IP addresses are assigned manually to specific devices, and do not change over time as the device is used. Static addressing is typically used where the source address of the device must not change, for example, to access a service such as a printer server. With this in mind, DHCP allows reservations - these are static IP addresses within the DHCP scope that can be assigned to specific servers or devices and never given out to other devices.

DHCP provides an automated way to distribute and update IP addresses and other configuration information on a network. A DHCP server provides this information to a DHCP client through the exchange of a series of messages, known as the DHCP conversation or the DHCP transaction. If the DHCP server and DHCP clients are located on different subnets, a DHCP relay agent is used to facilitate the conversation. DHCP is based on BOOTP, and is defined in RFC 2131.

Configuring Global Settings



This procedure explains how to enable or disable the DHCP server on the switch, and enable or disable ICMP echo requests. The latter is used by the server to determine whether IPv4 addresses in an address pool are already being used in the network and, therefore, cannot be assigned to other devices.

To configure the status of the DHCP server and ICMP echo requests:

1. Select **System** > **DHCP Server** > **Global Settings**. The switch displays the DHCP Server Global Settings window in Figure 45 on page 126.
2. Configure the settings in Table 33.
3. Click **Apply** to activate your changes.

Note
Select **Save** in the menu to save your changes.

Table 33. DHCP Server Global Settings Window

Field or Column	Description
Status	Enables or disables the DHCP server on the switch. When the server is enabled, the switch listens for DHCP requests on all ports and assigns IPv4 addresses from its address pools to requesting hosts. Settings are: - **Enabled**: Enables the DHCP server. - **Disabled**: Disables the DHCP server. This is the default setting.
Icmp Echo Status	Enables or disables ICMP echo requests. ICMP echo requests consist of PINGs that the DHCP server transmits to determine if IP addresses are already being used by other hosts. Settings are: - **Enabled**: Enables ICMP echo requests. - **Disabled**: Disables ICMP echo requests. This is the default setting.

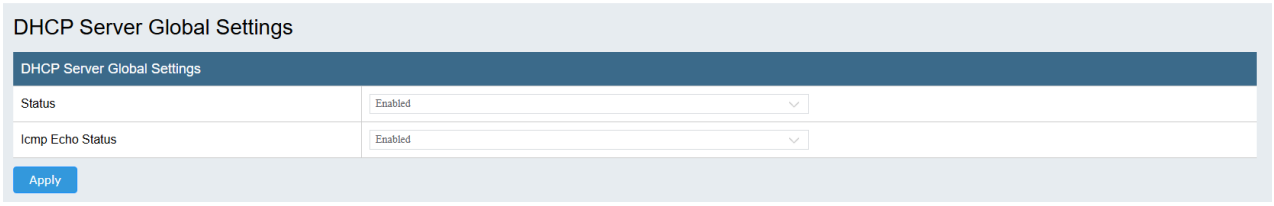
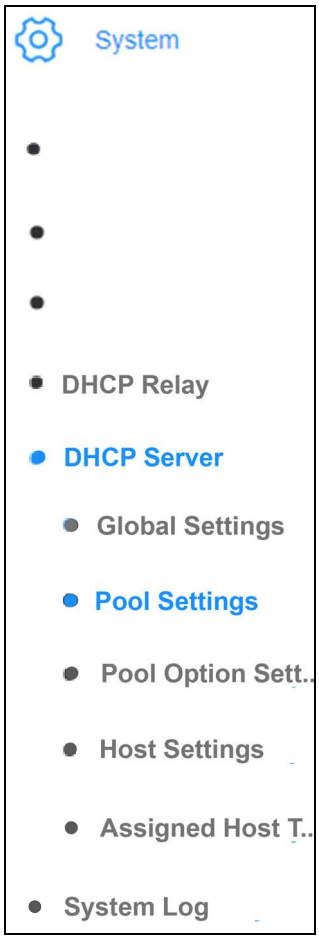


Figure 45. DHCP Server Global Settings

Configuring DHCP IPv4 Pools



This procedure explains how to add DHCP pools to the server. A pool defines a range of IPv4 addresses that the server can assign to clients in a network. A range consists of starting and ending IPv4 addresses and an IPv4 address mask.

To add, modify, or delete a DHCP IPv4 address pool:

1. Select **System** > **DHCP Server** > **Pool Settings**. The switch displays the DHCP Server Pool Settings window in Figure 46 on page 128. The window has two sections:
   - ❒ DHCP Server Pool Settings: Use this section to add new pools or modify existing pools.
   - ❒ DHCP Server Pool Table: Use this section to view the existing pools on the server. To modify a pool, click its **Modify** button. You can modify only one pool at a time, To delete a pool, click its **Delete** button.
2. To add or modify a pool, configure the settings in Table 34.

Table 34. DHCP Server Pool Settings Window

Field or Column	Description
Pool ID	Enter a unique, numerical ID for this DHCP pool. The range is 1 to 64.
Pool Name	Assign a name to the DHCP pool. The name can be up to twenty five alphanumeric characters. Spaces and special characters are not allowed.
Start IP	Enter the first IPv4 address in the address range for this DHCP pool.
End IP Address	Enter the last IPv4 address in the address range for this DHCP pool. If the range is to consist of a single IPv4 address, enter the same address for both the Start IP and End IP Address parameters.
Mask	Enter the IPv4 mask of the address range. A range can have only one mask.
Lease Time	Enter the time duration of the lease. The time is cumulative. The lease time is entered in seconds. The range is 1 to 2147483647 seconds (596K hours).

3. Click **Apply**. A new pool is immediately available.

Note
Select **Save** from the menu to save your changes

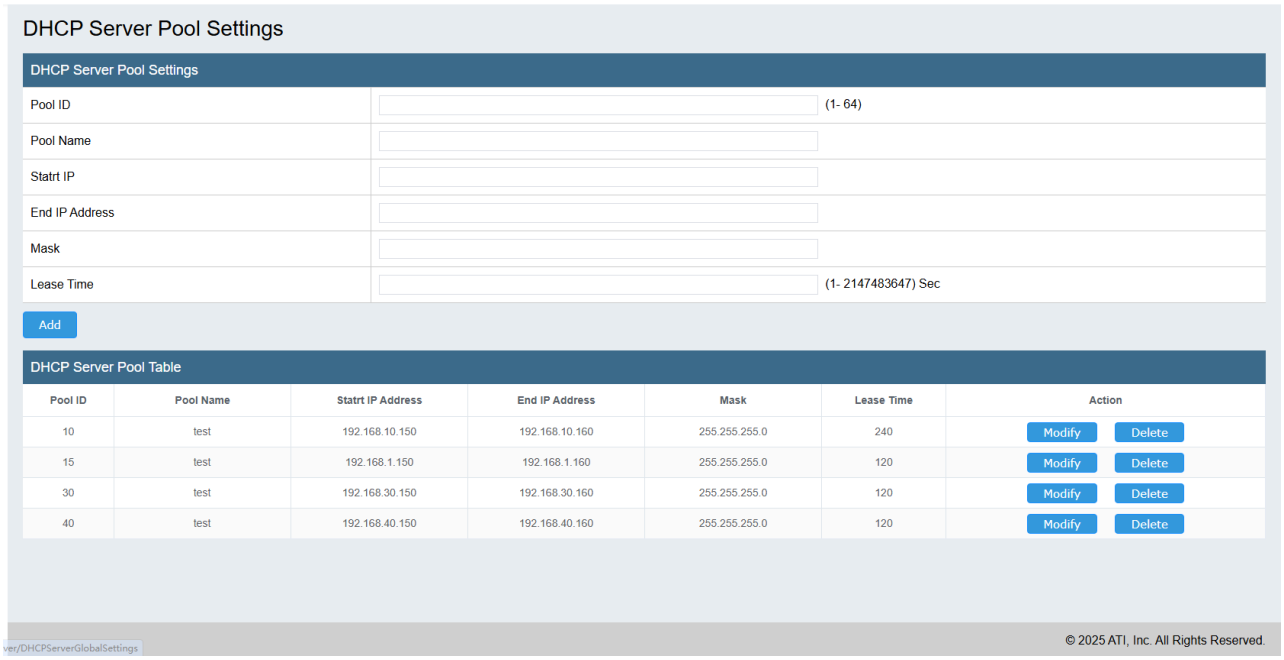
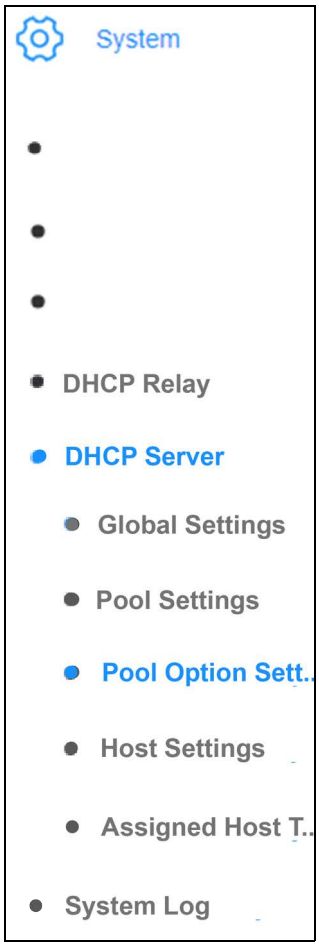


Figure 46. DHCP Server Pool Settings

Configuring DHCP Server Pool Options



The DHCP server can supply options to hosts that supply network information. Options are applied at the pool level. That is, all of the addresses in a pool share the same options.There are two categories of options: standard predefined options and user-defined options.

To configure or delete pool option settings:

1. Select **System** > **DHCP Server** > **Pool Option Settings**. The switch displays the DHCP Server Pool Options Settings window. Refer to Figure 47 on page 130. The window has two sections:
   - ❒ DHCP Server Pool Option Settings: Use this section to change pool option settings.
   - ❒ DHCP Server Pool Option Table: Use this section to view the existing pool option settings on the server. To delete a pool option settings, click its **Delete** button.
2. To add pool option settings, configure the settings in Table 35.

Table 35. DHCP Server Pool Option Settings Window

Field or Column	Description
Pool ID	Select the ID of an existing pool from the pull-down menu. You can configure only one pool at a time. To add a new pool or view the existing pools, refer to “Configuring DHCP IPv4 Pools” on page 127.
Option	Select a predefined option from the pull-down menu. The default is Time Offset (integer).
Option Code	Enter an option code. The range is 1 to 254. The default depends on the option.
Option Value	Enter an option value. The default is null.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

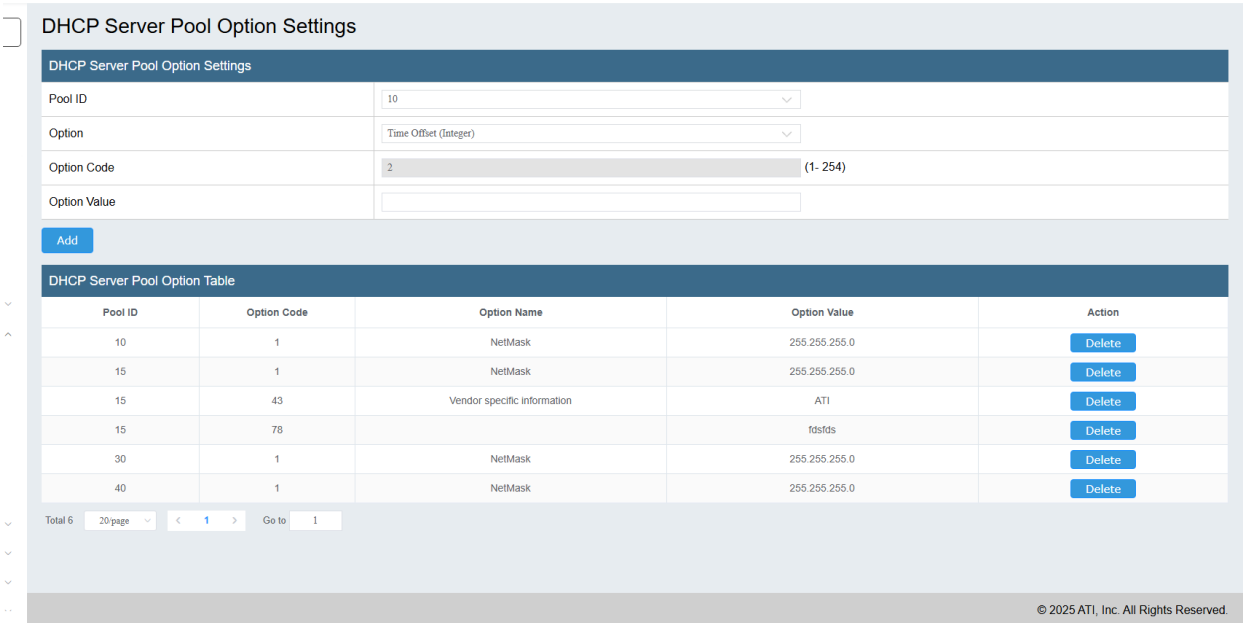
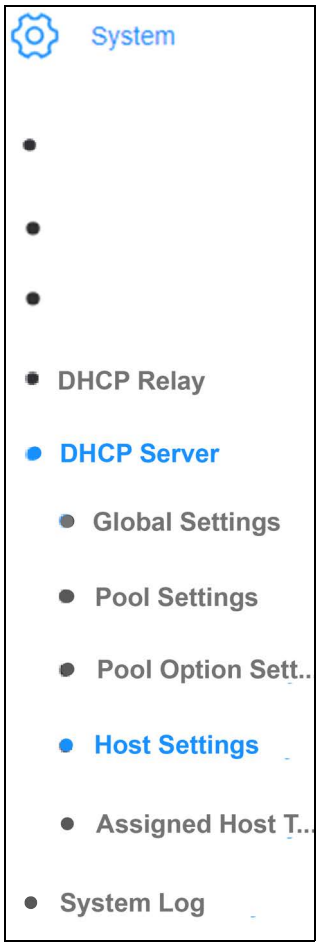


Figure 47. DHCP Server Pool Option Settings Window

Configuring DHCP Server Hosts



The DHCP server can assign the same IPv4 addresses to network devices whenever they query the server for an address. This feature is necessary for network devices that require the same address to function properly, such as file servers or network printers.

To assign a static IPv4 address in a pool in the DHCP server to a network device, or to view the current assignments:

1. Select **System** > **DHCP Server** > **Host Settings**. The switch displays the DHCP Server Host Settings window. Refer to Figure 48 on page 132. The window has two sections:
   - ❒ DHCP Server Host Settings: Use this section to add assignments of static addresses for hosts.
   - ❒ DHCP Server Host Table: Use this section to view the current static address assignments or to delete assignments. To delete a static address assignment, click its **Delete** button.
2. To add a static address assignment to a host, configure the settings in Table 36.

Table 36. DHCP Server Host Settings Window

Field or Column	Description
Pool ID	Enter the ID number of the pool containing the IPv4 address the server is to assign to the designated host as a static address. The pool must already exist. To add or view the available pools, refer to “Configuring DHCP IPv4 Pools” on page 127.
MAC Address	Enter the MAC address of the host to be assigned the designated address. You can enter only one MAC address.
IP Address	Enter the IPv4 address to be assigned the host by the server. The address must be a member of the designated pool in Pool ID. You can specify only one address.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

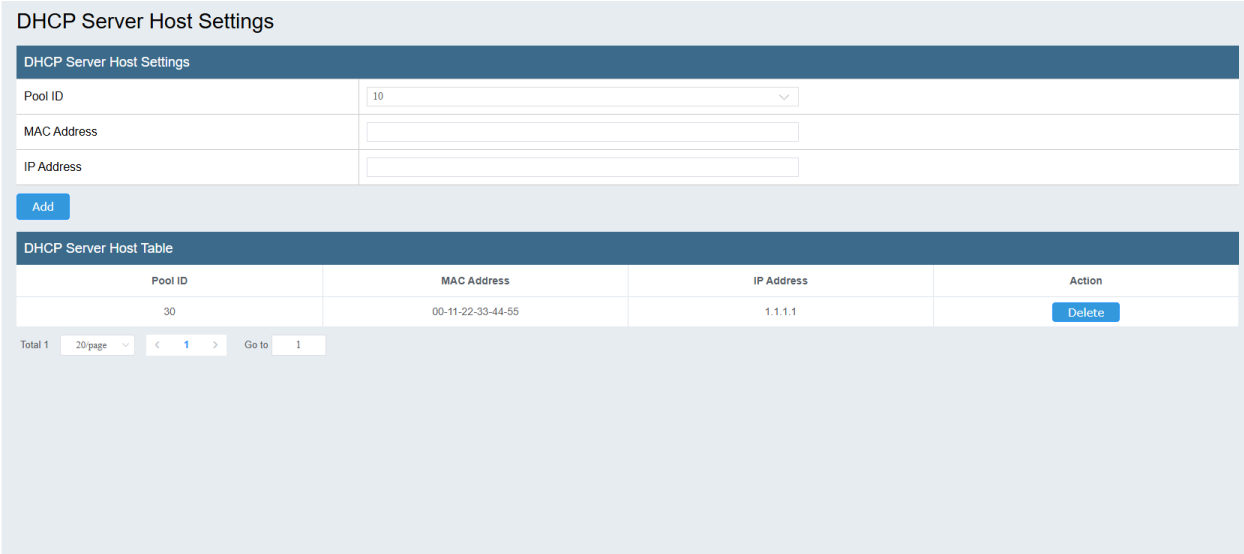
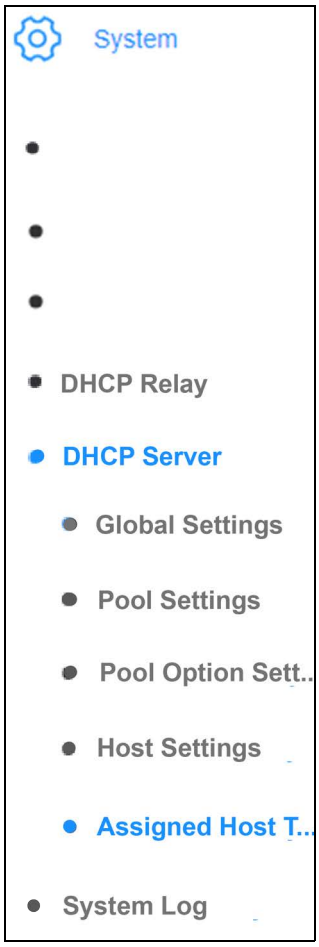


Figure 48. DHCP Server Host Settings

Displaying the DHCP Server Assigned Host Table



The DHCP server maintains a table that lists all the assigned IPv4 addresses and the corresponding hosts. To view the table, select **System** > **DHCP Server** > **Assigned Host Table**. The switch displays the DHCP Server Assigned Host Table window, shown in Figure 49. The columns in the window are defined in Table 37.

Table 37. DHCP Server Assigned Host Table Window

Column	Description
ID Address	Displays the IP address assigned to the host by the DHCP server.
MAC Address	Displays the MAC address of the host.
Allocate Method	Displays the category of the assigned IPv4 address. Categories include: - Dynamic: The IPv4 address was assigned randomly from the address pool that corresponds to the host's network, The host may receive the same or a different address the next time it queries the server for an address. - Static: The IPv4 address is always assigned to the same host. Refer to "Configuring DHCP Server Hosts" on page 131.
Expire Time (Sec)	Displays the amount of time in seconds the host has been assigned the IPv4 address.

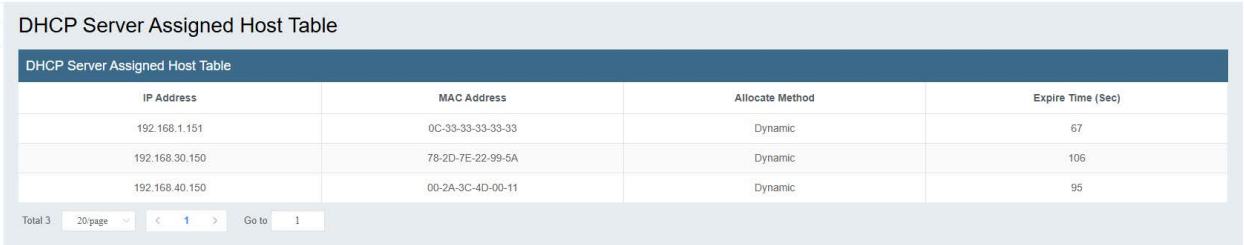


Figure 49. DHCP Server Assigned Host Table

Chapter 13

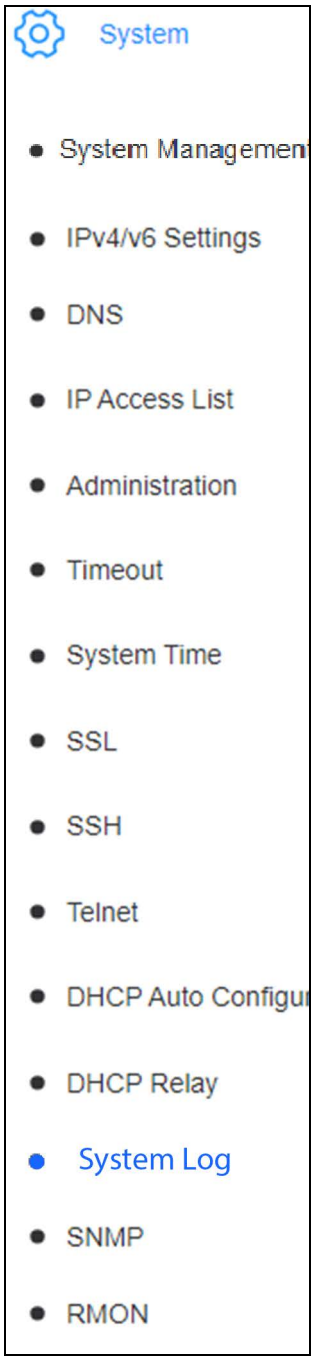
System Log and Syslog Client

This chapter contains the following sections:

- “Viewing the Event System Log” on page 136
- “Sending System Log Events to a Syslog Server” on page 138

Viewing the Event System Log

A managed switch is a complex piece of computer equipment that includes both hardware and software components. Multiple software features operate simultaneously, inter-operating with each other and processing large amounts of network traffic. It is often difficult to determine exactly what is happening when a switch appears not to be operating normally, or what happened when a problem occurred.



You can monitor the operations of the switch by viewing the event messages of by the device. The events and the vital information about system activity can help you identify and solve system problems.

The switch stores the events in an event log, in temporary memory. The events in the log are discarded whenever you reset or power cycle the switch.

To view the event log:

1. Select **System** > **System Log** from the menu. The System Log Settings window is shown in Figure 50 on page 137.

   The Syslog fields are described in “Sending System Log Events to a Syslog Server” on page 138.

   The window is static. The switch does not update the window. To view new events, click the Refresh button at the bottom of the window. Events have the following parts:

   - Index number
   - Facility number (local0)
   - Severity level
   - Date
   - Time
   - Description

   At the bottom of the window are the following buttons:

   - Clear - Clears all log events from the switch.
   - Refresh - Updates the window with the latest events.

2. To add or omit the time and date from event messages, select one of the following from Time Stamp:

   - **Enabled**: The switch adds the time and date to events. This is the default setting.
   - **Disabled**: The switch omits the time and date from event messages.

3. To set the limit on the number of events the log can store, select the Messages Buffered Size field. The range is 1 to 200 messages. The default is 50 messages. Once reaching its maximum capacity, the log deletes the oldest messages as it stores new messages.

4. Click **Apply** to activate your changes.

Note
Select **Save** from the menu to save your changes.

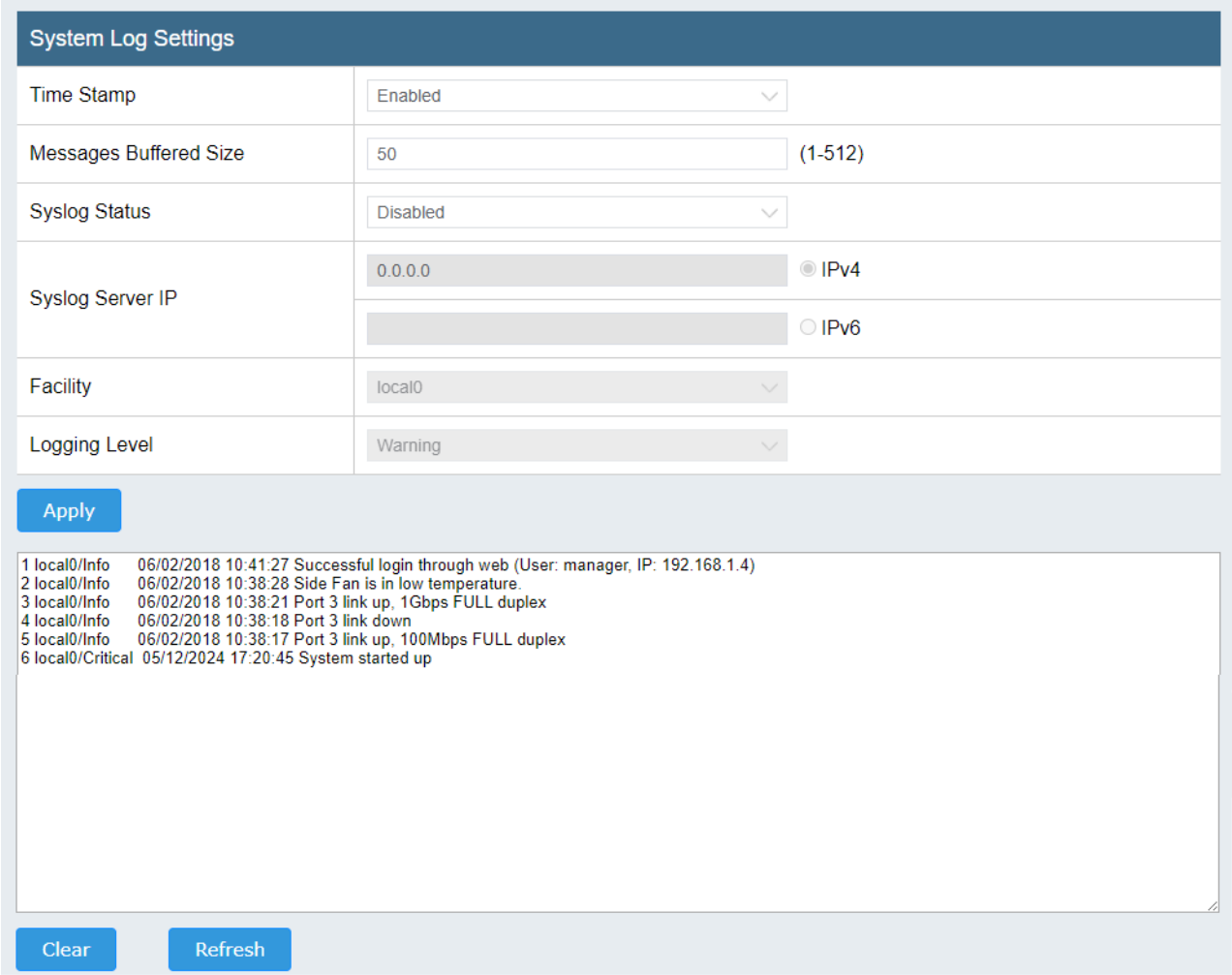


Figure 50. System Log Settings Window

Sending System Log Events to a Syslog Server

The system log events can play an important role in diagnosing and resolving network problems. However, when problems do occur it may not always be immediately evident which device was the cause. Troubleshooting problems might require the burdensome and time consuming task of reviewing system logs on multiple managed devices.

Having the managed devices send their events to a central server for storage can simplify troubleshooting problems. Rather than having the view the events on the individual devices, you can instead view them on a central server.

That is the function of the syslog client on the switch. It allows the switch to send its event messages to a syslog server on your network, for storage.

Here are the guidelines to using the syslog client:

- ❒ You can specify one syslog server.
- ❒ The switch must have a management IP address. For instructions, refer to Chapter 4, “Management IPv4 Addresses” on page 71 or Chapter 5, “Management IPv6 Addresses” on page 81.
- ❒ If the syslog server is not a member of the same subnet as the management IP address of the switch, the switch has to have a default gateway specifying the first hop to reaching the server. For instructions on specifying the default gateway, refer to refer to Chapter 4, “Management IPv4 Addresses” on page 71 or Chapter 5, “Management IPv6 Addresses” on page 81.
- ❒ The event messages are transmitted when they are generated. Any event messages already in the event log are not transmitted when you enable the syslog client.
- ❒ The syslog client uses UDP port 514. You cannot change the UDP port.

To configure the syslog client on the switch:

1. Select **System** > **System Log** from the menu. Refer to Figure 50 on page 137.
2. Configure the fields in Table 38 on page 139.

Note
The Time Stamp and Messages Buffered Size parameters are described in “Viewing the Event System Log” on page 136.

Table 38. System Log Settings Window - Syslog Client

Field	Description
Syslog Status	Select one of the following: - **Enabled**: Activates the Syslog client so that the switch sends events to a Syslog server. Syslog Status has to be set to Enabled for you to configure the other settings. - **Disabled**: Deactivates the Syslog client to stop the switch from sending events to a Syslog server. This is the default sending.
Syslog Server IP	Enter the IPv4 or IPv6 address of the Syslog server on your network. You can enter only one address. The format for an IPv4 address is shown here: nnn nnn nnn nnn Each N is a decimal number from 0 to 255. The format for an IPv6 address is shown here: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx Each x is a hexadecimal digit representing four bits. The eight groups of digits have to be separated by colons. Groups where all four digits are ‘0’ can be omitted. Leading ‘0’s in groups can also be omitted. As an example, the following IPv6 addresses are equivalent: 3710:421e:09a8:0000:0000:0000:00a4:1c50 3710:421e:9a8::a4:1c50
Facility	Select a facility level to add to the event messages as the switch transmits them to the syslog server. Facility levels are numerical codes that are commonly used to group entries on the syslog server according to the source network devices. You can specify only one facility level. Refer to RFC 3164 for facility code definitions. The range is local0 to local7.

Table 38. System Log Settings Window - Syslog Client (Continued)

Field	Description
Logging Level	Select the severity level of the log events to send to the Syslog server. The levels are listed here from highest to lowest severity: - Alert - Critical - Warning - Info Selecting a severity included the messages of that level and those levels above it. The default severity is Info. At the default setting, The switch transmits alert, critical, and warning messages. To send messages from all severities, select Info.

3. Click **Apply**.

   If you enabled the Syslog client, the switch begins transmitting log events as they occur, to the Syslog server. It does not transmit messages already stored in the event log.

   Note
   Select **Save** from the menu to save your changes.

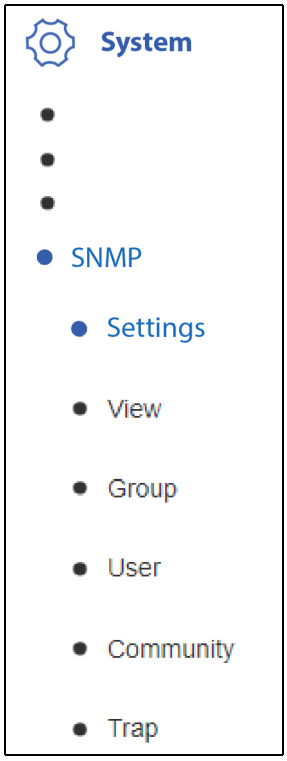
Chapter 14

SNMPv1 and v2c

This chapter described SNMPv1 and SNMPv2c in the following sections:

- ❒ “Enabling or Disabling SNMP Management” on page 142
- ❒ “Changing the SNMP Engine ID” on page 143
- ❒ “SNMPv1 and v2c View Names” on page 144
- ❒ “SNMPv1 and SNMPv2c User and Group Names” on page 146
- ❒ “SNMP Community Strings” on page 148
- ❒ “SNMP Traps” on page 150

Enabling or Disabling SNMP Management



To enable or disable SNMP management on the switch:

1. Select **System** > **SNMP** > **Settings** from the menu. The SNMP Engine ID Settings window is shown in Figure 51.

   Note
   The SNMP Engine ID Settings section in the window is described in “Changing the SNMP Engine ID” on page 143.

2. Choose one of the following from the **SNMP Agent Status** pull-menu:

   - **Enabled** - Enables the SNMP agent, allowing you to manage the switch with SNMP.
   - **Disabled** - Disables the SNMP agent, blocking SNMP management.

3. Click **Apply**.

   Note
   Select **Save** from the menu to save your changes.

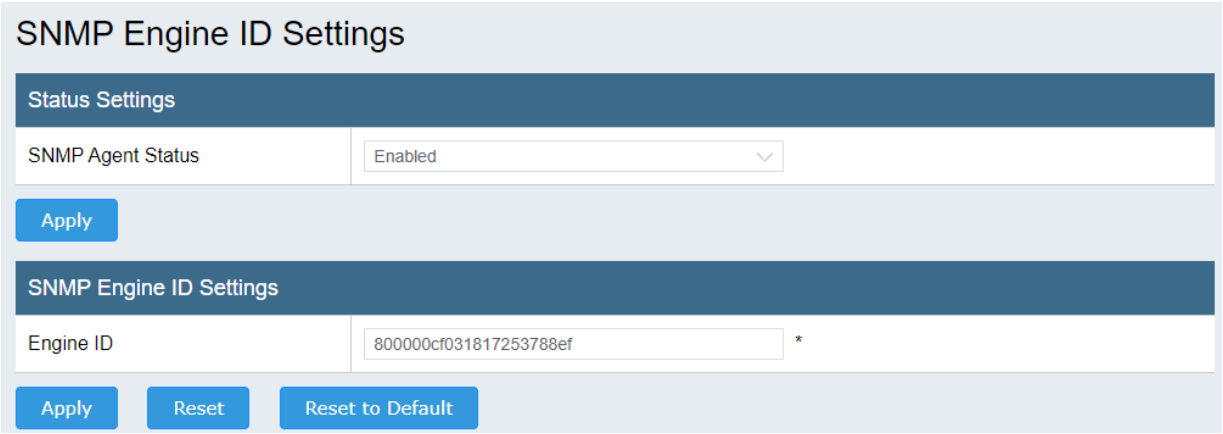
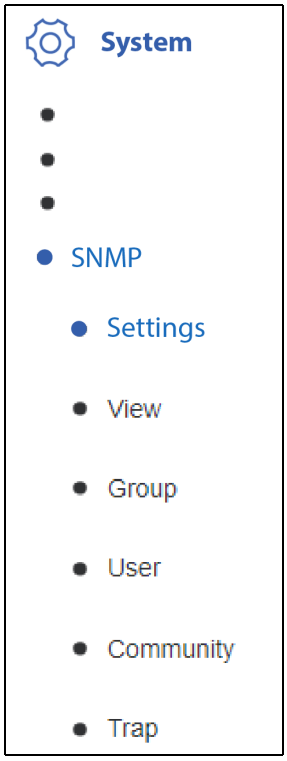


Figure 51. SNMP Engine ID Settings Window

Changing the SNMP Engine ID



The SNMP agent has an engine ID that uniquely identifies the agent in a device and the MIB objects in a domain. The engine ID of the switch follows the RFC 3411 standard and consists of the enterprise ID and the MAC address of the switch.

To modify or reset the SNMP engine ID:

1. Select **System** > **SNMP** > **Settings** from the menu. The SNMP Engine ID Settings window is shown in Figure 51 on page 142.
2. Perform one of the following:
   - ❒ Enter the new engine ID in the Engine ID field.
   - ❒ To reset the engine ID to the previous setting, click **Reset**.
   - ❒ To reset the engine ID to the default setting, click **Reset to Default**.
3. Click **Apply**.

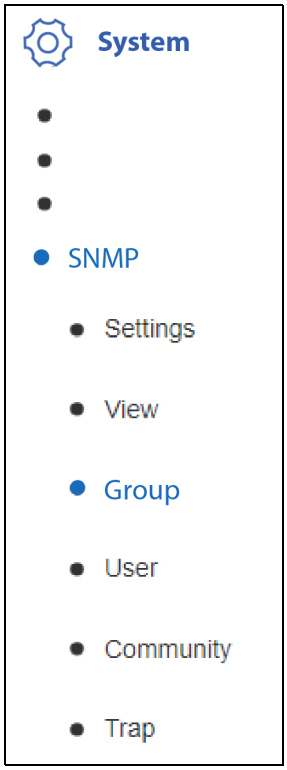
Note
Select **Save** from the menu to save your changes.

SNMPv1 and v2c View Names

The SNMPv1 and v2c view names are defined in the SNMP Group Access table and are based on the user and group names. Here are the procedures:

- ”Adding SNMPv1, v2c View Names”
- “Modifying SNMPv1, v2c View Names” on page 145
- “Deleting SNMPv1, v2c View Names” on page 145

Adding SNMPv1, v2c View Names



To add an SNMPv1 and v2c view name, you first have to define its group name with the SNMP User/Group window. Refer to “Adding User and Group Names” on page 146. To add SNMPv1 and v2c view names:

1. Select **System** > **SNMP** > **Group** from the menu. The SNMP Group Access Table window is shown in Figure 52 on page 145.
2. Configure the settings in Table 39.

Table 39. SNMP Group Access Table Window for v1 and v2c

Parameter	Description
Group Name	Enter the name of an existing group in the Group Name field. To add group names, refer to “Adding User and Group Names” on page 146.
Read View Name	Enter a read view name of up to 32 characters. The name is optional.
Write View Name	Enter a write view name of up to 32 characters. The name is optional.
Notify View Name	Enter a notify view name of up to 32 characters. The name is optional.
Security Model	Select **v1** or **v2c**. For information on the V3 selections included in this parameter, refer to Chapter 15, “SNMPv3” on page 153.
Security Level	This parameter does not apply to SNMPv1 and v2c view names. For information, refer to Chapter 15, “SNMPv3” on page 153.

3. Click **Add** to add the new SNMPv1 and v2c view name. To return the settings to their previous values, click **Reset**.

Note
Select **Save** from the menu to save your changes.

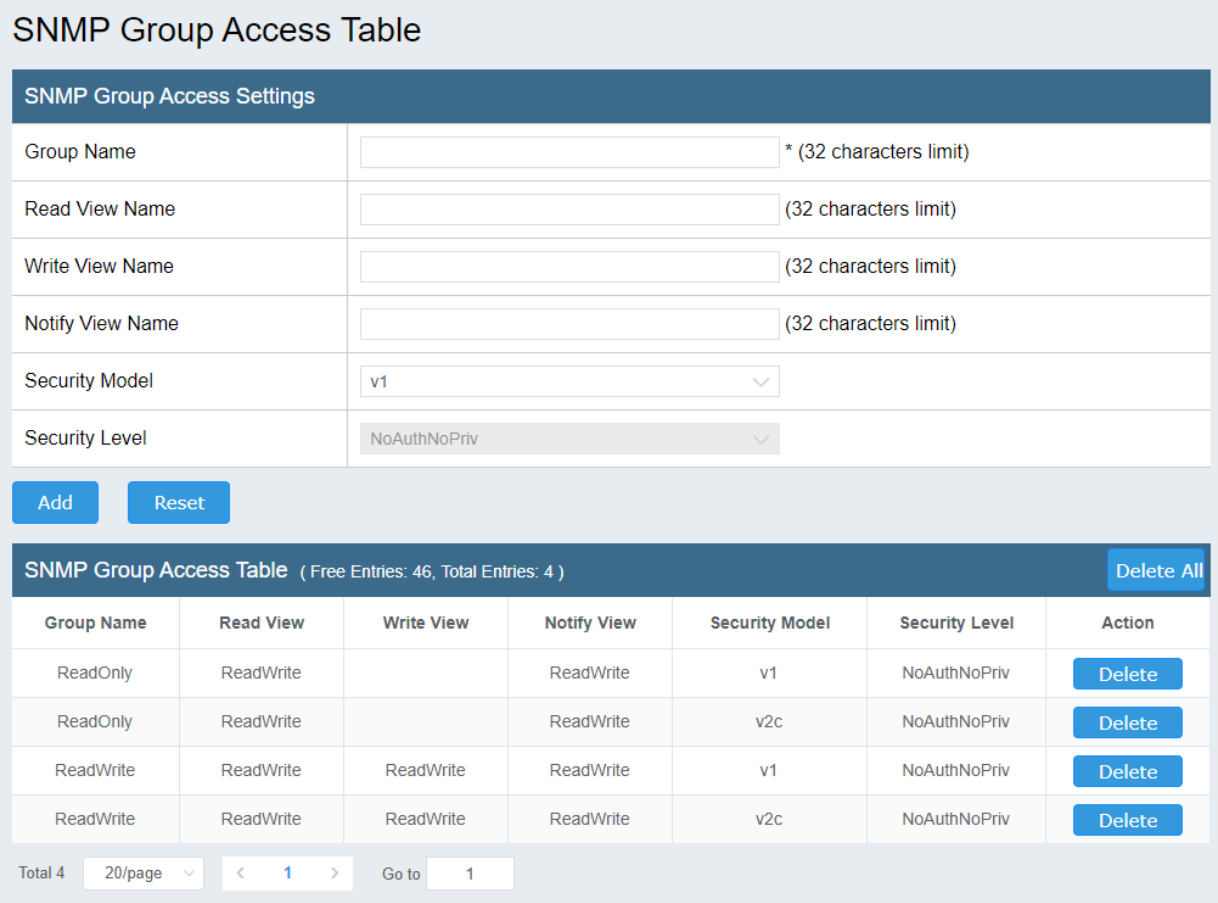


Figure 52. SNMP Group Access Table Window

Modifying SNMPv1, v2c View Names

You cannot modify entries in the SNMP Group Access window. To change an entry, you must delete and enter it again with the changes. Refer to "Deleting SNMPv1, v2c View Names," next and "Adding SNMPv1, v2c View Names" on page 144.

Deleting SNMPv1, v2c View Names

To delete entries from the SNMP Group Access Table window:

1. Select **System** > **SNMP** > **Group** from the menu. The SNMP Group Access Table window is shown in Figure 52 on page 145.

2. Click **Delete** in the Action column of the group name to be removed. You can delete only one group name at a time.

Note
Select **Save** from the menu to save your changes.

SNMPv1 and SNMPv2c User and Group Names

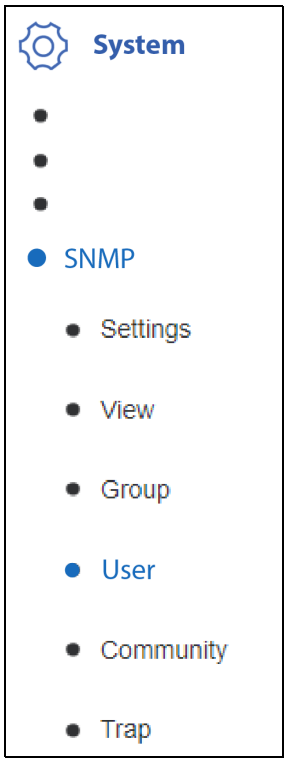
SNMPv1 and SNMPv2c User Name and Group Name definitions are the basis for adding SNMP communities. Use the following sections to create or delete User and Group Names:

- ❒ “Adding User and Group Names,” next
- ❒ “Modifying User and Group Names” on page 147
- ❒ “Deleting User and Group Names” on page 147

A community string has attributes for controlling who can use the string and what the string allows a network management station to do on the switch.

The iGS950 Switch does not have any default community strings. You have to define an SNMP User and Group Name on the SNMP User/Group window and then define a community name on the SNMP Community Table window.

Adding User and Group Names



Perform the following procedure to add SNMP Users and Group Names:

1. Select **System** > **SNMP** > **User** from the menu. The SNMP User/Group window is shown in Figure 53 on page 147.
2. Configure the settings in Table 40.

Table 40. SNMP User/Group Window for v1/v2c

Parameter	Description
User Name	Enter a user name up to 32 characters.
Group Name	Enter the group name ReadOnly or ReadWrite.
SNMP Version	Select either **v1** or **v2c.**

Note
The Auth-Protocol, Priv-Protocol, and Password fields are for SNMPv3 user and group names. Refer to Chapter 15, “SNMPv3” on page 153.

3. Click **Add** to add the new SNMP v1/v2c user and group names. To return the settings to their previous values, click **Reset**.

Note
Select **Save** from the menu to save your changes.

The SNMP User/Group window is shown in Figure 53.

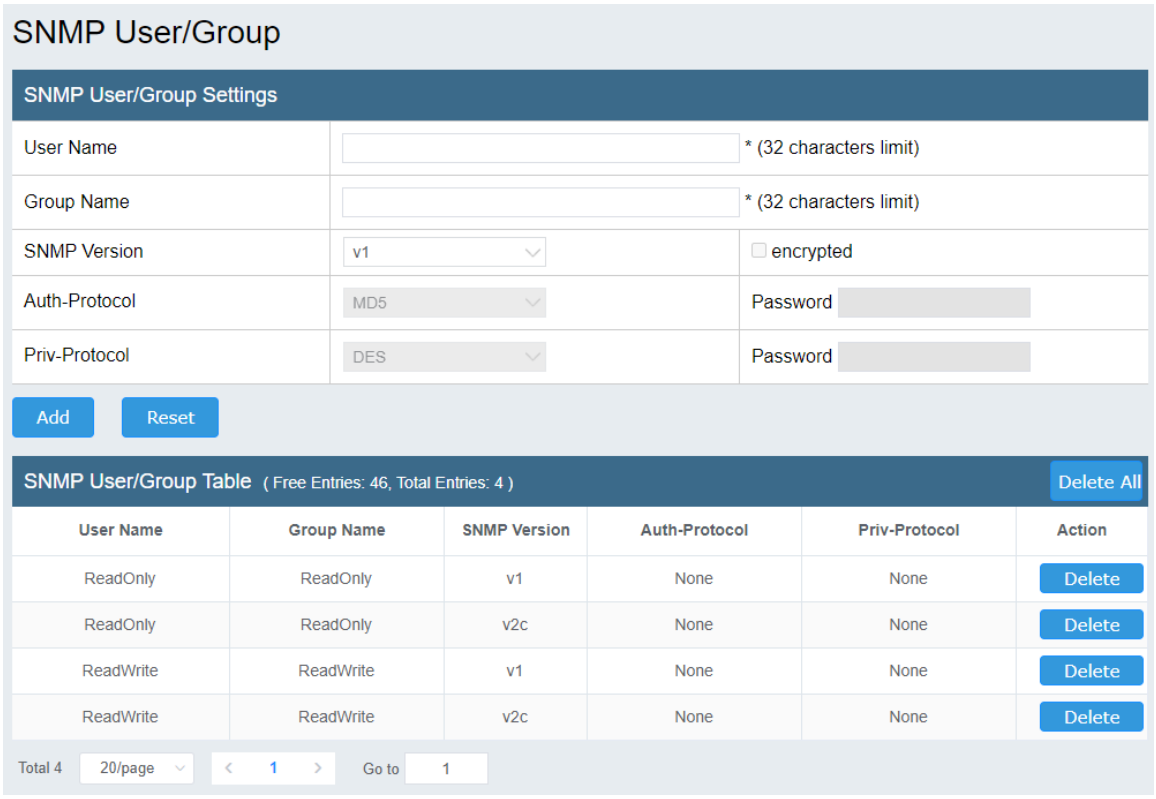


Figure 53. SNMP User/Group Window

Modifying User and Group Names

You cannot modify entries in the SNMP User/Group window. To change an entry, you have to delete it and reenter it with the changes.

Deleting User and Group Names

Perform this procedure to delete entries from the SNMP User/Group window:

1. Select **System** > **SNMP** > **User** from the menu. Refer to Figure 53.
2. In the **Action** column of the table, click **Delete** of the User and Group names to be deleted.

Note
Select **Save** from the menu to save your changes.

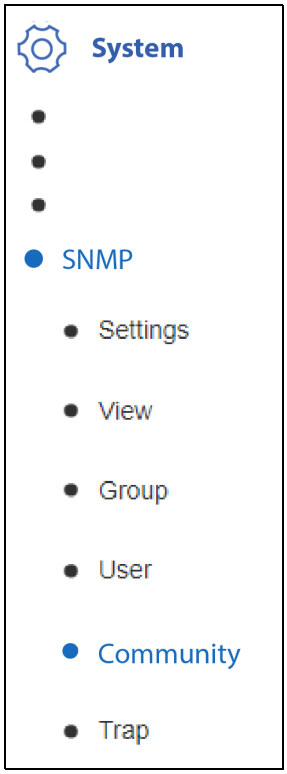
SNMP Community Strings

Community strings have attributes that control who can use them and what they will allow network management stations to do on the switch. You first have to define an SNMP User and Group Name on the SNMP User/Group page and then define a community name on the SNMP Community Table page.

Here are the SNMP community strings procedures:

- ❒ “Adding SNMP Community Strings,” next
- ❒ “Modifying SNMP Community Strings” on page 149
- ❒ “Deleting SNMP Community Strings” on page 149

Adding SNMP Community Strings



To add SNMPv1 and SNMPv2c community strings:

1. Select **System** > **SNMP** > **Community** from the menu. The Community Table window is shown in Figure 54 on page 149.
2. Configure the fields in Table 41.

Table 41. SNMP Community Table Window

Parameter	Description
Community Name	Enter a new community name up to 32 characters.
User Name (View Policy)	Enter a user name up to 32 characters. This name has to match one of the user names in the SNMP User/Group window. Refer to “Adding User and Group Names” on page 146.

3. Click **Add** to add the new community name to the table.

Note
Select **Save** from the menu to save your changes.

Figure 54. SNMP Community Table Window

Modifying SNMP Community Strings

To modify a Community Table entry, you have to delete it and reenter it with the desired changes.

Deleting SNMP Community Strings

To delete SNMP community names:

1. Select **System** > **SNMP** > **Community** from the menu to display the SNMP Community Table window.
2. Click **Delete** in the Action column of the entry you want to remove. You can deleter only one community at a time.

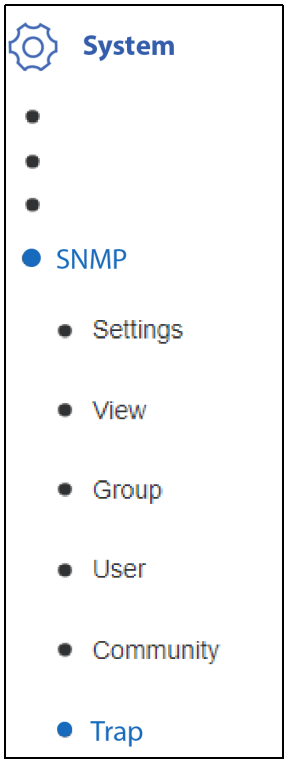
Note
Select **Save** from the menu to save your changes.

SNMP Traps

The switch can send SNMP traps to designated host IP addresses of management devices to alert you to network operational events. Here are the procedures:

- ❒ “Adding Trap Host Table Entries,” next
- ❒ “Modifying Trap Host Table Entries” on page 152
- ❒ “Deleting Trap Host Table Entries” on page 152

Adding Trap Host Table Entries



Use the following procedure to add trap Host Table entries:

1. Select **System** > **SNMP** > **Trap** from the menu. The Trap Management window is shown in Figure 55 on page 152.

   To enable or disable trap management, perform steps 2 and 3. To add new trap destinations, go to step 4.

2. Select one of the following from Trap Status:

   - ❒ **Enabled**: This activates trap management. You have to enable trap management to configure its settings.
   - ❒ **Disabled**: This deactivates trap management. The switch does not transmit traps when trap management is disabled.

3. Click **Apply**.

4. To add new trap destinations, configure the settings in Table 42 on page 150.

Table 42. Trap Management Window

Parameter	Description
Host IP Address	Enter the IP address of a host node to receive traps from the switch. The address can be either IPv4 or IPv6. Here are the guidelines for entering an IPv4 address: - An IPv4 address has to be entered in this format. nnn.nnn.nnn.nnn - Each “nnn” is a decimal number from 0 to 255 - The numbers have to be separated by periods.

Table 42. Trap Management Window (Continued)

Parameter	Description
Host IP Address (continued)	Here are the guidelines for entering an IPv6 address: - An IPv6 address has to be entered in this format. nnn:nnn:nnn:nnn:nnn:nnn:nnn:nnn N is a hexadecimal digit from 0 to F. - The eight groups are separated by colons. - You can omit groups where all four digits are “0”. - You can also omit leading “0”s in groups. As an example, the following two addresses are equivalent: - 12c4:421e:09a8:0000:0000:0000:00a4:1c50 12c4:421e:09a8:a4:1c50
SNMP Version	Select **v1**, **v2c, v3-NoAuthNoPriv, v3-AuthNoPriv,** and **v3-AuthPriv.**
Community Name/ User Name	Enter an existing community name from the SNMP Community Table. Refer to “SNMP Community Strings” on page 148.

5. Click **Add** to add the new trap. To return the settings to their previous values, click **Reset**.

Note
Select **Save** from the menu to save your changes.

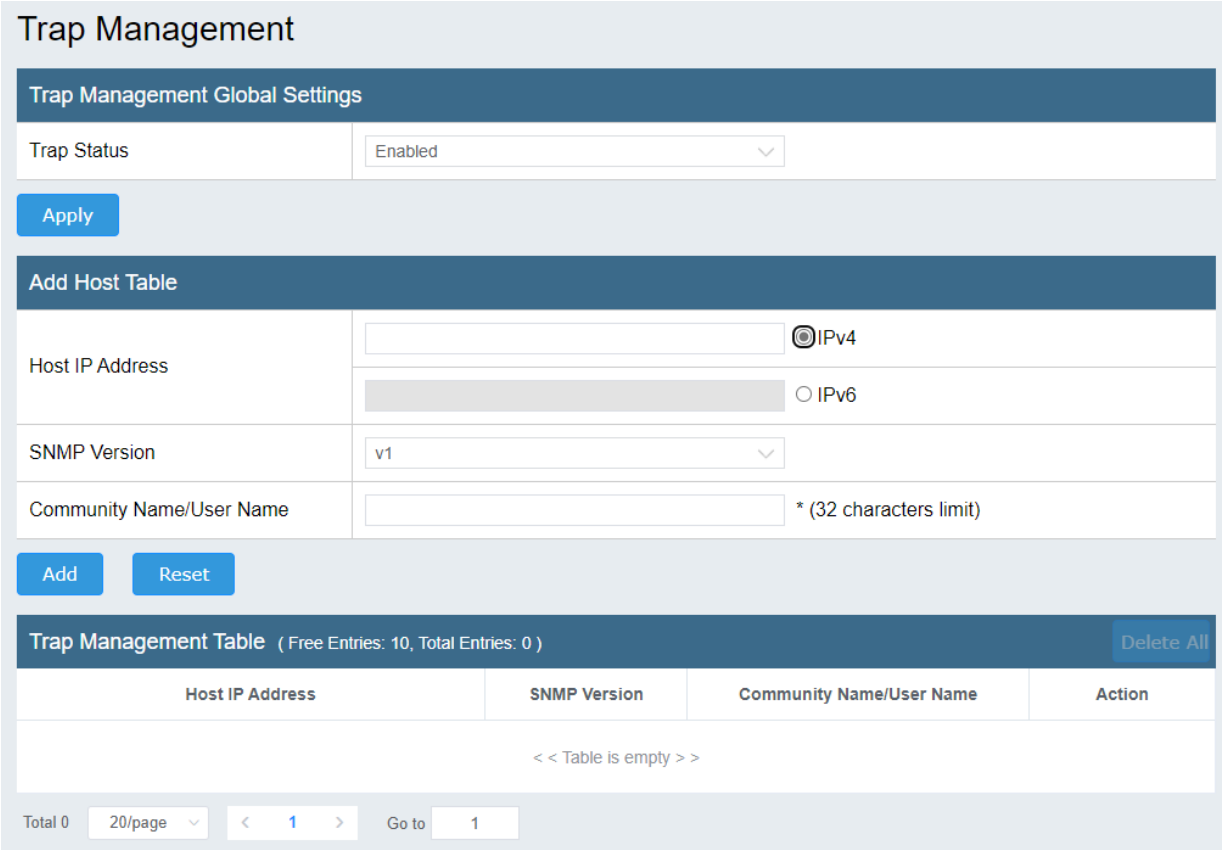


Figure 55. Trap Management Window

Modifying Trap Host Table Entries

To modify a trap host entry, you have to delete it and reenter it with the necessary changes.

Deleting Trap Host Table Entries

Perform the following procedure to delete trap host entries:

1. Select **System** > **SNMP** > **Trap** from the menu. The Trap Management window is shown in Figure 55.
2. Click **Delete** in the Action column of the entry to be deleted. No confirmation message is displayed.

Note
Select **Save** from the menu to save your changes.

Chapter 15
SNMPv3

This chapter describes SNMPv3 in the following sections:

- “SNMPv3 Overview” on page 154
- “SNMPv3 User and Group Names” on page 158
- “SNMPv3 View Names” on page 160
- “SNMPv3 View Table” on page 163
- “SNMPv3 Traps” on page 165
- “SNMP Engine ID” on page 166

SNMPv3 Overview

The SNMPv3 protocol builds on the existing SNMPv1 and SNMPv2c protocol implementation, which is described in Chapter 14, “SNMPv1 and v2c” on page 141. In SNMPv3, User-based Security Model (USM) authentication is implemented along with encryption, allowing you to configure a secure SNMP environment.

The SNMPv3 protocol uses different terminology than the SNMPv1 and SNMPv2c protocols. In the SNMPv1 and SNMPv2c protocols, the terms agent and manager are used. An agent is the software within an SNMP user, while a manager is an SNMP host. In the SNMPv3 protocol, agents and managers are called entities. In any SNMPv3 communication, there is an authoritative entity and a non-authoritative entity. The authoritative entity checks the authenticity of the non-authoritative entity. The non-authoritative entity checks the authenticity of the authoritative entity.

With the SNMPv3 protocol, you create users, determine the protocol used for message authentication and determine if data transmitted between two SNMP entities are encrypted. In addition, you can restrict user privileges by defining which portions of the Management Information Bases (MIBs) can be viewed by specific users. In this way, you restrict which MIBs a user can display and modify. In addition, you can restrict the types of messages, or traps, the user can send. (A trap is a type of SNMP message.) After you have created a user, you define SNMPv3 message notification. This consists of determining where messages are sent and which types of messages can be sent. This configuration is similar to the SNMPv1 and SNMPv2c configurations because you configure IP addresses of trap receivers, or hosts.

This section describes the features of the SNMPv3 protocol. The following subsections are included:

- ”SNMPv3 Authentication Protocols”
- “SNMPv3 Privacy Protocol” on page 155
- “SNMPv3 MIB Views” on page 155
- “SNMPv3 Configuration Process” on page 156

SNMPv3 Authentication Protocols

The SNMPv3 protocol supports two authentication protocols— HMAC-MD5-96 (MD5) and HMAC-SHA-96 (SHA). Both MD5 and SHA use an algorithm to generate a message digest. Each authentication protocol authenticates a user by checking the message digest. In addition, both protocols use keys to perform authentication. The keys for both protocols are generated locally using the Engine ID and the user password. You can only modify a key by modifying the user password.

In addition, you have the option of assigning no user authentication. In this case, no authentication is performed for this user. You may want to make this configuration for someone with super-user capabilities.

SNMPv3 Privacy Protocol

After configuring an authentication protocol, you have the option of assigning a privacy protocol. In SNMPv3 protocol terminology, privacy is equivalent to encryption. Currently, the DES protocol is the only encryption protocol supported. The DES privacy protocol requires the authentication protocol to be configured as either MD5 or SHA.

If you assign a DES privacy protocol to a user, then you are also required to assign a privacy password. If you choose to not assign a privacy value, then SNMPv3 messages are sent in plain text format.

SNMPv3 MIB Views

The SNMPv3 protocol allows you to configure MIB views for users and groups. The MIB tree is defined by RFC 1155 (Structure of Management Information). See Figure 56.

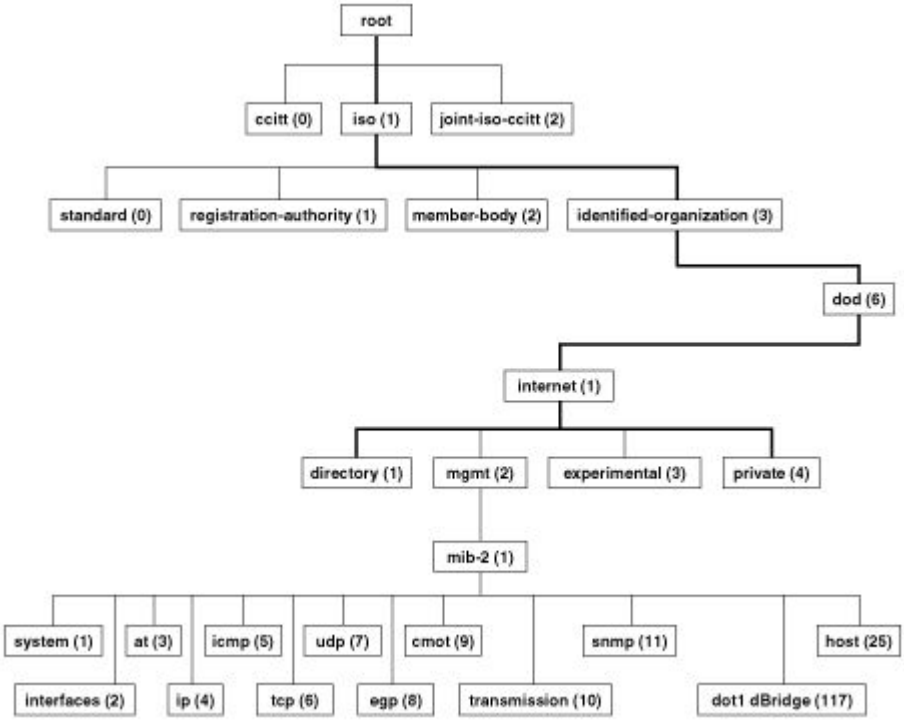


Figure 56. MIB Tree

The iGS950 Switches support the MIB tree, starting with the Internet MIBs, as defined by 1.3.6.1. There are two ways to specify an MIB view. You can enter the OID number of the MIB view or its equivalent text name. For example, to specify MIBs in the Internet view, you can enter the OID format “1.3.6.1” or the text name, “internet.”

In addition, you can define an MIB view that a user can access or an MIB view that a user cannot access. When you want to permit a user to access an MIB view, you include a particular view. When you want to deny a user access to an MIB view, you exclude a particular view.

After specifying an MIB subtree view, you have the option of further restricting a view by defining a subtree mask. The relationship between an MIB subtree view and a subtree mask is analogous to the relationship between an IP address and a subnet mask. The switch uses the subnet mask to determine which portion of an IP address represents the network address and which portion represents the node address. In a similar way, the subtree mask further refines the subtree view and enables you to restrict an MIB view to a specific row of the OID MIB table. You need a thorough understanding of the OID MIB table to define a subtree mask.

SNMPv3 Configuration Process

The SNMPv3 parameters are contained in the following tables:

- ❒ SNMPv3 User/Group table
- ❒ SNMPv3 Access table
- ❒ SNMPv3 View table
- ❒ SNMPv3 Community table
- ❒ Trap Management

The SNMPv3 configuration information must be entered in a specific sequence:

Note
The SNMP Interface has to be activated first. Refer to “Enabling or Disabling SNMP Management” on page 142.

1. Create a user name and associated group name in the SNMPv3 User/Group table.
2. Define view names in the Access table for each group name.
3. Define the MIB view in the SNMPv3 View table for each view name.
4. Enter information in the Community table based on a pre-defined user name.

Note
The community strings do not have a default value defined and are initially blank.

5. Define the traps on the Trap Management page based on the community or user name.

See Figure 57 for an illustration of how the user configuration tables are linked.

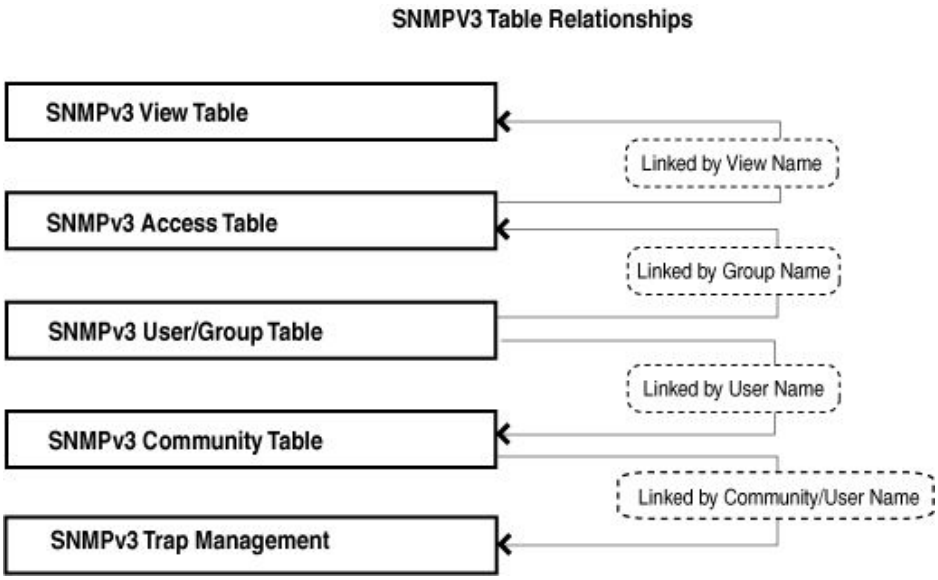


Figure 57. SNMPv3 Table Relationships

SNMPv3 User and Group Names

SNMPv3 user and group names are the basis for all SNMPv3 tables. Here are the procedures:

- ”Adding SNMPv3 User and Group Names”
- “Modifying SNMPv3 User and Group Names” on page 159
- “Deleting SNMPv3 User and Group Names” on page 159

Adding SNMPv3 User and Group Names

Perform this procedure to add SNMPv3 user and group names:

1. Select **System** > **SNMP** > **User** from the menu. The SNMP User/Group window is shown in Figure 53 on page 147.
2. Configure the settings in Table 43.

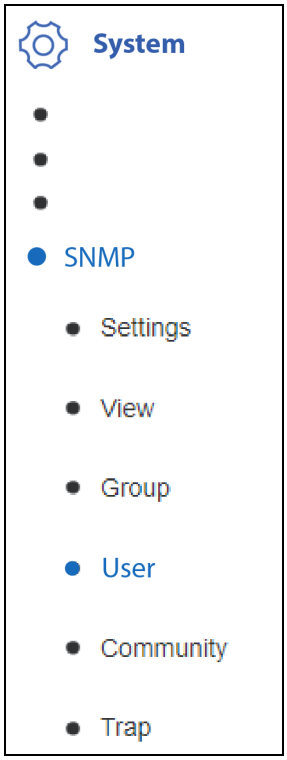


Table 43. SNMP User/Group Window for v3

Parameter	Description
User Name	Enter a user name up to 32 characters.
Group Name	Enter a group name up to 32 characters.
SNMP Version	Select **v3**.
encrypted	To add encryption to the user name, click the **encrypted** check box to add a check mark.
Auth-Protocol	Select one of the following: - **MD5**: The switch uses MD5 authentication to authenticate the SNMPv3 user. This is the default value. - **SHA**: The switch uses SHA authentication to authenticate the SNMPv3 user.
Password	Enter a password for Auth-Protocol.
Priv-Protocol	Select one of the following: - **DES**: The switch uses DES encryption to encrypt the SNMP packets. This is the default value. - **none**: The switch does not encrypt the SNMP packets.
Password	Enter a password for Priv-Protocol. Auth-Protocol has to have a password if DES for Priv-Protocol has a password.

3. Click **Add**.

   The new user name and group name are displayed on the SNMP User/Group page.

   Note
   Select **Save** from the menu to save your changes.

Modifying SNMPv3 User and Group Names

You cannot modify user or group name entries. To change an entry, you have to delete it and reenter it with the changes. Refer to “Deleting SNMPv3 User and Group Names” on page 159 and “Adding SNMPv3 User and Group Names” on page 158.

Deleting SNMPv3 User and Group Names

Perform this procedure to delete entries from the SNMP User/Group window.

1. Select **System** > **SNMP** > **User** from the menu. The SNMP User/ Group window is shown in Figure 53 on page 147.

2. Click **Delete** In the **Action** column of the user name to be removed. You cannot delete the default SNMPv1 and v2c entries.

   Note
   Select **Save** from the menu to save your changes.

SNMPv3 View Names

The SNMPv3 view names are defined in the SNMP Group Access table and are based on the user and group names.You can add and delete view names with the following procedures:

- ”Adding SNMPv3 View Names”
- “Modifying SNMPv3 View Names” on page 162
- “Deleting SNMPv3 View Names” on page 162

Adding SNMPv3 View Names

To add an SNMPv3 view name, you first have to define its group name with the SNMP User/Group window. Refer to “Adding SNMPv3 User and Group Names” on page 158.

Perform this procedure to add SNMPv3 view names.

1. Select **System** > **SNMP** > **Group** from the menu.

   The SNMP Group Access Table window is shown in Figure 58.

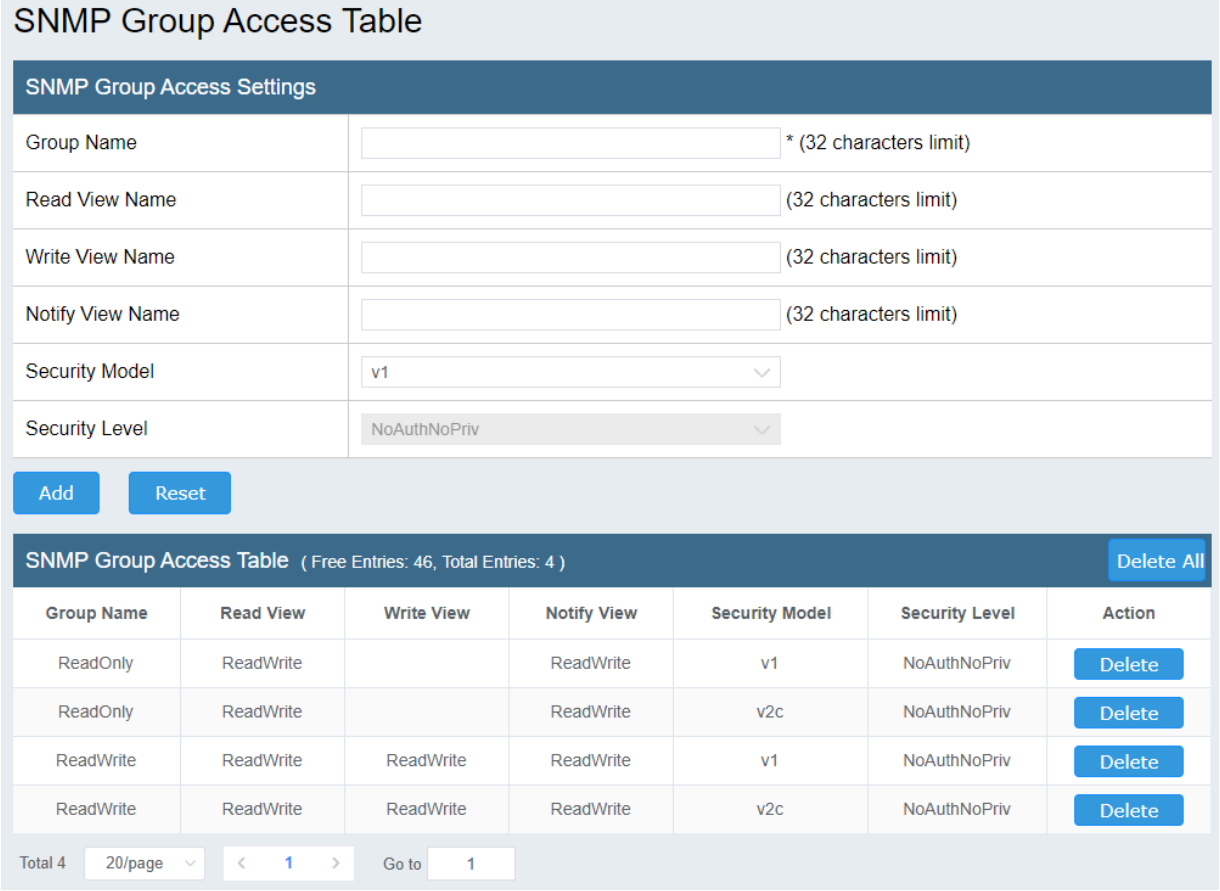


Figure 58. SNMP Group Access Table Window

2. Configure the settings in Table 44.

Table 44. SNMP Group Access Table Window for v3

Parameter	Description
Group Name	Enter the name of an existing group in the Group Name field. To add group names, refer to “Adding SNMPv3 User and Group Names” on page 158.
Read View Name	Enter a read view name of up to 32 characters. The name is optional.
Write View Name	Enter a write view name of up to 32 characters. The name is optional.
Notify View Name	Enter a notify view name of up to 32 characters. The name is optional.
Security Model	Select **v3**.
Security Level	Choose a Security Level from the menu. The selections are listed here: - **NoAuthNoPriv**: This selection is appropriate when no Auth-Protocol or Priv-Protocol (no encryption) are selected on the SNMP User/ Group page. - **AuthNoPriv**: Choose this selection when encryption has been enabled, but only the Auth-Protocol has a password assigned, and the Priv-Protocol has been selected as none on the SNMP User/Group page. - **AuthPriv**: When both the Auth-Protocol and Priv-Protocol have been enabled, choose this selection. For information on the SNMPv1 and v2c selections in this parameter, refer to “Adding SNMPv1, v2c View Names” on page 144.

3. Click **Add**.

Note
Select **Save** from the menu to save your changes.

Modifying SNMPv3 View Names

You cannot modify entries in the SNMP Group Access window. To change an entry, you have to delete it and reenter it with the changes. Refer to “Deleting SNMPv3 View Names” next and “Adding SNMPv3 View Names” on page 160.

Deleting SNMPv3 View Names

Perform this procedure to delete entries from the SNMP Group Access Table window:

1. Select **System** > **SNMP** > **Group** from the menu. The SNMP Group Access Table window is shown in Figure 58 on page 160.
2. Click **Delete** in the **Action** column of the group name to be removed.

Note
Select **Save** from the menu to save your changes.

SNMPv3 View Table

The SNMPv3 View table specifies the MIB object access criteria for each view name. If the view name is not specified on this page, then it has access to all MIB objects. You can specify specific areas of the MIB that can be accessed or denied based on the entries in this table. You can add and delete entries in the View table by following the procedures in these sections:

- ”Adding SNMPv3 View Table Entries”
- “Modifying SNMPv3 View Table Entries” on page 164
- “Deleting SNMPv3 View Table Entries” on page 164

Adding SNMPv3 View Table Entries

Perform this procedure to add entries to the SNMPv3 View table.

1. Select **System** > **SNMP** > **View** from the menu.

   The SNMP View Table window is shown in Figure 59.

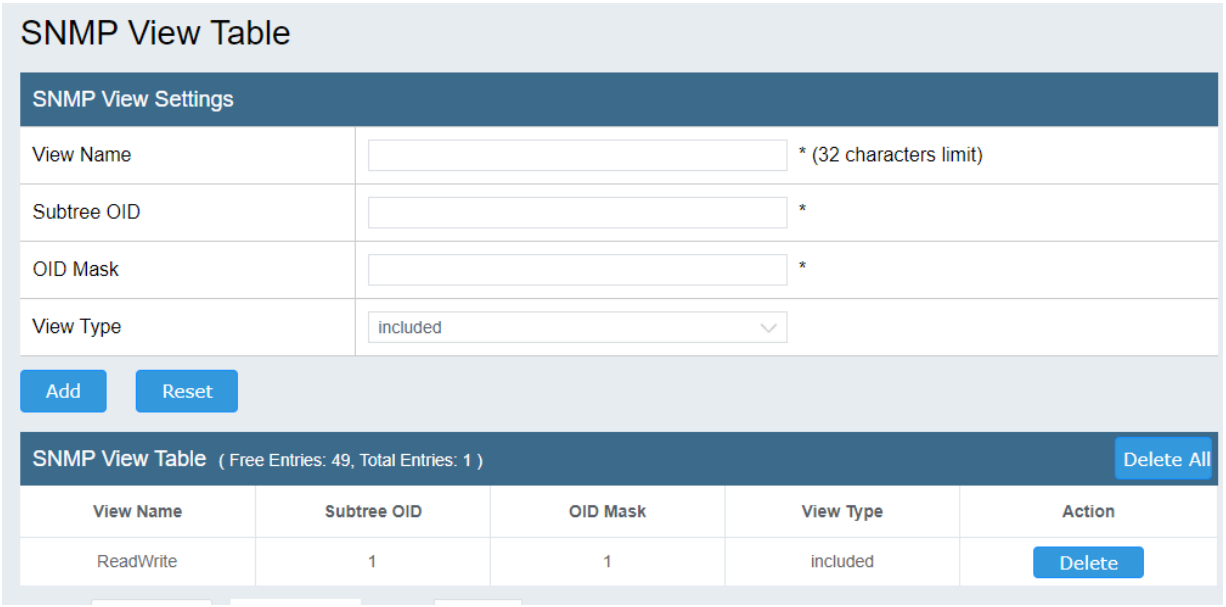


Figure 59. SNMP View Table Window

2. Configure the settings in Table 45.

Table 45. SNMP View Table Window for v3

Parameter	Description
View Name	Enter the name of an existing view. Refer to “Adding SNMPv3 View Names” on page 160.
Subtree OID	Enter the subtree OID.
OID Mask	Enter “1” for the mask.
View Type	Select one of the following: - **Included**: This selection allows the view to include the specified MIB object. - **Excluded**: This selection blocks the view of the specified MIB object.

3. Click **Add**.

   The updated view is displayed in the View table.

Note
Select **Save** from the menu to save your changes.

Modifying SNMPv3 View Table Entries

You cannot modify an entry in the View Table page. To change an entry, you have to delete it and reenter it with the changes. Refer to ”Deleting SNMPv3 View Table Entries” and “Adding SNMPv3 View Table Entries” on page 163.

Deleting SNMPv3 View Table Entries

Perform this procedure to delete entries from the SNMPv3 View table.

1. Select **System** > **SNMP** > **View** from the menu. Refer to Figure 59 on page 163.

2. Click **Delete** In the Action column of the entry you want to remove.

Note
Select **Save** from the menu to save your changes.

SNMPv3 Traps

The procedures for adding, modifying, or deleting SNMPv3 traps are the same as for SNMPv1/v2 traps. Refer to “SNMP Traps” on page 150.

SNMP Engine ID

An SNMP agent has an engine ID that uniquely identifies the agent in a device and the MIB objects in a domain. The engine ID of the switch follows the RFC 3411 standard and consists of the enterprise ID and the MAC address of the switch.

To modify the engine ID, perform the following procedure.

1. Select **System** > **SNMP** > **Settings** from the menu.

   The SNMP Engine ID Settings window is shown in Figure 51 on page 142.

2. Do one of the following:

   - ❒ To change the engine ID, enter the new value in the Engine ID field.
   - ❒ To reset the engine ID to the previous setting, click **Reset**.
   - ❒ To reset the engine ID to the default setting, click **Reset to Default**.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Chapter 16
RMON

This chapter contains the following sections:

- “RMON Overview” on page 168
- “Enabling and Disabling RMON” on page 169
- “RMON Port Statistics Groups” on page 170
- “RMON Histories” on page 172
- “RMON Events” on page 175
- “RMON Alarms” on page 179

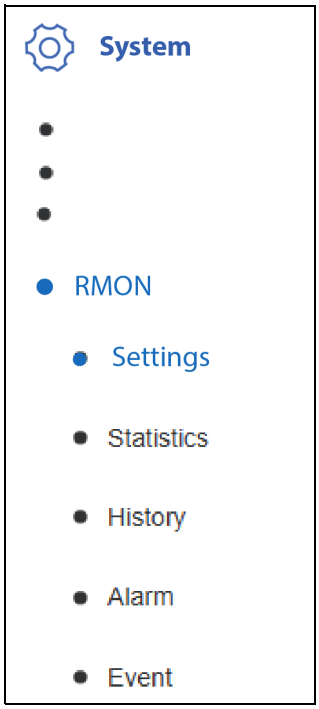
RMON Overview

The RMON (Remote MONitoring) MIB is used with SNMP applications to monitor the operations of network devices. The switch supports the four RMON MIB groups listed here:

- Statistic groups — Collects port statistics. Refer to “RMON Port Statistics Groups” on page 170.
- History groups — Collects histories of port statistics. Refer to “RMON Histories” on page 172.
- Event groups — Defines the actions of RMON alarms that switches perform when packet statistic thresholds are crossed. Refer to “RMON Events” on page 175.
- Alarm groups —Defines the statistics thresholds that trigger alarms and alarm actions. Refer to “RMON Alarms” on page 179.

For instructions on how to configure SNMP on your switch, refer to Chapter 14, “SNMPv1 and v2c” on page 141 or Chapter 15, “SNMPv3” on page 153.

Enabling and Disabling RMON



RMON allows you to monitor the statistics and histories of switch ports, with SNMP Network Management System (NMS) software and the RMON section of the MIB tree. You can also use RMON to add alarms in the forms of log entries or SNMP traps that alert you when port traffic cross defined thresholds.

Because RMON requires SNMP, the SNMP agent on the switch has to be enabled for the RMON feature to be active. Refer to Chapter 14, “SNMPv1 and v2c” on page 141 or Chapter 15, “SNMPv3” on page 153.

To enable or disable RMON:

1. Select **System** > **RMON** > **Settings** from the menu.The RMON Basic Settings window is shown in Figure 60.
2. Select one of the following from the RMON Status menu:
   - **Enabled**: Enables the RMON feature.
   - **Disabled**: Disable the RMON feature. This is the default setting.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

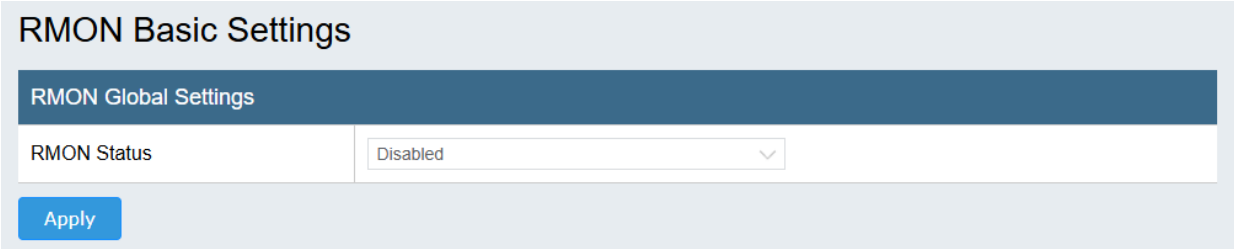


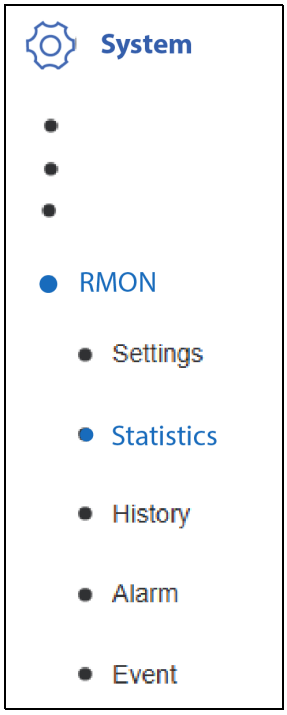
Figure 60. RMON Basic Settings Window

RMON Port Statistics Groups

Port statistics groups are used for the following functions:

- To view port statistics from the RMON portion of the MIB tree with SNMP NMS software.
- Combined with RMON alarms to alert you to defined traffic events.

Adding RMON Port Statistics Groups



To add RMON statistics groups to ports:

1. Select **System** > **RMON** > **Statistics** from the menu. The Ethernet Statistics Settings window is shown in Figure 61 on page 171. The table in the window lists the current Ethernet statistics groups, with the collected statistics.
2. To add a new RMON statistics group, configure the fields in Table 46.

Table 46. Ethernet Statistics Settings Window

Parameter	Description
Index	Enter a unique ID number for the new statistics group. The range is 1 to 65535. Some SNMP programs identify statistics groups by their ID numbers and not by port numbers. Consequently, statistics groups will be easier to identify if you make their ID numbers the same as the port numbers. For instance, a group assigned to port 16 should be assigned the ID number 16.
Port	Enter the port to be monitored. You can enter only one port.
Owner	Enter the name of the person responsible for this entry. This optional parameter is for switches that are managed by more than one person.

3. Click **Add** to add the new entry. New statistics groups become active as soon as you add them.
4. To add RMON statistics groups for other ports, repeat steps 2 and 3.

Note
Select **Save** from the menu to save your changes.

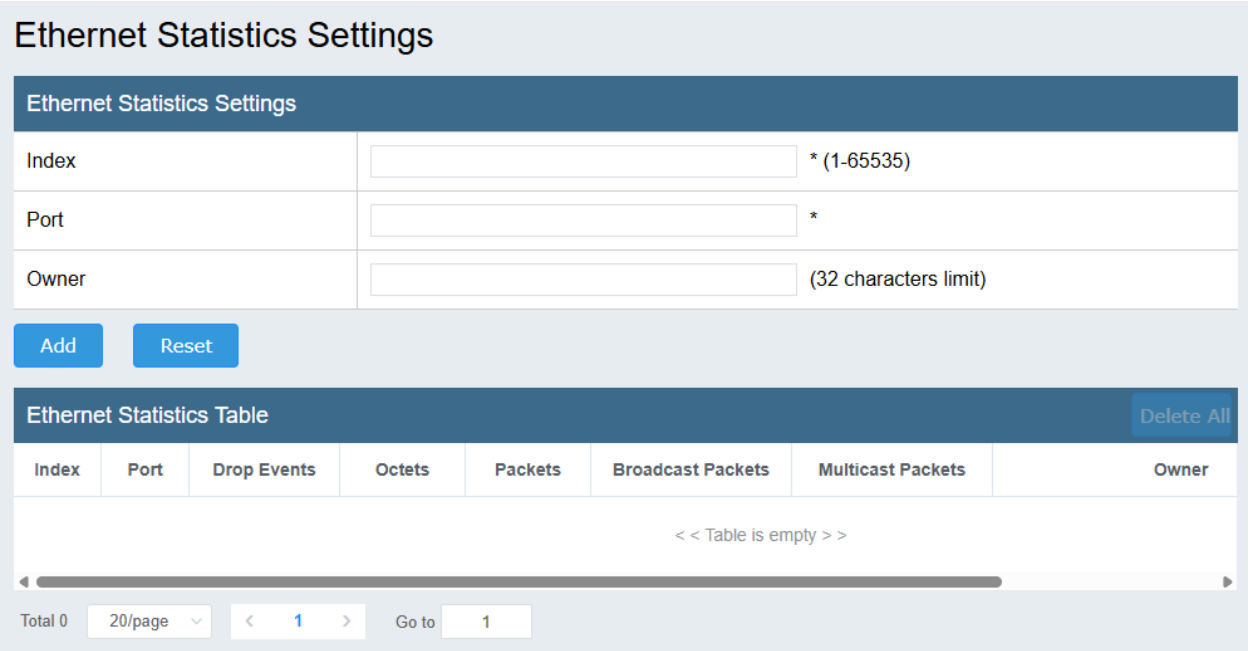


Figure 61. Ethernet Statistics Settings Window

Modifying or Deleting RMON Port Statistics Groups

Perform the following procedure to modify or delete port statistics groups:

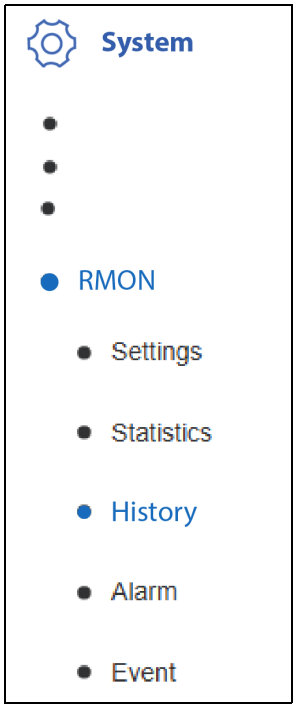
1. Select **System** > **RMON** > **Statistics** from the menu. Refer to Figure 61 on page 171.
2. To modify a statistics group, do the following:
   a. In the table at the bottom of the window. click **Modify** in the Action column of the group you want to modify. You can modify only one group at a time.
   b. Modify the fields as needed. Refer to Table 46 on page 170. You cannot change the policy index number.
3. To delete groups, do one of the following:
   - ❒ To delete a group, click **Delete** in the Action column.
   - ❒ To delete all the groups, click **Delete All**.
4. Click **Apply** to activate your changes.

Note
Select **Save** from the menu to save your changes.

RMON Histories

RMON histories are snapshots of port statistics taken by the switch at predefined intervals. By comparing the snapshots you can identify trends or patterns in the numbers or types of ingress packets on the ports. The snapshots can be viewed with SNMP NMS software in the RMON portion of the MIB tree.

Adding RMON History Groups



To add RMON histories:

1. Select **System** > **RMON** > **History** from the menu.

   The History Control Settings window is shown in Figure 62 on page 174. The table in the window lists the current RMON histories. The table columns are defined in Table 47. The Buckets Granted column lists the number of buckets for a history group the switch can support in its free memory. Depending on the number of histories and requested buckets, the switch might not be able to support all of the requested buckets.

2. Configure the fields in Table 47.

Table 47. History Control Settings Window

Field	Description
Index	Enter a unique ID number of the new group. The range is 1 to 65535. Some SNMP programs identify history groups by their ID numbers and not by the port numbers. Consequently, the groups will be easier to identify if you make their ID numbers the same as the port numbers. For instance, a history group assigned to port 16 should be assigned the ID number 16.
Port	Enter the port to be monitored. You can enter only one port.
Buckets Requested	Enter the maximum number of buckets for storing snapshots of the port's statistics. Each bucket can store one snapshot of RMON statistics of one port. The more buckets in a group, the more snapshots it can store. Different ports can have different numbers of buckets. The range is 1 to 50 buckets.

Table 47. History Control Settings Window (Continued)

Field	Description
Interval	Enter how frequently the switch is to take snapshots of the port's statistics. The range is 1 to 3600 seconds (1 hour). For example, enter 60 seconds to have the switch take a snapshot once a minute on a port.
Owner	Enter the name of the person responsible for the entry. This optional parameter is for switches that are managed by more than one person.

3. Click **Add** to add the new RMON history group.

   After you add a new group, the switch determines whether it has sufficient free memory to add all the requested buckets. If it does not have enough memory, it reduces the number of buckets to a supportable amount. If it does not have any available free memory, it cancels the history group.

   The switch takes the first snapshot at the end of the first interval. A history group that has an interval of 1800 seconds, for instance, does not take its first snapshot for 30 minutes. Once all the buckets of a group are full, the switch continues storing snapshots by deleting the oldest snapshots as it adds new snapshots. For instance, for a history group of three buckets, the switch deletes the first bucket when it adds the fourth bucket.

4. Repeat steps 2 and 3 to add additional RMON histories for other ports.

Note
Select **Save** from the menu to save your changes.

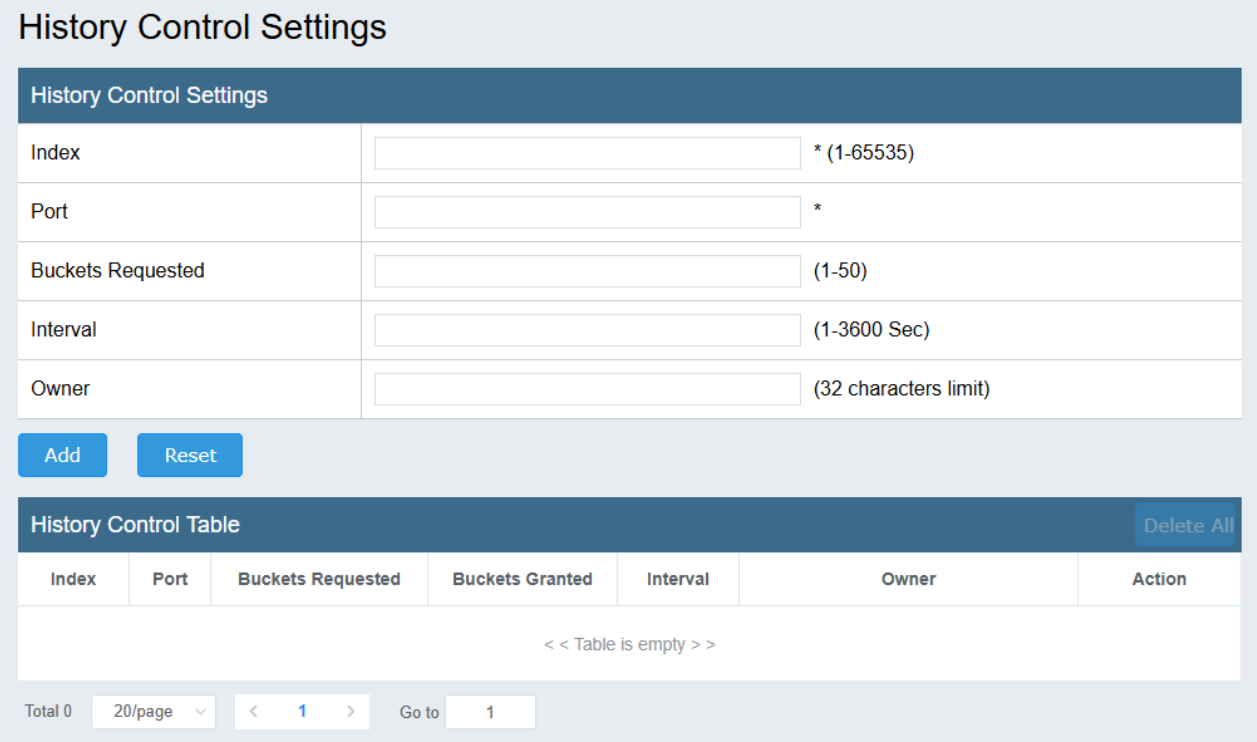


Figure 62. History Control Settings Window

Modifying or Deleting RMON History Groups

Perform the following procedure to modify or delete RMON history groups:

1. Select **System** > **RMON** > **History** from the menu. The History Control Settings window is shown in Figure 62 on page 174.
2. To modify a history group, do the following:
   a. In the table at the bottom of the window. click **Modify** in the Action column of the group you want to modify. You can modify only one group at a time.
   b. Change the fields, as needed. Refer to Table 47 on page 172. You cannot change the policy index number.
3. To delete history groups, do one of the following:
   - ❒ To delete a group, click **Delete** in the Action column.
   - ❒ To delete all the groups, click **Delete All**.
4. Click **Apply** to activate your change.

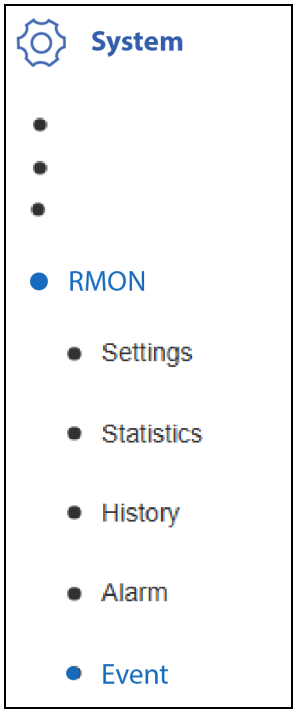
Note
Select **Save** from the menu to save your changes.

RMON Events

RMON events define the actions of RMON alarms. They specify the action the switch performs when port statistics cross defined thresholds, triggering an alarm. Events can log a message in the event log of the switch, send an SNMP trap to an SNMP network device, or both. Events can be used with more than one alarm. The switch supports up to 256 events.

Adding Events

To add RMON events:



1. Select **System** > **RMON** > **Event** from the menu. The RMON Event Settings window is shown in Figure 63 on page 177.

   The table in the window lists the current RMON events. The columns are described in Table 48. The Last Time Sent column contains the date and time when an event's alarm was last triggered.

2. To add a new RMON event, configure the fields in Table 48.

Table 48. RMON Event Settings Window

Field	Description
Index	Enter a unique ID number of the new group. The range is 1 to 65535.
Description	Enter a description of the event, up to 32 characters.
Type	Select the action that the switch is to perform when it determines that a statistics threshold of an alarm has been crossed. The options are listed here: - **None**: Take no action. - **Log**: Log a message in the event log. - **SNMP**: Send an SNMP trap. - **Log and Trap**: Log a message in the event log and send an SNMP trap.

Table 48. RMON Event Settings Window (Continued)

Field	Description
Community	Enter the SNMP trap community name to receive traps. Here are the guidelines: - This parameter is required when Type is SNMP or Log and Trap. - The community name has to already exist on the switch. Refer to “Adding SNMP Community Strings” on page 148. - The community name is case sensitive. - An event can have only one community name.
Owner	Enter the name of the person responsible for the entry. This optional parameter is for switches that are managed by more than one person.

3. Click **Add** to add the RMON event.
4. Repeat steps 2 and 3 to add more RMON events.

Note
Select **Save** from the menu to save your changes.

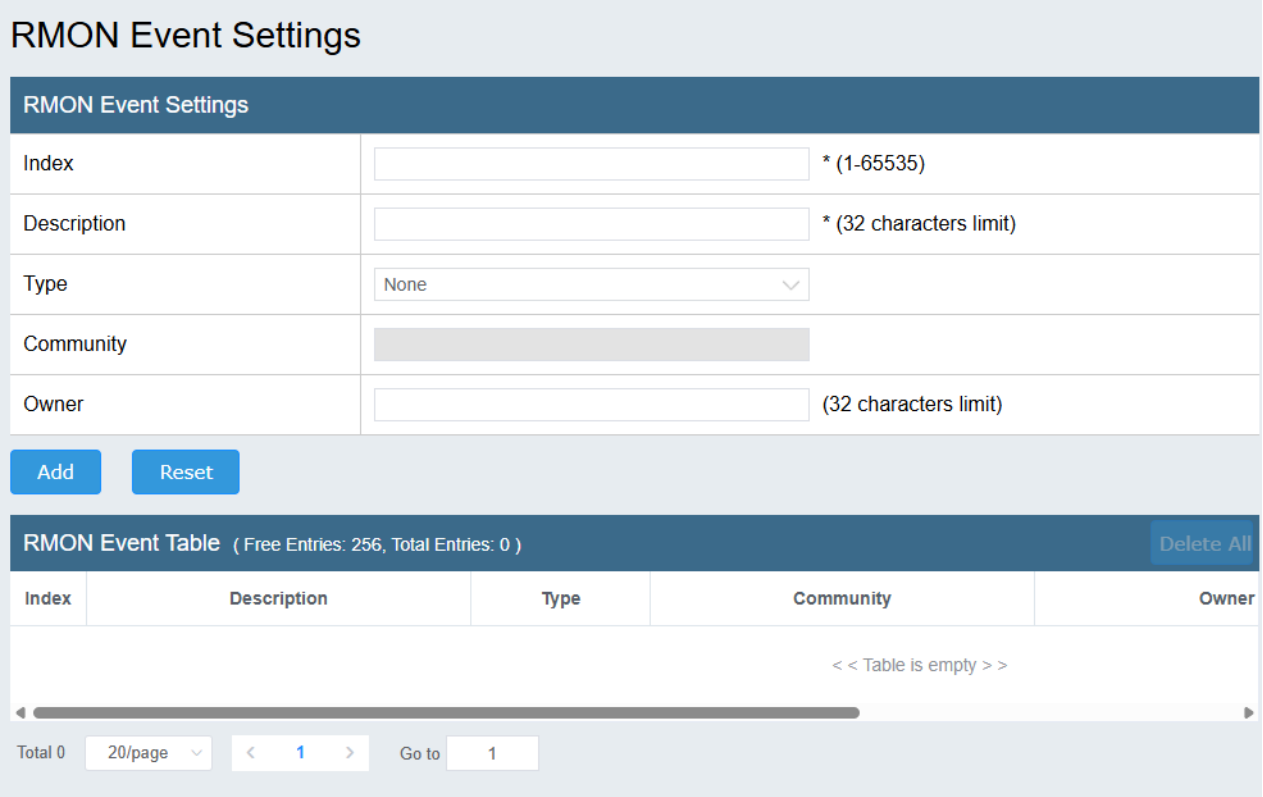


Figure 63. RMON Event Settings Window

Modifying or Deleting Events

To modify or delete RMON events:

Note
You cannot delete events that are assigned to alarms. You have to remove the events from the alarms or delete the alarms. Refer to “Modifying or Deleting Alarms” on page 182.

1. Select **System** > **RMON** > **Event** from the menu. Refer to Figure 63 on page 177. The RMON Event Settings window is shown in Figure 63 on page 177.
2. To modify an event, do the following:
   a. Click **Modify** in the Action column in the table. You can modify only one event at a time.
   b. Change the fields as needed. Refer to Table 48 on page 175. You cannot change the event index number.
3. To delete events, do one of the following:
   - To delete a event, click **Delete** in the Action column.

- To delete all the events, click **Delete All**.

4. Click **Apply** to activate your change.

Note
Select **Save** from the menu to save your changes.

RMON Alarms

RMON alarms are used to generate alert messages when packet activity on designated ports rises above or falls below defined threshold values. The alert messages can take the form of messages that are entered in the event log on the switch, traps that are sent to your SNMP network devices, or both. You can use alarms to alert you when traffic flows on ports raise above or fall below defined thresholds. The switch supports up to eight alarms.

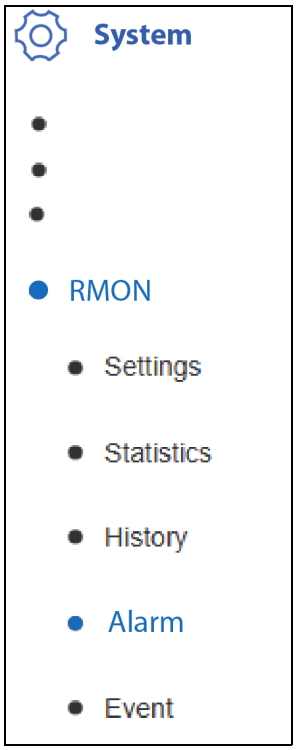
RMON alarms have rising threshold and falling thresholds. An alarm is triggered if the value of the monitored RMON statistic of the designated port raises above the rising threshold or falls below the falling threshold. The response of the switch is determined by an RMON event. The response can be to enter a message in the event log, send an SNMP trap, or both.

The frequency with which the switch samples the thresholds of an alarm against the actual RMON statistic is controlled by a time interval parameter. You can adjust this interval for each alarm.

RMON alarms have the following three components:

- RMON statistics group: A port has to have an RMON statistics group to have an alarm. When you add an alarm, you specify the port to which it is to be assigned, not by the port number, but rather by the ID number of the port's statistics group. (As explained in "RMON Port Statistics Groups" on page 170, statistics groups are also used to remotely view port statistics in the RMON portion of the MIB tree.)
- RMON event: An event specifies the action of the switch when the ingress packet activity on a port crosses a statistical threshold defined in an alarm. The choices are to log a message in the event log of the switch, send an SNMP trap to an SNMP network device, or both.
- Alarm: The last component is the alarm itself. It defines the port statistic to be monitored and the rising and falling thresholds that trigger the switch to perform the event. The thresholds of an alarm can have the same event or different events.

Adding RMON Alarms



To add RMON alarms:

1. Select **System** > **RMON** > **Alarm** from the menu.

   The RMON Alarm Settings page is shown in Figure 64 on page 182. The table in the window lists the current RMON alarms. The table columns are defined in Table 49.

2. To add a new alarm, configure the fields in Table 49.

Table 49. RMON Alarm Settings Window

Field	Description
Index	Enter a unique ID number for the new alarm. The range is 1 to 65535.
Interval	Enter the time period (in seconds) the switch waits to poll the statistics group to determine whether a threshold has been crossed. The range is 1 to 2^{31}-1 (2147483647) seconds.
Variable	Enter the RMON MIB object that the event is to monitor.
Sample Type	Select the change to the port statistic that triggers the alarm: Here are the choices: - Absolute Value: Compares the current statistic value against the threshold. - Delta Value: Compares the difference between the previous and current statistic values against the threshold.
Rising Threshold	Enter the rising threshold for the monitored statistics that, when crossed, causes the switch to perform the specified rising event. The range is 0 to 2^{31}-1 (2147483647).
Falling Threshold	Enter the falling threshold for the monitored statistics that, when crossed, causes the switch to perform the specified falling event. The range is 0 to 2^{31}-1 (2147483647).

Table 49. RMON Alarm Settings Window (Continued)

Field	Description
Rising Event Index	Enter the event index for the rising threshold. The event determines the action of the switch when the monitored statistic exceeds the rising threshold. The range is 1 to 65535. The specified event should already exist on the switch. Refer to “RMON Events” on page 175. Rising and falling thresholds can use the same event. This field is required.
Falling Event Index	Enter the event index for the falling threshold. The event determines the action of the switch when the monitored statistic falls below the falling threshold. The range is 1 to 65535. The specified event should already exist on the switch. Refer to “RMON Events” on page 175. The rising and falling thresholds can use the same event. This field is required.
Owner	Enter the name of the person responsible for this entry. This optional parameter is for switches that are managed by more than one person.

3. Click **Apply** to add the new alarm to the table. To return all parameters to their default values, click **Reset**.

4. Repeat steps 2 and 3 to add more RMON alarms.

Note
Select **Save** from the menu to save your changes.

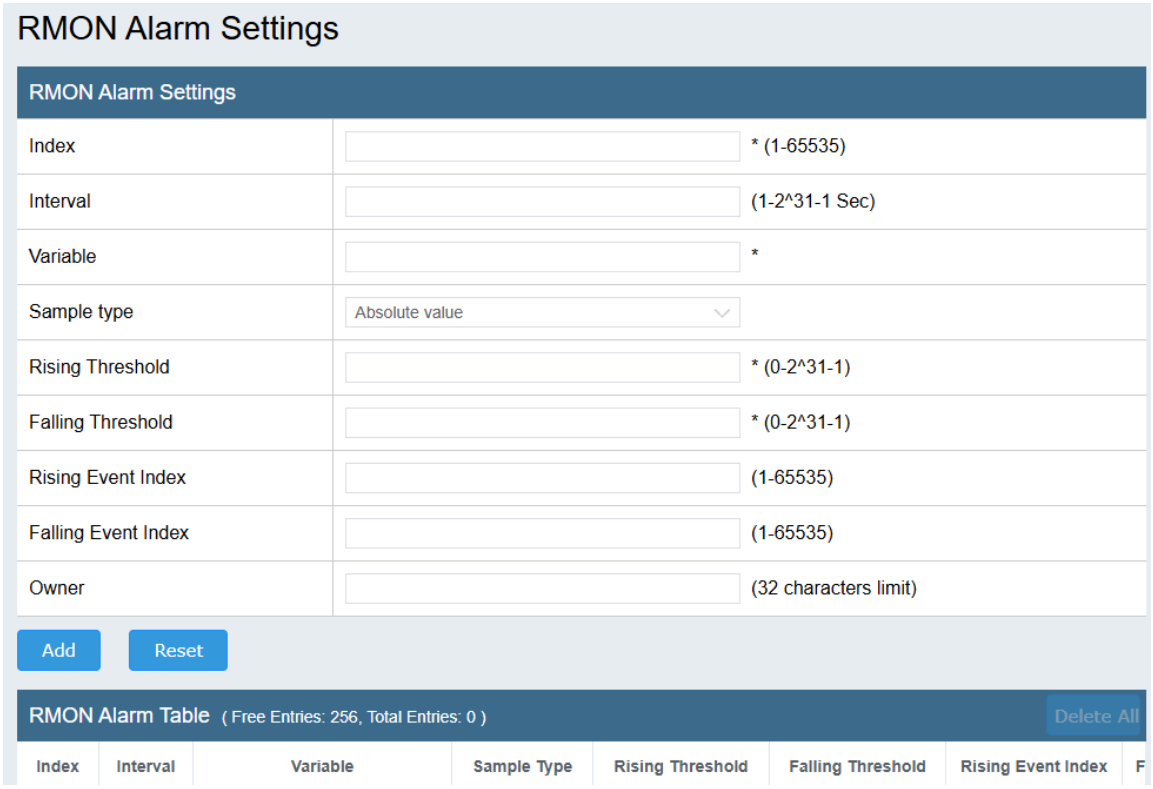


Figure 64. RMON Alarm Settings Window

Modifying or Deleting Alarms

To modify or delete RMON alarms:

1. Select **System** > **RMON** > **Alarms** from the menu. The RMON Event Settings window is shown in Figure 64 on page 182.
2. To modify an alarm, do the following:
   a. Click **Modify** in the Action column in the table. You can modify only one alarm at a time.
   b. Change the fields, as needed. Refer to Table 49 on page 180. You cannot change the event index number.
3. To delete alarms, do one of the following:
   - ❒ To delete an alarm, click **Delete** in the Action column.
   - ❒ To delete all the alarms, click **Delete All**.
4. Click **Apply** to activate your changes.

Note
Select **Save** in the menu to save your changes.

Chapter 17

Traffic Statistics and Charts

This chapter describes traffic charts in the following sections:

- “Network Statistics Overview” on page 184
- “Displaying Traffic Statistics” on page 185
- “Displaying Port Error Statistics” on page 186

Network Statistics Overview

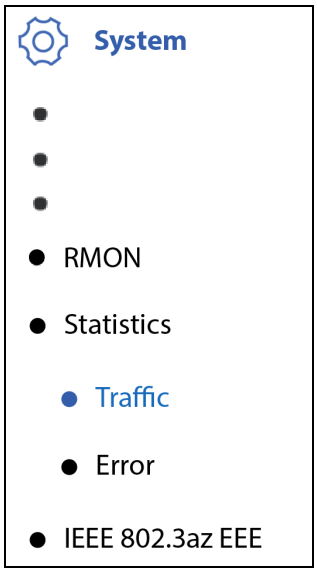
Statistics provide important information for troubleshooting switch problems at the port level. The switch provides a versatile set of statistics charts you can customize for your needs, including (depending upon the chart) the ports whose statistics you want to view and the chart colors.

Note
Your web browser has to have the Java SSV Helper plug-in to display the network traffic statistics charts.

There are two types of statistics charts:

- Traffic: This chart displays traffic statistics per port. You can select from 24 statistics and 12 chart colors. Refer to “Displaying Traffic Statistics” on page 185.
- Error: This chart displays discard and error counts for ports. Refer to “Displaying Port Error Statistics” on page 186.

Displaying Traffic Statistics



Perform the following procedure to display traffic statistics per port:

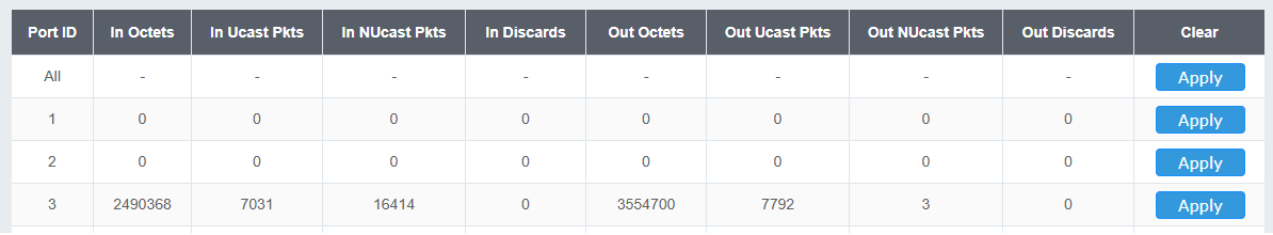
1. Select **System** > **Statistics** > **Traffic** from the menu.

   The Traffic Comparison Chart window is shown in Figure 65 on page 185. The traffic statistic are defined in Table 50.

Table 50. Port Traffic Statistics

Statistics	Definition
In Octets	Displays the total number of inbound octets.
In Ucast Pkts	Displays the total number of inbound unicast packets.
In NUcast Pkts	Displays the total number of inbound non-unicast packets.
In Discards	Displays the total number of inbound discarded packets.
Out Octest	Displays the total number of outbound octets.
Out Ucast Pkts	Displays the total number of outbound unicast packets.
Out NUcast Pkts	Displays the total number of outbound non-unicast packets.
Out Discards	Displays the total number of outbound discarded packets.

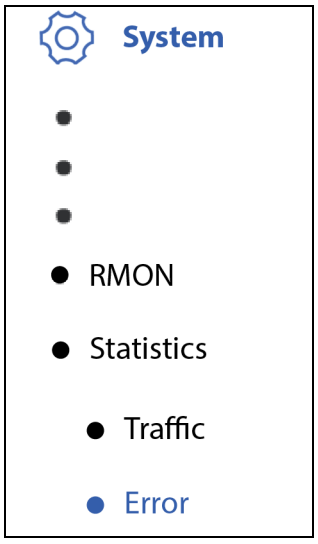
2. To clear traffic statics for a port, click **Apply** in the Clear column.



Port ID	In Octets	In Ucast Pkts	In NUcast Pkts	In Discards	Out Octets	Out Ucast Pkts	Out NUcast Pkts	Out Discards	Clear
All	-	-	-	-	-	-	-	-	Apply
1	0	0	0	0	0	0	0	0	Apply
2	0	0	0	0	0	0	0	0	Apply
3	2490368	7031	16414	0	3554700	7792	3	0	Apply

Figure 65. Statisticcs Traffic Information Window

Displaying Port Error Statistics



To display port error statistics:

1. Select **System** > **Statistics** > **Error** from the menu. The Statistics Error Information window is shown in Figure 66. The statistics are defined in Table 51
2. To clear error statics for a port, click **Apply** in the Clear column.

Table 51. Error Statistics

Statistics	Definition
InErrors (Inbound Errors - Pkts)	Displays the number of inbound packets with errors.
OutErrors (Outbound Error Rate - Pkts)	Displays the rate of outbound errors.
DropEvents (Dropped Events)	Displays the number of packets dropped on the port
CRCAlignErrors (CRC Alignment Errors)	Displays the rate of Ethernet packets with CRC alignment errors.
UnderSizePkts (Ethernet Undersize Packets)	Displays the rate of undersized Ethernet packets in packets per second.
OverSizePkts (Ethernet Oversize Packets)	Displays the number of oversized Ethernet packets.
Fragments	Displays the number of fragments on the port
Collisions	Displays the number of collisions on the port.

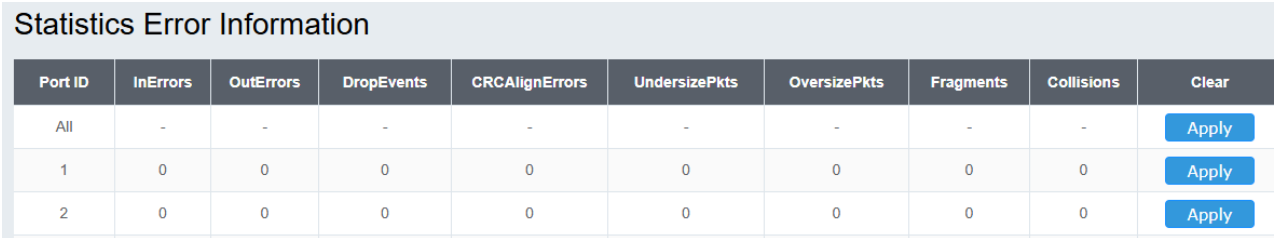
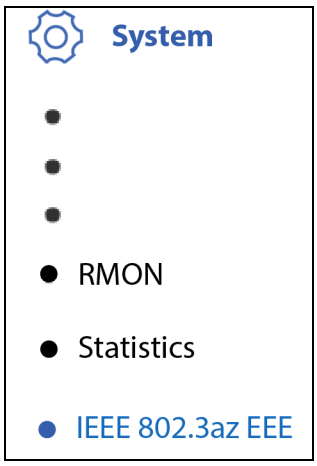


Figure 66. Statistics Error Information Window

Chapter 18

Managing IEEE

Description and Procedure



The switch supports IEEE 802.3az Energy-Efficient Ethernet (EEE), which saves engery by reducing power consumption during periods of no data activity. When the feature is enabled and all ports are inactive, the switch conserves electricity by placing the Ethernet circuitry in a special sleep mode. When data activity resumes, the switch automatically resumes normal operations. The default setting for the feature is disabled.

To enable or disable IEEE 802.3az EEE:

1. Select **System** > **IEEE 802.3az EEE** from the menu. The IEEE 802.3az EEE window is shown in Figure 67.
2. Select either **Enabled** or **Disabled** from the pull-down menu. The default is disabled.

Note
Select **Save** from the menu to save your changes.

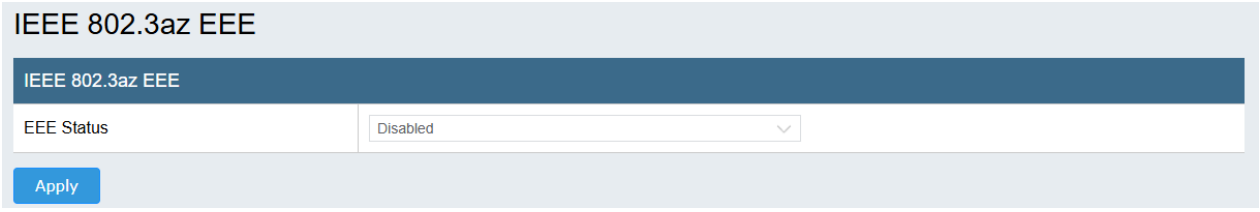


Figure 67. IEEE Window

Section III

Network Menu

This section contains the following chapters:

- Chapter 19, “Basic Port Settings” on page 191
- Chapter 20, “Spanning Tree and Rapid Spanning Tree Protocols” on page 197
- Chapter 21, “Multiple Spanning Tree Protocol Overview” on page 217
- Chapter 22, “Multiple Spanning Tree Protocol” on page 233
- Chapter 23, “Static Port Trunks” on page 249
- Chapter 24, “LACP Trunks” on page 257
- Chapter 25, “Port Mirroring” on page 269
- Chapter 26, “Loopback Detection” on page 275
- Chapter 27, “Static Unicast MAC Addresses” on page 281
- Chapter 28, “Static Multicast MAC Addresses” on page 289
- Chapter 29, “IGMP Snooping” on page 295
- Chapter 30, “MLD Snooping” on page 305
- Chapter 31, “Multicast VLANs” on page 313
- Chapter 32, “Multicast Filtering” on page 327
- Chapter 33, “Bandwidth Control” on page 329
- Chapter 34, “802.1Q Tagged Virtual LANs” on page 337
- Chapter 35, “Private Virtual LAN” on page 353
- Chapter 36, “VLAN Forwarding Modes” on page 359
- Chapter 37, “GARP VLAN Registration Protocol” on page 361
- Chapter 38, “Voice VLAN” on page 371
- Chapter 39, “Link Layer Discovery Protocol” on page 381
- Chapter 40, “MAC VLANs” on page 397

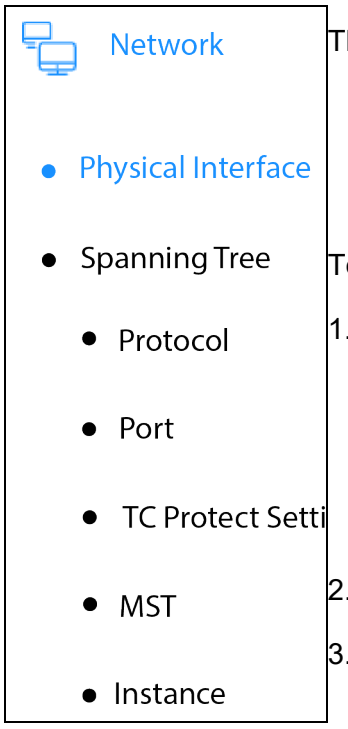
Chapter 19

Basic Port Settings

Description and Procedure

This procedure explains how to configure the following port settings:

- Enable or disable ports (referred to as Admin status)
- Set speed and duplex modes
- Forward or block jumbo frames
- Enable or disable flow control
- Forward or block Extensible Authentication Protocol (EAP) frames
- Forward or block spanning tree protocol BPDU frames



The procedure also displays the following parameters:

- Trunk group number
- Port type
- Link status

To view or configure the basic parameter settings on switch ports:

1. Select **Network** > **Physical Interface** from the menu.

   The Physical Interface window is shown in Figure 68 on page 192. For a quick way to set all the ports to the same setting, use the All row at the top of the table. Parameters set in the All row are applied to all ports. The Ignore setting means the All row is ignored for that parameter.

2. Configure the port settings in Table 52 on page 192 and click **Apply**.
3. Select **Save** from the menu to save your changes.

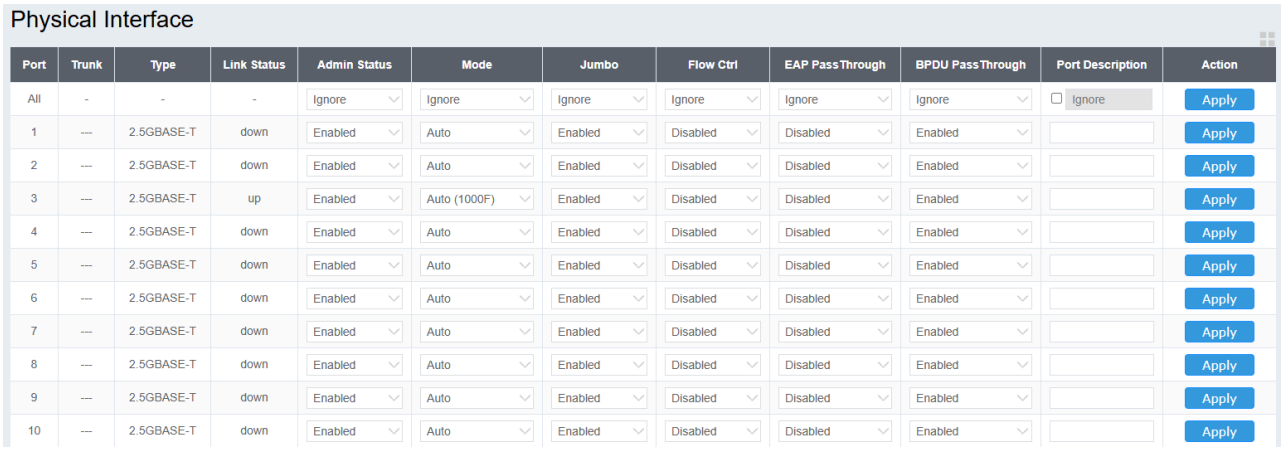


Figure 68. Physical Interface Window

Table 52. Physical Interface (Port) Settings

Parameter	Definition
Port	Displays the port number.
Trunk	Displays the static or LACP trunk number. This value is empty for ports that are not members of trunks. Refer to Chapter 25, “Static Port Trunks” on page 219 or Chapter 26, “LACP Trunks” on page 227.
Type	Displays the port type. Examples include: - Copper ports: 10/100/1000M - Fiber optic ports: 100/1000M
Link Status	Displays the link state: - Up -The port has a valid link to a network device. - Down -The port does not have a link to a network device. Examples of the Down state are listed here: - The port is not connected to a network device. - The port is disabled. - The network device is not powered on. - There is a problem with the copper or fiber optic cable.

Table 52. Physical Interface (Port) Settings (Continued)

Parameter	Definition
Admin Status	Enables or disables ports. The menu has these options: - **Enabled**: Enables the port. The switch forwards network traffic on the port. This is the default setting. - **Disabled**: Disables the port. The switch blocks all ingress and egress traffic on the port. Reasons for disabling ports include: - Secure unused ports to protect the network from unauthorized connections. - Ports are under network attack. - The copper or fiber optic cable has a problem. - The network device is not operating correctly.
Mode	Sets the speed and duplex mode of the port. The menu has these options: - **Auto** -Sets the port to Auto-Negotiation. Once a port establishes a link to a network device, the operating speed and duplex mode are displayed in parentheses (for example, “1000F” for 1000M full duplex mode). This is the default setting. - **1000/Full**: Sets the port to 1G, full-duplex mode. - **100/Full**: Sets the port to 100M, full-duplex mode. - **100/Half**: Sets the port to 100M, half-duplex mode.

Table 52. Physical Interface (Port) Settings (Continued)

Parameter	Definition
Mode (Continued)	Here are guidelines to setting speed and duplex mode: - Fiber port support force mode setting, default is Auto mode. - Do not use the Auto setting for copper ports that are connected to remote network devices that do not support Auto-Negotiation. Instead, manually set the speed and duplex mode on copper port to match the remote devices.
Jumbo	Enables or disables support for jumbo frames of up to 10KB on the port. The menu has the following selections: - **Enabled**: Enables jumble frame support. This is the default setting. - **Disabled**: Disables jumble frame support. The port discards ingress and egress jumbo frames. You cannot enable jumbo frame support on ports where CoS is also enabled. Refer to “Mapping CoS Priorities to Egress Queues” on page 374.
Flow Control	Enables or disables flow control. Ports use flow control to temporarily stop their remote counterparts from sending packets, to allow them time to process packets already stored in their buffers. Ports initiate flow control by sending pause packets. The switch can also respond to pause packets from other devices by temporarily delaying the transmission of network packets on ports. The pull-down menu has these options: - **Enabled**: Enables flow control. The port transmits pause packets and responds to pause packets from its network counterpart. - **Disabled**: Disables flow control. This is the default setting.

Table 52. Physical Interface (Port) Settings (Continued)

Parameter	Definition
EAP Pass-through	Enables or disables forwarding of Extensible Authentication Protocol (EAP) packets. The menu has these options: - **Enabled**: The port forwards ingress and egress EAP packets. - **Disabled**: The port discards ingress and egress EAP packets. This is the default setting,
BPDU Pass-through	Enables or disables forwarding of spanning tree BPDU packets by the switch from other network devices. The menu has these options: - **Enabled**: The port forwards ingress spanning tree BPDU packets from other network devices. This is the default setting. - **Disabled**: The port does not pass-through ingress spanning tree BPDU packets. You have to disable BPDU pass-through on all ports to enable spanning tree on the switch.
Port Description	Alpha numeric description of the port's function.

Chapter 20

Spanning Tree and Rapid Spanning Tree Protocols

This chapter explains the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) in the following sections:

- ❒ “STP and RSTP Overview” on page 198
- ❒ “Configuring STP and RSTP Global Settings” on page 206
- ❒ “Configuring STP and RSTP Port Settings” on page 210
- ❒ “Configuring Topology Change Protection” on page 214

STP and RSTP Overview

The performance of an Ethernet network can be adversely affected by the existence of physical loops in the network topology. Loops exist when two or more nodes on a network can transmit packets to each other over more than one physical path. Packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and can significantly reduce network performance.

STP and RSTP prevent data loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode, leaving only one main active path. STP and RSTP can also activate a redundant path if a main path go down, thereby maintaining network connectivity.

Where the two protocols differ is in the time each takes to complete the process referred to as *convergence*. With the convergence process, when a change is made to the network topology, such as the addition of a new bridge, the spanning tree protocol has to determine whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain connections between the various network segments.

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

RSTP is much faster. It can complete convergence in seconds, and as such, greatly diminish the possible impact the process can have on your network. The STP implementation complies with the IEEE 802.1d standard.

Only one spanning tree at a time can be active on the switch.

The following subsections provide a basic overview on how STP and RSTP operate and define the different adjustable parameters. For further information about STP and RSTP, refer to IEEE Std 802.1D and IEEE Std 802.1w, respectively.

Bridge Priority and the Root Bridge

When a spanning tree protocol is activated on a network, the bridges select of a *root bridge*. A root bridge distributes network topology information to the other network bridges and is used by the other bridges to determine if there are redundant paths in the network.

A root bridge is selected by the *bridge priority* number, also referred to as the bridge identifier, and sometimes the bridge's MAC address. The bridge with the lowest bridge priority number in the network is selected as the root bridge. If two or more bridges have the same lowest bridge priority

number, the one with the lowest MAC address is designated as the root bridge.

You can change the bridge priority number on the switch. You can designate which switch on your network is the root bridge by giving it the lowest bridge priority number. You may also consider which bridge should function as the backup root bridge in the event you need to take the primary root bridge off line and assign that bridge the second lowest bridge identifier number.

The bridge priority has a range of 0 to 61440 in increments of 4096. You specify the increment that represents the desired bridge priority value. The range is divided into the following sixteen increments:

- 0
- 4096
- 8192
- 12288
- 16384
- 20480
- 24576
- 28672
- 32768
- 36864
- 40960
- 45056
- 49152
- 53248
- 57344
- 61440

Path Costs and Port Costs

After selecting the root bridge, the bridges determine if the network contains redundant paths and, if one is found, select a preferred path while placing the redundant paths in a backup or blocking state.

Where there is only one path between a bridge and the root bridge, the bridge is referred to as the *designated bridge*, and the port through which the bridge is communicating with the root bridge is referred to as the *root port*.

If redundant paths exist, the bridges that are a part of the paths must determine which path is the primary, active path, and which path(s) are placed in the standby, blocking mode. This is accomplished by calculating *path costs*. The path offering the lowest cost to the root bridge becomes the primary path, and all other redundant paths are placed into a blocking state.

Path cost is determined by evaluating *port costs*. Every port on a bridge participating in STP has a cost associated with it. The cost of a port on a bridge is typically based on port speed. The faster the port, the lower the port cost. The exception to this is the ports on the root bridge, where all ports have a port cost of 0.

Path cost is the sum of the port costs between a bridge and the root bridge.

The port cost of a port on the switch is adjustable. For STP and RSTP, the range is from 0 to 200,000,000.

Port Priority

If two paths have the same port cost, the bridges must select a preferred path. In some instances, this can involve the use of the *port priority* parameter which is used as a tie breaker when two paths have the same cost.

The range for port priority is 0 to 240. As with bridge priority, this range is broken into increments, in this case, multiples of 16. To select a port priority for a port, you enter the desired value. Table 53 on page 200 lists the values that are valid.

Table 53. Valid Port Priority Values

Step	Port Priority
1	0
2	16
3	32
4	48
5	64
6	80
7	96
8	112
9	128

Table 53. Valid Port Priority Values (Continued)

Step	Port Priority
10	144
11	160
12	176
13	192
14	208
15	224
16	240

Forwarding Delay and Topology Changes

If there is a change in the network topology due to a failure, removal, or addition of active components, the active topology might also change. This might trigger a change in the state of some blocked ports. However, a change in a port state is not activated immediately.

It may take time for the root bridge to notify all bridges that a topology change has occurred, especially if it is a large network. A temporary data loop could occur if a topology change is made before all bridges have been notified and that could adversely impact network performance.

To forestall the formation of temporary data loops during topology changes, a port designated to change from blocking to forwarding passes through two additional states - listening and learning - before it begins to forward frames. The amount of time a port spends in these states is set by the forwarding *delay* value. This value states the amount of time that a port spends in the listening and learning states prior to changing to the forwarding state.

The forwarding delay value is adjustable on the switch. The appropriate value for this parameter depends on a number of variables; the size of your network is a primary factor. For large networks, you should specify a value large enough to allow the root bridge sufficient time to propagate a topology change throughout the entire network. For small networks, you should specify a smaller value so that the time for a topology change is optimized for minimum data loss.

Note
The forwarding delay parameter applies only to ports that are operating in the STP mode.

Hello Time and Bridge Protocol Data Units (BPDU)

The bridges that are part of a spanning tree domain communicate with each other using a bridge broadcast frame that contains a special section devoted to carrying STP or RSTP information. This portion of the frame is referred to as the bridge protocol data unit (BPDU). When a bridge is brought on-line, it issues a BPDU in order to determine whether a root bridge has already been selected on the network, and if not, whether it has the lowest bridge priority number of all the bridges and should therefore become the root bridge.

The root bridge periodically transmits a BPDU to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The frequency with which the root bridge sends out a BPDU is called the *hello time*. This is a value that you can set on the switch. The interval is measured in seconds. If the switch is selected as the root bridge of a spanning tree domain, and the hello time is set to the default of two seconds, it transmits a BPDU every two seconds.

Point-to-Point and Edge Ports

This section applies only to RSTP. Part of the task of configuring RSTP is defining the port types on the bridge, which is directly related to the device(s) connected to the port. With the port types defined, RSTP can reconfigure a network much quicker than STP when a change in network topology is detected.

There are two possible selections:

- Point-to-point port
- Edge port

If a bridge port is connected to another bridge or router port, it normally operates in full-duplex mode and is functioning as a point-to-point port. Figure 69 on page 203 illustrates two switches that are connected with one data link. This link is operating between two point-to-point ports.

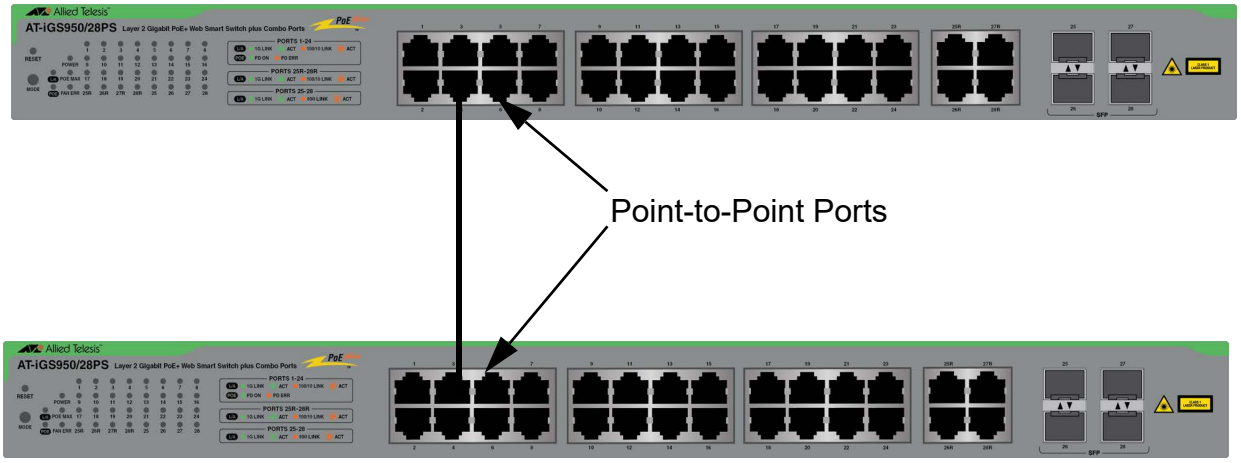


Figure 69. Point-to-Point Ports

A port operates as an edge port when it is connected to a network terminal device such as a workstation or a server. An edge port on a bridge should not have any STP or RSTP devices connected to it either directly or through another device connected to that port. In this configuration, since the port has no STP or RSTP devices connected to it, it will always forward network traffic. Figure 70 illustrates a port functioning as an edge port.

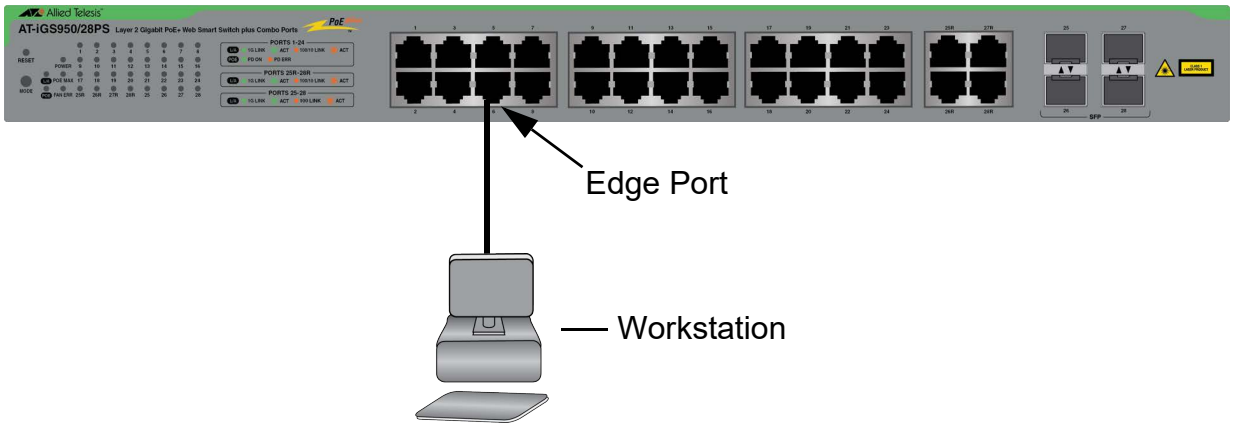


Figure 70. Edge Port

Mixed STP and RSTP Networks

RSTP IEEE 802.1w is fully compliant with STP IEEE 802.1d. As such, RSTP is compatible with STP. A network can have bridges running STP and RSTP.

If you decide to activate spanning tree on the switch, Allied Telesis recommends RSTP instead of STP, even if all of the other switches in the network are running STP. The switch can combine RSTP with the STP of the other switches. The switches monitor the traffic on each port for BPDU packets. Ports that receive RSTP BPDU packets operate in RSTP mode, while ports receiving STP BPDU packets operate in STP mode.

Spanning Tree and VLANs

The spanning tree implementation on the switch supports a single-instance spanning tree that encompasses all switch ports. If the ports are grouped into VLANs, spanning tree crosses VLAN boundaries. This can pose a problem in networks containing multiple VLANs that span two bridges and are connected with untagged ports. In this situation, spanning tree might block data links because it detects suspected data loops, which can cause VLAN fragmentation.

This is illustrated in Figure 71. VLANs 1 to 3 span two switches. The separate VLAN parts on the two switches are connected by dedicated links.

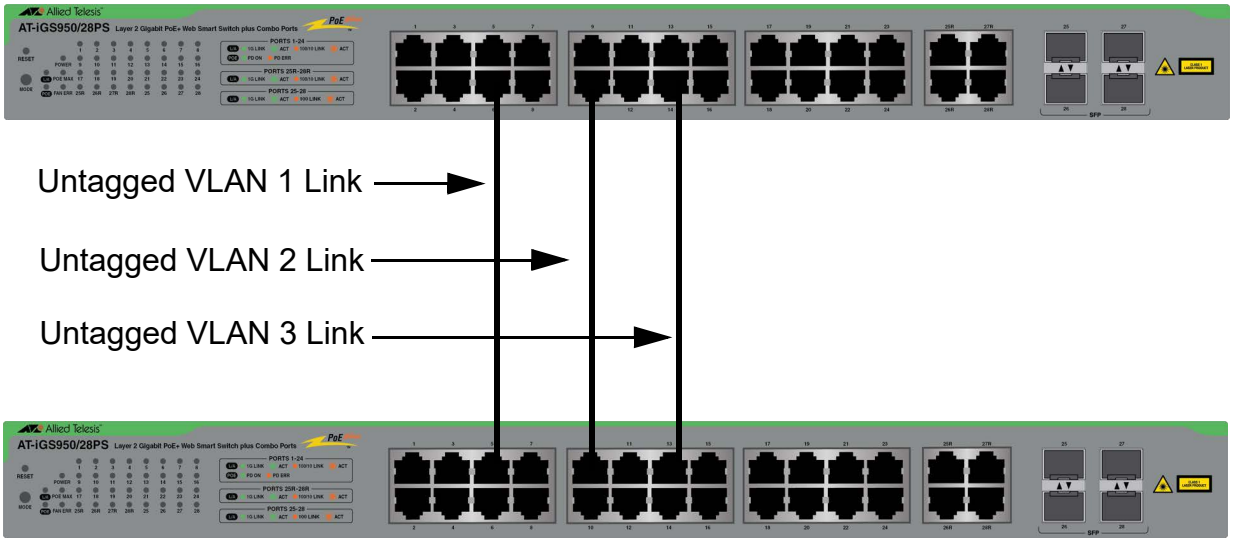


Figure 71. STP and VLAN Fragmentation with Untagged Ports

When STP or RSTP is activated on the switches, two links are disabled because the three links represent loops, even though they reside in different VLANs. Refer to Figure 72 on page 205. As a result, two VLANs are disconnected between the bridges. In this example, the ports on the top switch linking the two parts of the VLANs 2 and 3 are changed to the blocking state, disrupting their VLAN connections.

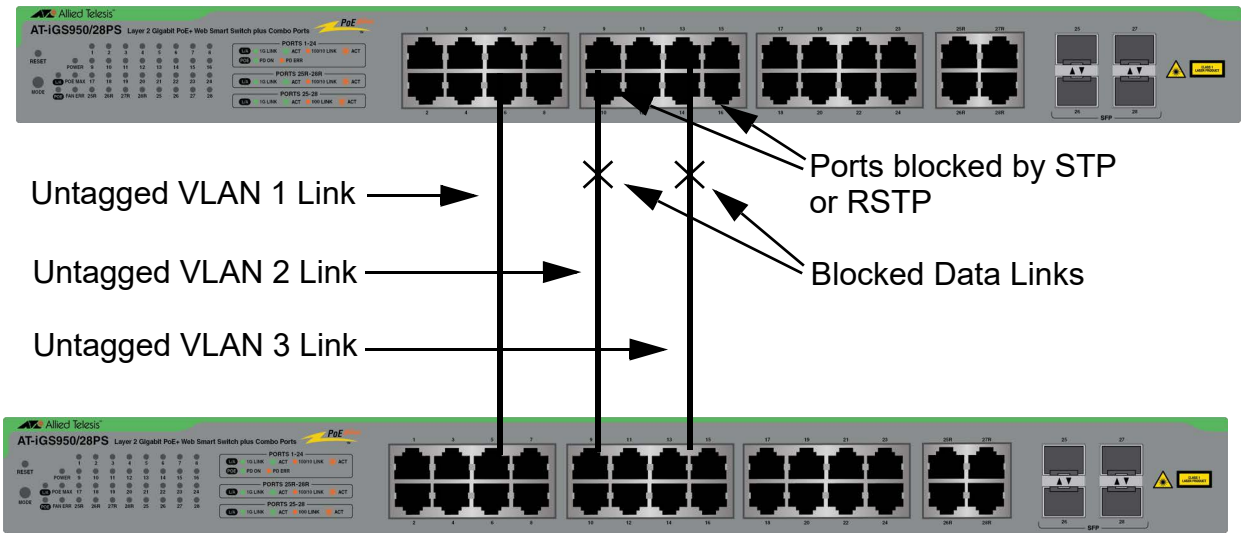


Figure 72. STP and VLAN Fragmentation

You can avoid this problem by either not activating the spanning tree protocol or connecting the switches using tagged ports. As explained in Chapter 34, “802.1Q Tagged Virtual LANs” on page 337, a link of tagged ports can carry traffic from multiple VLANs simultaneously. Refer to Figure 73.

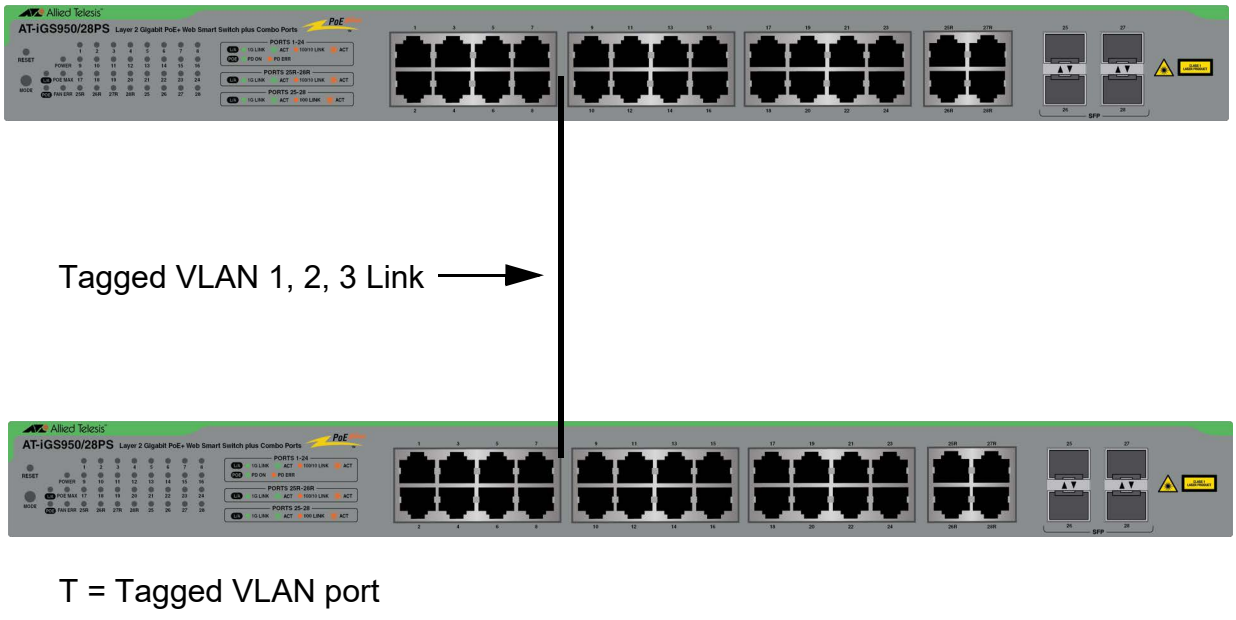
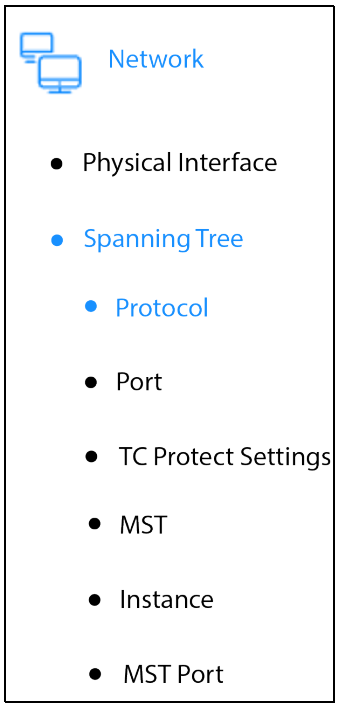


Figure 73. STP and VLAN Compatibility with Tagged Ports

Configuring STP and RSTP Global Settings



This section explains how to configure the following spanning tree protocol parameters:

- ❒ Enable or disable spanning tree protocol
- ❒ Choose STP or RSTP as the active protocol
- ❒ Configure global (non port-specific) settings

Note
You have to disable BPDU pass-through on all ports before enabling spanning tree protocol. Refer to Chapter 19, “<$paratextt191.

Note
The switch briefly stops forwarding Ethernet traffic when spanning tree is enabled or disabled.

Note
To save your changes, click **Save** at the bottom of the menu.

To configure basic spanning tree protocol parameters:

1. Select **Network** > **Spanning Tree** > **Protocol** from the menu. The Spanning Tree Protocol Settings window is shown in Figure 74 on page 209. Configure the settings in Table 54.

Table 54. Spanning Tree Protocol Settings Window for STP and RSTP

Field	Definition
Global STP Status	Select one of the following from the menu: - **Enabled**: Activates the spanning tree protocol on the switch. You have to enable the protocol to configure the settings in the window. - **Disable**: Deactivates the spanning tree protocol. This is the default setting.

Table 54. Spanning Tree Protocol Settings Window for STP and RSTP

Field	Definition
Protocol Version	Select the spanning tree version from the menu: - STP - RSTP - This is the default setting. - MSTP
Bridge Priority	Select the priority number for the bridge. This number is used to determine the root bridge of the spanning tree domain. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. If a root bridge goes off-line, the bridge with the next lowest priority number automatically becomes the root bridge. The range is 0 (zero) to 61,440 in increments of 4096. The highest priority is 0. The default is 32768.
Maximum Age	Enter the maximum length of time the bridge stores bridge protocol data units (BPDUs). Bridges in a bridged LAN use the aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs) and to delete expired data units. For example, when set to the default value 20 seconds, bridges delete configuration messages after 20 seconds. The range is 6 to 40 seconds. Observe the following rules when setting the maximum age: - Maximum Age must be greater than (2 x (Hello Time + 1)) - Maximum Age must be less than (2 x (Forward Delay - 1)) - The aging time for BPDUs is different from the aging time for the MAC address table.

Table 54. Spanning Tree Protocol Settings Window for STP and RSTP

Field	Definition
Hello Time	Enter the time interval at which the root bridge transmits BPDUs to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. The range is 1 to 10 seconds. The default is 2 seconds.
Forward Delay	Enter the waiting period in seconds before a bridge changes to a new state, for example, becomes the new root bridge after a topology change. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.
Transmit Hold Count	Applies to MSTP. Refer to “Configuring MSTP Global Settings” on page 234.
Max Hop Count	Applies to MSTP. Refer to “Configuring MSTP Global Settings” on page 234.
Root Information	
Root Bridge	Displays the MAC address of the root bridge of the spanning tree domain. This value is zero when the spanning tree protocol is disabled.
Root Cost	Displays the sum of the root port costs of the bridges between the switch’s root port and the root bridge.
Root Maximum Age	Displays the maximum age setting on the root bridge.
Root Forward Delay	Displays the forward delay setting on the root bridge.
Root Port	Displays the port on the switch leading to the root bridge. This value will be zero when the switch is the root bridge or spanning tree is disabled.

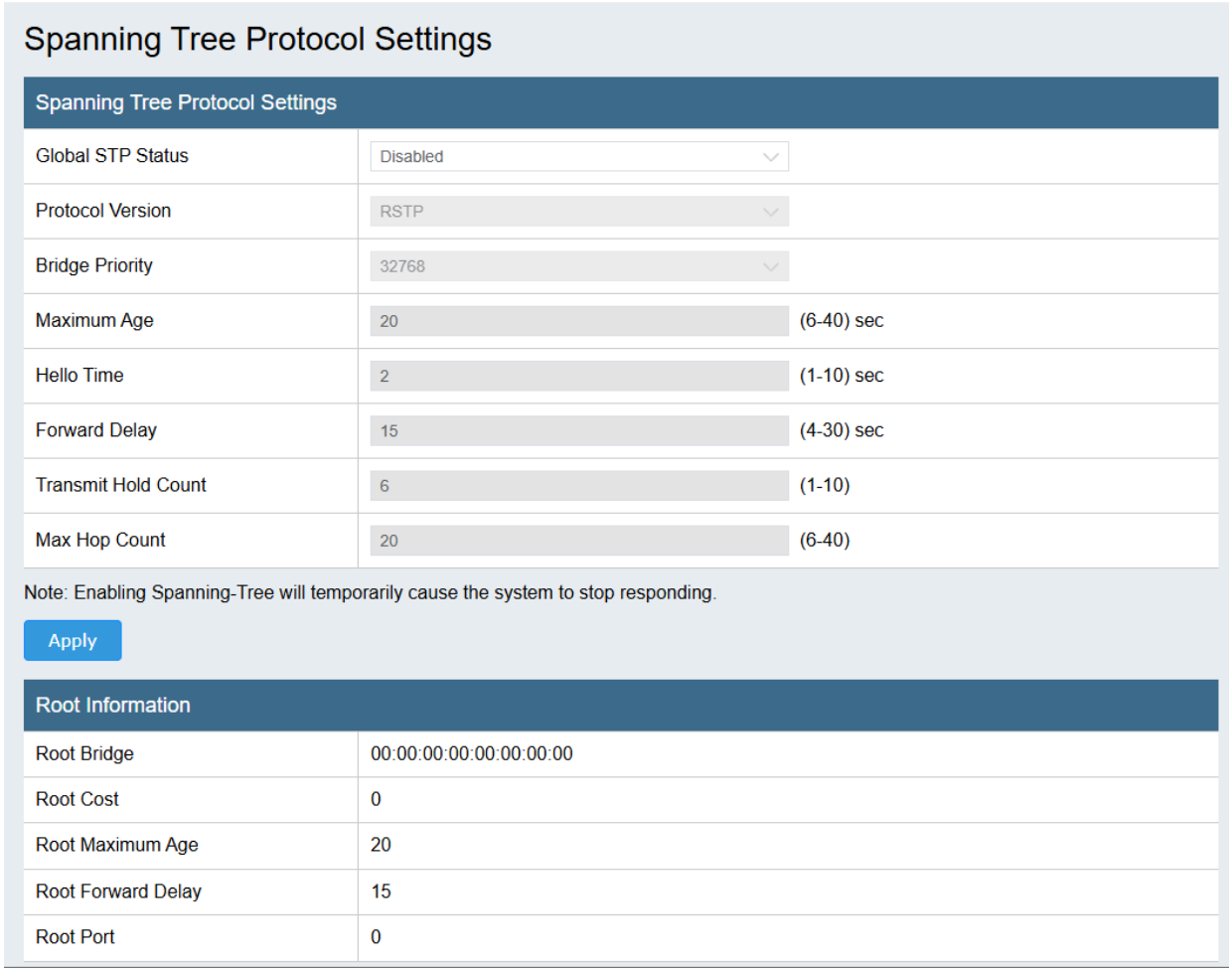
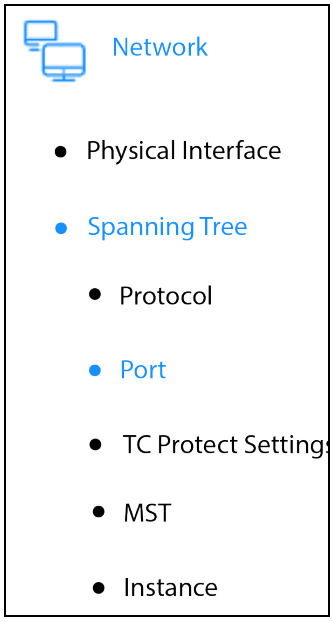


Figure 74. Spanning Tree Protocol Settings Window

Configuring STP and RSTP Port Settings



The instructions in this section configure STP and RSTP port settings. You have to perform the following two functions before configuring STP and RSTP port settings:

- ❒ Enable spanning tree on the switch. Refer to “Configuring STP and RSTP Global Settings” on page 206.
- ❒ Disable BPDU Pass Through on all ports. Refer to Chapter 19, “Basic Port Settings” on page 191.

To configure the port parameters for STP or RSTP:

1. Select **Network** > **Spanning Tree** > **Port** from the menu. The switch displays the Port Settings window. Refer to Figure 75 on page 213.
2. Configure the settings in Table 55.

Table 55. STP and RSTP Port Settings Window

Field	Definition
Port	Displays the port numbers on the switch. You can use the All row at the top of the table as a shortcut to applying the same parameter settings to all ports. The default Ignore parameter setting means to ignore the All row for that parameter.
STP Status	Enable or disable the spanning tree protocol on the port by selecting one of the following from the menu: - **Enabled**: Activates the protocol on the port. This is the default setting. - **Disabled**: Deactivates the protocol.
Priority	Select the port priority from the menu. This parameter is used as a tie breaker when two or more ports have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 128.

Table 55. STP and RSTP Port Settings Window (Continued)

Field	Definition
Admin Cost	Enter the port cost. The spanning tree algorithm uses the cost to select the port that provides the lowest cost path to the root bridge when there are multiple physical paths. The range is 0 to 65,535. The default setting is 0 (Auto-detect), which sets port cost depending on port speed. Auto-Detect assigns a value of 100 to a port operating at 10M, 10 for 100M, and 4 for 1000M.
External Cost	Reserved for MSTP. Refer to “Configuring MSTP Port Settings” on page 238.
Status	Displays the current port state. STP and RSTP have different port states. The STP states are listed here: - Blocking - The port is blocking all traffic, except for BPDUs, because the protocol detected a network loop. The path is blocked because its cost to the root bridge is higher than another path. - Listening - The port is in the convergence state, prior to transitioning to the forwarding or blocking state. - Learning - The port is in the convergence state, learning source addresses from ingress frames, prior to transitioning to the forwarding or blocking state. - Forwarding - The port is forwarding network traffic. This indicates normal operation. STP continues monitoring the port for BPDUs that indicate whether the port should return to the blocking state to prevent a loop. - Disabled - The port does not have a link to a network device or the spanning tree protocol is disabled on the port.

Table 55. STP and RSTP Port Settings Window (Continued)

Field	Definition
Status (continued)	The possible RSTP states are listed here: - Discarding - The port is discarding all traffic, except for BPDUs, because a loop is detected. The path is blocked because its cost to the root bridge is higher than another path. - Forwarding - The port is forwarding network traffic. This indicates normal operation. RSTP continues to monitor the port for BPDUs that indicate whether the port should return to the blocking state to prevent a loop.
Edge	Select a setting for the edge port parameter. Edge ports are connected to edge devices, such as computers or printers. Applies to RSTP only. Here are the settings: - **Auto**: The switch automatically determines whether the port is an edge port. This is the default setting. The port is automatically designated an edge port and placed in the forwarding state if it does not receive any BPDUs for three seconds: - **ForceTrue**: Designates the port as an edge port. The port will always be in a forwarding state. - **ForceFalse**: Designates the port as not an edge port.
P2P	Select a setting for the point-to-point port parameter. The settings are listed here: - **Auto**: The switch automatically determines whether the port is a point-to-point port. This is the default setting. - **ForceTrue**: Designates the port as a point-to-point port. - **ForceFalse**: Designates the port as not a point-to-point port.

Table 55. STP and RSTP Port Settings Window (Continued)

Field	Definition
Restricted Role	Reserved for MSTP. Refer to “Configuring MSTP Port Settings” on page 238.
Restricted TCN	Reserved for MSTP. Refer to “Configuring MSTP Port Settings” on page 238.
Migrate	Click the button to reset the port so that it resumes sending RSTP BPDUs. An RSTP port that receives STP BPDUs changes to the STP mode and transmits STP BPDUs. You can use this button to return the port to the RSTP mode so that it transmits RSTP BPDUs again.

Figure 75. Port Settings Window

Configuring Topology Change Protection

Network

- Physical Interface
- Spanning Tree
  - Protocol
  - Port
  - TC Protect Setting
  - MST
  - Instance

The instructions in this section explain how to set the topology change (TC) protection feature on the switch. This feature is designed to protect the switch from being flooded with topology change notifications from other switches. Switches automatically transmit topology change notifications whenever they detect a change to the topology of the devices connected to their ports. Too many change notifications in a short period of time can negatively impact switch and network performance. This feature allows you to set thresholds on the switch for both number of change notifications and time period. Notifications exceeding the defined number within the time threshold are discarded by the switch to prevent notification flooding.

Note
TC protection is supported on RSTP and MSTP. It is not supported on STP.

To configure TC protection parameters:

1. Select **Network** > **Spanning Tree** > **TC Protect Settings** from the menu. The switch displays the Spanning Tree Protocol TC Protect window. Refer to Figure 76 on page 215.
2. Configure the settings in Table 56.

Table 56. Spanning Tree Protool TC Protect Window

Field	Definition
TC Protect Status	Enables and disables the TC protect feature with these options: - **Enabled**: Activates TC protection on the switch. - **Disabled**: Deactivates TC protection on the switch. This is the default setting.
TC Protect Threshold	Specifies the maximum number of TC notifications the switch accepts during a time protection cycle. TC notifications exceeding the threshold within a time cycle are discarded by the switch. The range is 1 to 100 notifications. The default is 20 notifications.

Table 56. Spanning Tree Protool TC Protect Window (Continued)

Field	Definition
TC Protect Cycle	Specifies the time protection cycle. The range is 1 to 10 seconds. The defaut is 5 seconds.

3. Click **Apply**.

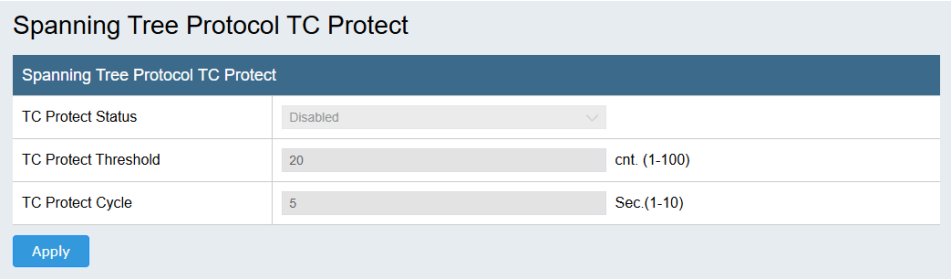


Figure 76. Spanning Tree Protocol TC Protect

Chapter 21

Multiple Spanning Tree Protocol Overview

This chapter provides background information on the Multiple Spanning Tree Protocol (MSTP). The sections are listed here:

- ❒ “Overview” on page 218
- ❒ “Multiple Spanning Tree Instance (MSTI)” on page 219
- ❒ “Multiple Spanning Tree Regions” on page 221
- ❒ “Common and Internal Spanning Tree (CIST)” on page 224
- ❒ “MSTP with STP and RSTP” on page 225
- ❒ “Summary of Guidelines” on page 226
- ❒ “Associating VLANs to MSTIs” on page 228
- ❒ “Connecting VLANs Across Different Regions” on page 230

Overview

MSTP searches for loops in the wiring topology of a network and, where loops exist, blocks bridge ports to prevent broadcast storms. This is the same function as that performed by STP and RSTP, as explained in Chapter 20, “Spanning Tree and Rapid Spanning Tree Protocols” on page 197. It, The main difference between MSTP and the other spanning tree protocols is that it lets you group the bridges of a network into multiple spanning tree domains. This can be useful in networks with large number of bridges because it enables the spanning tree protocol to react to and resolve loops more quickly than if all of the bridges are one domain.

The following sections describe some of the terms and concepts related to MSTP.

Note
Do not activate MSTP on the switch without first familiarizing yourself with the following concepts and guidelines. Unlike STP and RSTP, you cannot activate this spanning tree protocol without configuring the protocol parameters.

Note
The MSTP implementation on the switch complies with the IEEE 802.1s standard and is compatible with other vendors’ compliant 802.1s implementations.

Multiple Spanning Tree Instance (MSTI)

The individual spanning trees domains in MSTP are referred to as Multiple Spanning Tree Instances (MSTIs). An MSTI can span any number of switches.

To create an MSTI, you assign it a number, referred to as the MSTI ID. in the range 1 to 31. (The switch is shipped with a default MSTI with an ID of 0. This default spanning tree instance is discussed later in “Common and Internal Spanning Tree (CIST)” on page 224.)

After selecting an MSTI ID, you need to define the scope of the MSTI by assigning one or more VLANs to it. An instance can contain any number of VLANs, but a VLAN can belong to only one MSTI at a time.

Here are the MSTI guidelines:

- The switch supports up to sixteeen spanning tree instances, including the CIST.
- An MSTI can contain any number of VLANs.
- A VLAN can belong to only one MSTI at a time.
- A switch port can belong to more than one spanning tree instance at a time by being a member of VLANs belonging to different MSTIs. This is possible because a port can be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance. For further information, refer to “Ports in Multiple MSTIs” on page 219.

VLAN and MSTI Associations

Part of the task to configuring MSTP involves assigning VLANs to spanning tree instances. The mappings of VLANs to MSTIs are called associations. A VLAN can belong to only one instance at a time, but an instance can contain any number of VLANs.

Ports in Multiple MSTIs

A port can be a member of more than one MSTI at a time if it is a tagged member of one or more VLANs assigned to different MSTIs. In this circumstance, a port might have to operate in different spanning tree states simultaneously, depending on the requirements of the MSTIs. For example, a port that belongs to two different VLANs in two different MSTIs might operate in the forwarding state in one MSTI and the blocking state in the other.

A port’s MSTI parameter settings are divided into two groups. The first group is referred to as generic parameters. These are set only once on a port and apply to all the MSTIs where the port is a member. One of these parameters is the external path cost, which sets the operating cost of a port connected to a device outside its region. A port, even if it belongs to

multiple MSTIs, can have only one external path cost. Another generic parameter designates a port as an edge port or a point-to-point port.

The second group of port parameters can be set differently for each MSTI where a port is a member. One parameter, the internal path cost, specifies the operating cost of a port when it is connected to a bridge in the same MSTP region. The other parameter in this group sets the port priority, which acts as a tie breaker when two or more ports have equal costs to a regional root bridge.

Multiple Spanning Tree Regions

Another important concept of MSTP is regions. An MSTP region is defined as a group of bridges that share exactly the same MSTI characteristics. The characteristics are listed here:

- Configuration name
- Revision number
- VLANs
- VLAN to MSTI ID associations

A configuration name is a name that identifies a region. You must assign each bridge in a region exactly the same name; even the same upper and lowercase lettering. Identifying the regions in your network is easier if you choose names that are characteristic of the functions of the nodes and bridges of the region. Examples are Sales Region and Engineering Region.

The revision number is an arbitrary number assigned to a region. You might use this number to keep track of the revision level of a region's configuration. For example, you might use this value to maintain the number of times you revise a particular MSTP region. It is not important that you maintain this number, only that all of the bridges in a region have the same number.

The bridges of a particular region must also have the same VLANs. The names of the VLANs and the VIDs must be same on all of the bridges in a region.

Finally, the VLANs in the bridges must be associated to the same MSTIs.

If any of the above information is different on two bridges, MSTP considers the bridges as residing in different regions.

Figure 77 on page 222 illustrates the concept of regions. It shows one MSTP region with two switches. The switches have the same configuration names and revision levels. They also have the same five VLANs and the VLANs are associated with the same MSTIs.

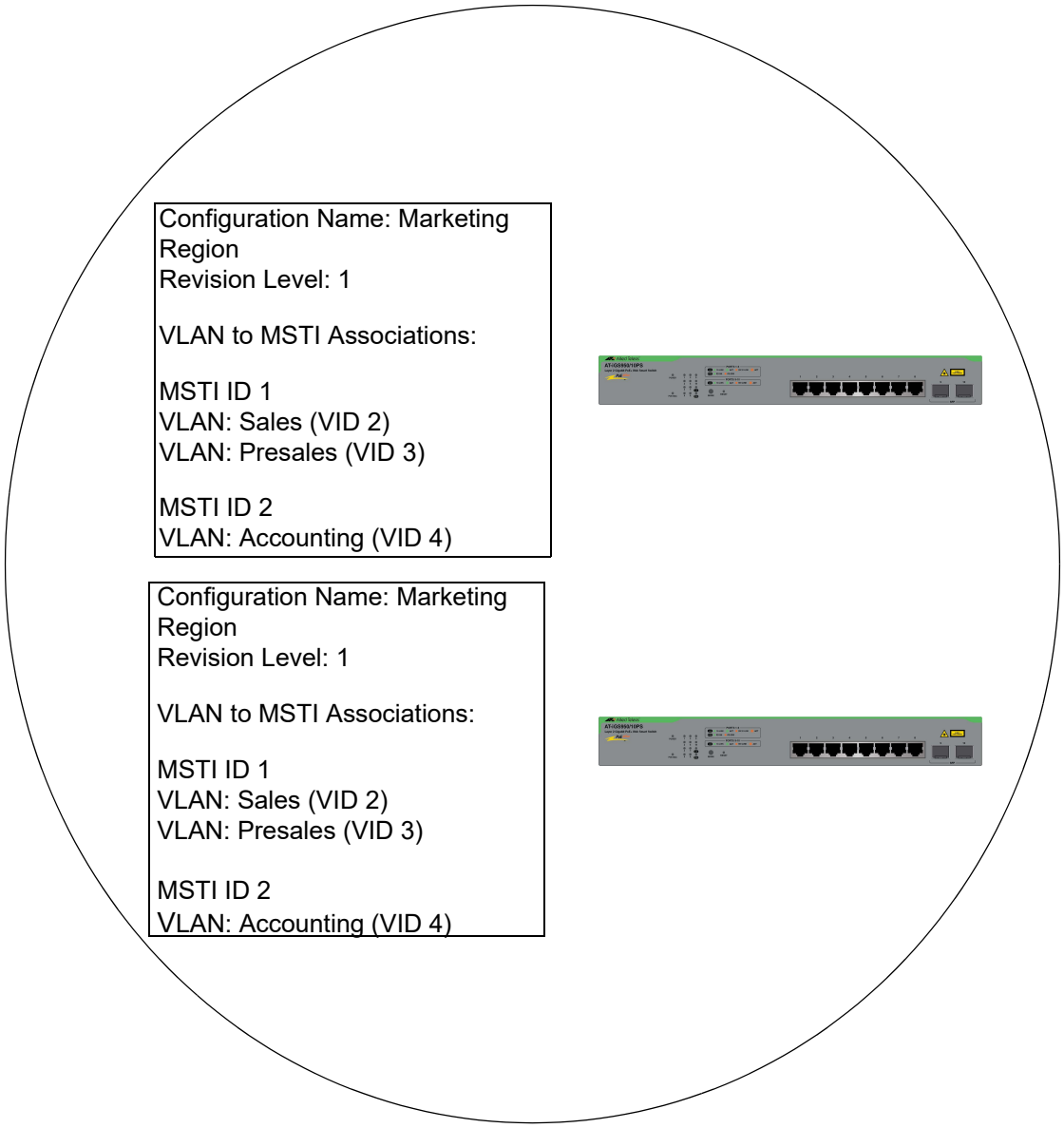


Figure 77. Multiple Spanning Tree Region

The switch determines regional boundaries by examining the MSTP BPDUs it receives on the ports. A port that receives an MSTP BPDU from another bridge with regional information different from its own is considered to be a boundary port and the bridge connected to the port as belonging to another region.

The same is true for ports connected to bridges running STP or RSTP. Those ports are also considered as part of another region.

Each MSTI functions as an independent spanning tree within a region. Consequently, each MSTI must have a root bridge to locate physical loops within the spanning tree instance. An MSTI's root bridge is called a regional root. The MSTIs within a region may share the same regional root or they can have different regional roots.

A regional root of an MSTI must be within the region where the MSTI is located. An MSTI cannot have a regional root that is outside its region.

A regional root is selected by a combination of the MSTI priority value and the bridge's MAC address. The MSTI priority is analogous to the RSTP bridge priority value. Where they differ is that while the RSTP bridge priority is used to determine the root bridge for an entire bridged network, MSTI priority is used to determine the regional root of a particular MSTI.

The range for this parameter is the same as the RSTP bridge priority; from 0 to 61,440 in sixteen increments of 4,096.

Region Guidelines

Here are the guidelines for regions.

- A network can contain any number of regions and a region can contain any number of switches.
- A switch can belong to only one region at a time.
- A region can contain any number of VLANs.
- All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.
- An MSTI cannot span multiple regions.
- Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots.
- A regional root is determined by the MSTI priority value and a bridge's MAC address.
- The regional root of an MSTI must be in the same region as the MSTI.

Common and Internal Spanning Tree (CIST)

MSTP has a default spanning tree instance called the Common and Internal Spanning Tree (CIST). This instance has an MSTI ID of 0.

This instance has unique features and functions that make it different from the MSTIs you create yourself. First, you cannot delete this instance or change its MSTI ID. Second, when you create a new VLAN, it is by default associated with the CIST and is automatically given an MSTI ID of 0. The default VLAN is also associated by default with CIST.

Another important difference is that when you assign a VLAN to another MSTI, it still partially remains a member of CIST. This is because CIST is used by MSTP to communicate with other MSTP regions and with any RSTP and STP bridges in a network. MSTP uses CIST to participate in the creation of a spanning tree between different regions and between regions and STP and RSTP bridges, to form one spanning tree for the entire bridged network.

MSTP uses CIST to form the spanning tree of an entire bridged network because CIST can cross regional boundaries, while an MSTI cannot. If a port is a boundary port, that is, if it is connected to another region, that port automatically belongs solely to CIST, even if it was assigned to an MSTI, because only CIST is active outside of a region.

As mentioned earlier, every MSTI must have a root bridge, referred to as a regional root, in order to locate loops that might exist within the instance. CIST must also have a regional root. However, the CIST regional root communicates with the other MSTP regions and STP and RSTP bridges in the bridged network.

The CIST regional root is set with the CIST Priority parameter. This parameter, which functions similar to the RSTP bridge priority value, selects the root bridge for the entire bridged network. If the switch has the lowest CIST Priority value among all the spanning tree bridges, it functions as the root bridge for all the MSTP regions and STP and RSTP bridges in the network.

MSTP with STP and RSTP

MSTP is fully compatible with STP and RSTP. If a port on the switch running MSTP receives STP BPDUs, the port sends only STP BPDU packets. If a port receives RSTP BPDUs, the port sends MSTP BPDUs because RSTP can process MSTP BPDUs.

A port connected to a bridge running STP or RSTP is considered to be a boundary port of the MSTP region and the bridge as belonging to a different region.

An MSTP region can be considered as a virtual bridge. The implication is that other MSTP regions and STP and RSTP single-instance spanning trees cannot discern the topology or constitution of an MSTP region. The only bridge they are aware of is the regional root of the CIST instance.

Summary of Guidelines

Careful planning is essential for the successful implementation of MSTP. This section reviews all of the rules and guidelines mentioned in earlier sections, and provides a few new ones:

- The switch can support up to sixteen spanning tree instances, including the CIST.
- An MSTI can contain any number of VLANs.
- A VLAN can belong to only one MSTI at a time.
- An MSTI ID can be from 1 to 31.
- The CIST ID is 0. You cannot change this value.
- A switch port can belong to more than one spanning tree instance at a time. This allows you to assign ports as members of VLANs that belong to different MSTIs. What makes this possible is a port's ability to be in different MSTP states for different MSTIs simultaneously. For example, a port can be in the MSTP blocking state for one MSTI and the forwarding state for another spanning tree instance.
- A router or Layer 3 network device is required to forward traffic between VLANs.
- A network can contain any number of regions and a region can contain any number of switches.
- The switch can belong to only one region at a time.
- A region can contain any number of VLANs.
- All of the bridges in a region must have the same configuration name, revision level, VLANs, and VLAN to MSTI associations.
- An MSTI cannot span multiple regions.
- Each MSTI must have a regional root for locating loops in the instance. MSTIs can share the same regional root or have different roots. A regional root is determined by the MSTI priority value and a bridge's MAC address.
- The regional root of an MSTI must be in the same region as the MSTI.
- The CIST must have a regional root for communicating with other regions and single-instance spanning trees.
- MSTP is compatible with STP and RSTP.
- A port transmits CIST information even when it is associated with another MSTI ID. However, in determining network loops, MSTI takes precedence over CIST. (This is explained more in "Associating VLANs to MSTIs" on page 228.

Note
The MSTP implementation on the switch complies with the IEEE 802.1s standard and is compatible with similar products from other vendors, provided that their products are also compliant with the standard.

Associating VLANs to MSTIs

Allied Telesis recommends that you assign all VLANs on the switch, including the default VLAN, to an MSTI. You should not leave VLANs assigned only to CIST. This is to prevent the switch from blocking ports that should be in the forwarding state. The reason for this guideline is explained here.

An MSTP BPDU contains the instance to which the port transmitting the packet belongs. By default, all of the ports belong to the CIST instance. So CIST is included in the BPDU. If a port is a member of a VLAN that has been assigned to another MSTI, that information is also included in the BPDU.

This is illustrated in Figure 78. Port 4 in switch A is a member of a VLAN assigned to MSTI ID 7 while port 1 is a member of a VLAN assigned to MSTI ID 10. The BPDUs transmitted by port 4 to switch B indicate that the port is a member of both CIST and MSTI 7, while the BPDUs from port 1 indicate the port is a member of the CIST and MSTI 10.

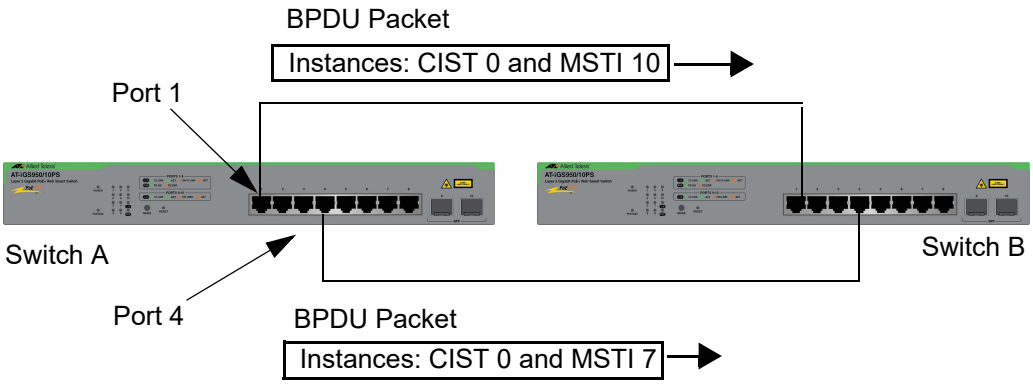


Figure 78. CIST and VLAN Guideline - Example 1

At first glance, it might appear that because both ports belong to CIST, a loop would exist between the switches and that MSTP would block a port to stop the loop. However, within a region, MSTI takes precedence over CIST. When switch B receives a packet from switch A, it uses MSTI, not CIST, to determine whether a loop exists. And because both ports on switch A belong to different MSTIs, switch B determines that no loop exists.

A problem can arise if you assign some VLANs to MSTIs while leaving others only in CIST. The problem is illustrated in Figure 79 on page 229. The network is the same as the previous example. The difference is that the VLAN containing port 4 on Switch A has not been assigned to an MSTI, and belongs only to CIST with its MSTI ID 0.

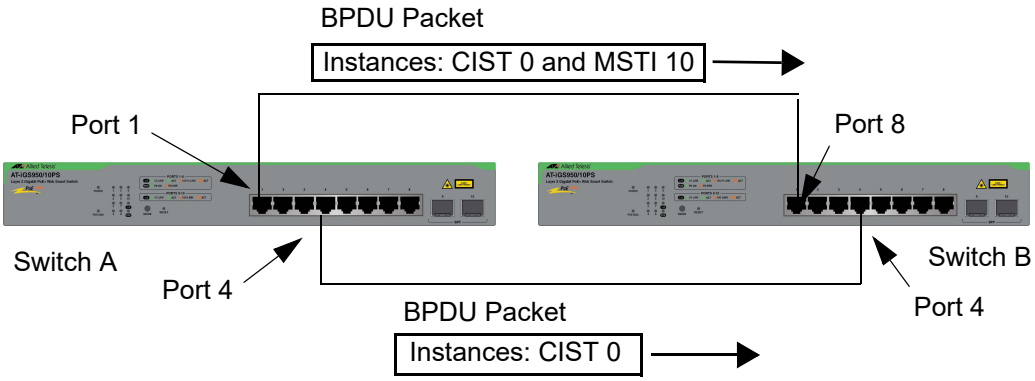


Figure 79. CIST and VLAN Guideline - Example 2

When port 4 on switch B receives a BPDU, the switch notes the port sending the packet belongs only to CIST. Therefore, switch B uses CIST to determine whether a loop exists. The result would be that the switch detects a loop because the other port is also receiving BPDU packets from CIST 0. Switch B would block a port to block the loop.

To avoid this issue, always assign all VLANs on the switch, including the Default VLAN, to MSTIs. This guarantees that all ports on the switch have an MSTI ID and ensures that loop detection is based on the MSTIs and not CIST.

Connecting VLANs Across Different Regions

Special consideration needs to be taken into account when connecting different MSTP regions or an MSTP region and an STP or RSTP region. Unless planned properly, VLAN fragmentation can occur between the VLANS of the network.

As mentioned previously, only the CIST can span regions. Consequently, you may run into problems if you use more than one physical data link to connect together various parts of VLANs that reside in bridges in different regions. The result can be a physical loop, which spanning tree disables by blocking ports.

This is illustrated in Figure 80. The example shows two switches that reside in different regions. Port 1 in switch A is a boundary port. It is a member of the Accounting VLAN, which has been associated with MSTI 4. Port 8 is a member of three different VLANs, all associated with MSTI 12.

If both switches were a part of the same region, there would be no problem because the ports reside in different spanning tree instances. However, the switches are part of different regions and MSTIs do not cross regions. Consequently, the result is that spanning tree would determine that a loop exists between the regions, and Switch B would block a port.

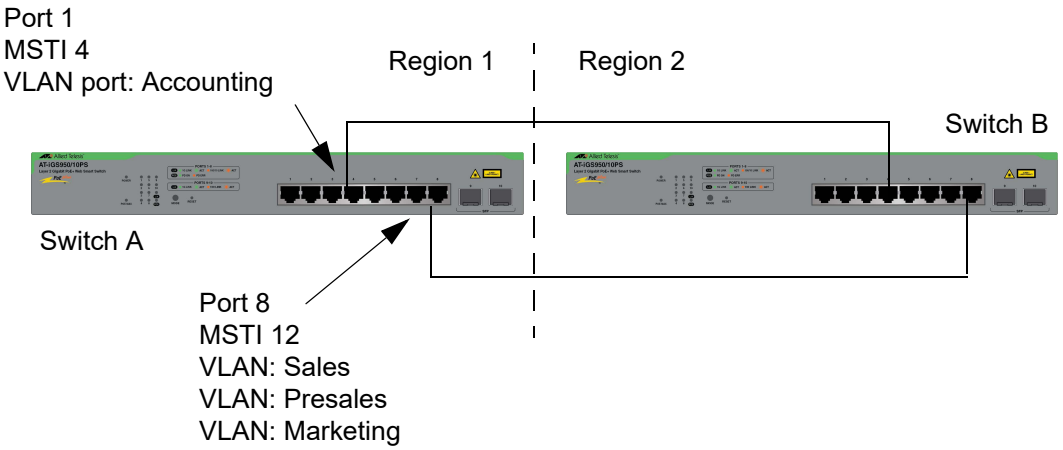


Figure 80. Spanning Regions

There are several ways to address this issue. One way is to have only one MSTP region for each subnet in your network.

Another approach is to group those VLANs that need to span regions into the same MSTI. Those VLANs that do not span regions can be assigned to other MSTIs.

Here is an example. Assume that you have two regions that contain the following VLANS:

Region 1 VLANs
Sales
Presales
Marketing
Advertising
Technical Support
Product Management
Project Management
Accounting

Region 2 VLANs
Hardware Engineering
Software Engineering
Technical Support
Product Management
CAD Development
Accounting

The two regions share three VLANs: Technical Support, Product Management, and Accounting. You could group those VLANs into the same MSTI in each region. For instance, for Region 1 you might group the three VLANs in MSTI 11 and in Region 2 you could group them into MSTI 6. After they are grouped, you can connect the VLANs across the regions using a link of tagged ports.

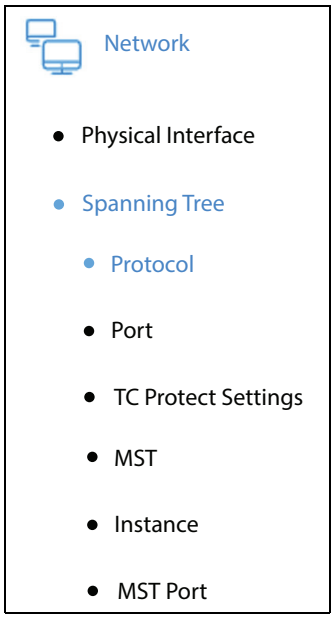
Chapter 22

Multiple Spanning Tree Protocol

This chapter contains the configuration procedures for the Multiple Spanning Tree Protocol (MSTP) in the following sections:

- ❒ “Configuring MSTP Global Settings” on page 234
- ❒ “Configuring MSTP Port Settings” on page 238
- ❒ “Configuring MST and MSTI Settings” on page 242
- ❒ “Configuring MST Port Settings” on page 244
- ❒ “Displaying MST Instance Information” on page 247

Configuring MSTP Global Settings



This section explains how to configure the following MSTP parameters:

- ❒ Enable or disable spanning tree protocol
- ❒ Choose MSTP as the active protocol
- ❒ Configure global (non port-specific) settings

Note
You have to disable BPDU pass-through on all ports before enabing the spanning tree protocol. Refer to Chapter 19, “Basic Port Settings” on page 191.

Note
The switch briefly stops forwarding Ethernet traffic when you enable or disable a spanning tree protocol.

To configure global MSTP parameters:

1. Select **Network** > **Spanning Tree** > **Protocol** from the menu. The Spanning Tree Protocol Settings window is shown in Figure 74 on page 209.
2. Configure the parameters for MSTP be referring to Table 57.
3. Click **Apply** in the Action column to activate your changes.

Note
Click **Save** in the menu to save your changes.

Table 57. Spanning Tree Protocol Settings Window for MSTP

Field	Definition
Spanning Tree Protocol Settings	
Global STP Status	Select one of the following from the menu: - **Enabled**: Activates the spanning tree protocol. You must enable the protocol to configure the settings. - **Disabled**: Deactivates the spanning tree protocol. This is the default setting.
Protocol Version	Select **MSTP** from the menu.

Table 57. Spanning Tree Protocol Settings Window for MSTP

Field	Definition
Bridge Priority	Select the priority number for the bridge. This number is used to determine the root bridge the regional root for a particular MSTI. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. If a root bridge goes off-line, the bridge with the next lowest priority number automatically takes over as the root bridge. The range is 0 (zero) to 61,440 in increments of 4096, with 0 as the highest priority.
Maximum Age	Enter the maximum length of time the bridge stores bridge protocol data units (BPDUs). Bridges in a bridged LAN use the aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs) and to delete expired data units. For example, when set to the default value 20 seconds, bridges delete configuration messages after 20 seconds. The range is 6 to 40 seconds. Observe the following rules when setting the maximum age: - Maximum Age must be greater than (2 x (Hello Time + 1)) - Maximum Age must be less than (2 x (Forward Delay - 1)) - The aging time for BPDUs is different from the aging time for the MAC address table. MSTP uses this parameter when interacting with STP/RSTP domains on boundary ports.

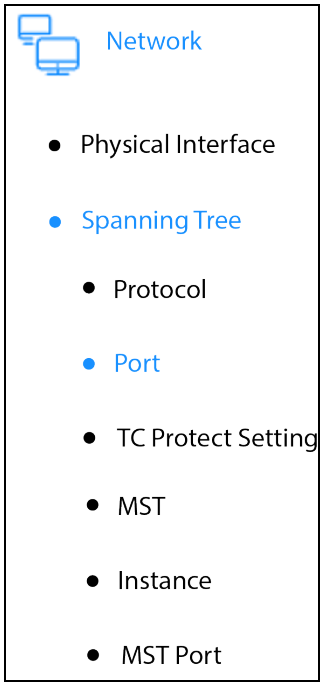
Table 57. Spanning Tree Protocol Settings Window for MSTP

Field	Definition
Hello Time	Enter the time interval at which the root bridge transmits BPDUs to determine whether there have been any changes to the network topology and to inform other bridges of topology changes. This parameter is active only on the root bridge. The range is 1 to 10 seconds. The default is 2 seconds.
Forward Delay	Enter the waiting period in seconds before a bridge changes to a new state, for example, becomes the new root bridge after a topology change. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.
Transmit Hold Count	Enter the maximum number of BPDUs the bridge can send per second. The range is 1 to 10 BPDUs. The default is 6 BPDUs.
Max Hop Count	Enter the maximum number of hops before BPDUs are deleted. The Max Hop counter in a BPDU is decremented every time a BPDU crosses an MSTP region boundary. BPDUs are deleted after the counter reaches zero.
Root Information	
Root Bridge	Displays the MAC address of the root bridge of the spanning tree domain. This value is zero when MSTP is disabled on the switch.
Root Cost	Displays the sum of the root port costs of the bridges between the switch's root port and the root bridge.
Root Maximum Age	Displays the maximum age setting on the root bridge.
Root Forward Delay	Displays the forward delay setting on the root bridge.

Table 57. Spanning Tree Protocol Settings Window for MSTP

Field	Definition
Root Port	Displays the port on the switch that leads to the root bridge. This value will be zero if the switch is the root bridge or spanning tree is disabled.

Configuring MSTP Port Settings



To configure MSTP port settings:

1. Select **Network** > **Spanning Tree** > **Port** from the menu. The Port Settings window is shown in Figure 75 on page 213.
2. Configure the MSTP parameters in Table 58.
3. Click **Apply** in the Action column to activate your changes.

Note
Click **Save** in the menu to save your changes.

Table 58. MSTP Port Settings

Field	Definition
Port	Displays the port numbers on the switch. You can use the All row at the top of the table as a shortcut to applying the same parameter settings to all the ports. The default Ignore parameter setting means to ignore the All row for that parameter.
STP Status	Enable or disable the spanning tree protocol on the port by selecting one of the following from the menu: - **Enabled**: Activates the protocol on the port. This is the default setting. - **Disabled**: Deactivates the protocol.
Priority	Select the port priority from the menu. This parameter is used as a tie breaker when two or more ports have equal costs to the root bridge. The range is 0 to 240 in increments of 16. The default value is 128.

Table 58. MSTP Port Settings (Continued)

Field	Definition
Admin Cost	Enter the port cost. The spanning tree algorithm uses the cost to select the port that provides the lowest cost path to the root bridge when there are multiple physical paths. The range is 0 to 65,535. The default setting is 0 (Auto-detect), which sets port cost depending on port speed. Auto-Detect assigns a value of 100 to a port operating at 10M, 10 for 100M, and 4 for 1000M.
External Cost	Displays the operating cost of the port when connected to a device outside its region.
State	Displays the current MSTP port state, listed here: - Blocking - The port is blocking all traffic, except for BPDUs, because the protocol detected a network loop. The path is blocked because its cost to the root bridge is higher than another path. - Listening: The port is in the convergence state, prior to transitioning to the forwarding or blocking state. - Learning - The port is in the convergence state, learning source addresses from ingress frames, prior to transitioning to the forwarding or blocking state. - Forwarding - The port is forwarding network traffic. This indicates normal operation. STP continues monitoring the port for BPDUs that indicate whether the port should return to the blocking state to prevent a loop. - Disabled - The port does not have a link to a network device or the spanning tree protocol is disabled on the port.

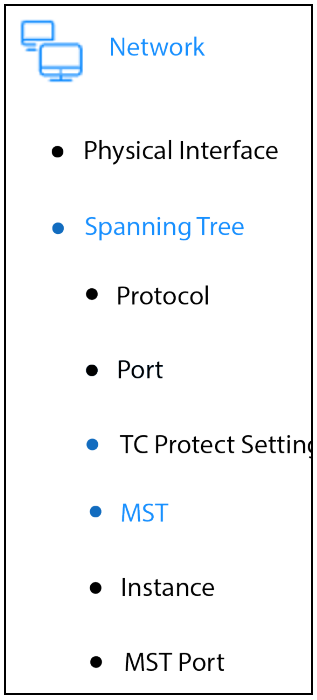
Table 58. MSTP Port Settings (Continued)

Field	Definition
Edge	Select a setting for the edge port parameter. Edge ports are connected to edge devices, such as computers or printers. Applies to RSTP only. Here are the settings: - **Auto**: The switch automatically determines whether the port is an edge port. This is the default setting. The port is automatically designated an edge port and placed in the forwarding state if it does not receive any BPDUs for three seconds: - **ForceTrue**: Designates the port as an edge port. The port will always be in a forwarding state. - **ForceFalse**: Designates the port as not an edge port.
P2P	Select a setting for the point-to-point port parameter from the menu: - **Auto**: The switch automatically determines whether the port is a point-to-point port. This is the default setting. - **ForceTrue**: Designates the port as a point-to-point port. - **ForceFalse**: Designates the port as not a point-to-point port.
Restricted Role	Select the restricted role of the port from the menu: - **True**: Blocks the port from being a root port or from communicating with the root bridge. - **False:** Permits the port to become a root port. This is the default setting The net effect of setting all ports on the switch to True is that it forces the switch into the role of the root bridge regardless of other path costs in the network.

Table 58. MSTP Port Settings (Continued)

Field	Definition
Restricted TCN	Select the Restricted TCN setting from the menu: - **True**: Blocks the port from transmitting Topology Change Notification (TCN) BPDUs when there is a topology change. - **False:** Allows the port to transmit TCN BPDUs when there is a topology change. This is the default setting.
Migrate	Click the button to reset the port so that it resumes sending MSTP BPDUs. MSTP ports that receive STP BPDUs change to the STP mode and transmit STP BPDUs. You can use this button to return ports to the MSTP mode so that they transmit MSTP BPDUs again.

Configuring MST and MSTI Settings



To configure MST settings and manage MST instances:

1. Select **Network** > **Spanning Tree** > **MST** from the menu. The MST Settings window is shown in Figure 81 on page 243.
2. To configure the settings in the MST Settings section of the window, refer to Table 59.
3. Click **Apply** in the Action column to activate your changes.

Note
Select **Save** in the menu to save your changes.

Table 59. MST Settings Window - MST Configuration Identification Settings

Field	Description
Configuration Name	Enter the name of the region where the bridge is a member. All the switches in an MSTP region must have the same name.
Revision Level	Enter the region's revision level. All the switches in an MSTP region must have the same revision level. The range is 0, the default, to 65535.

4. To map VLANs to MST instances (MSTI), configure the settings in the MST Instance Settings section of the window by referring to Table 60, and click **Add**. New MST instances are added to the MST Table section in the window.

Table 60. MST Settings Window - MST Instance Settings

Field	Description
MSTI ID	Enter a unique ID for the new MST instance. The range is 1 to 31.
VID List	Enter VIDs of the VLANs to be associated with the MST instance.

Table 60. MST Settings Window - MST Instance Settings (Continued)

Field	Description
Priority	Choose a priority value from the menu. The switch uses the priority to select the MSTI regional root. The range is 0 (zero) to 61,440 in increments of 4,096. The highest priority is 0. The default is 32768.

- To modify an MSTI, adjust the corresponding MSTI ID in the MST Table and click **Apply**. Refer to Table 60.
- To delete an MSTI, click **Delete** in the **Action** column in the MST Table. The instance and its mapped VLAN associations are deleted.

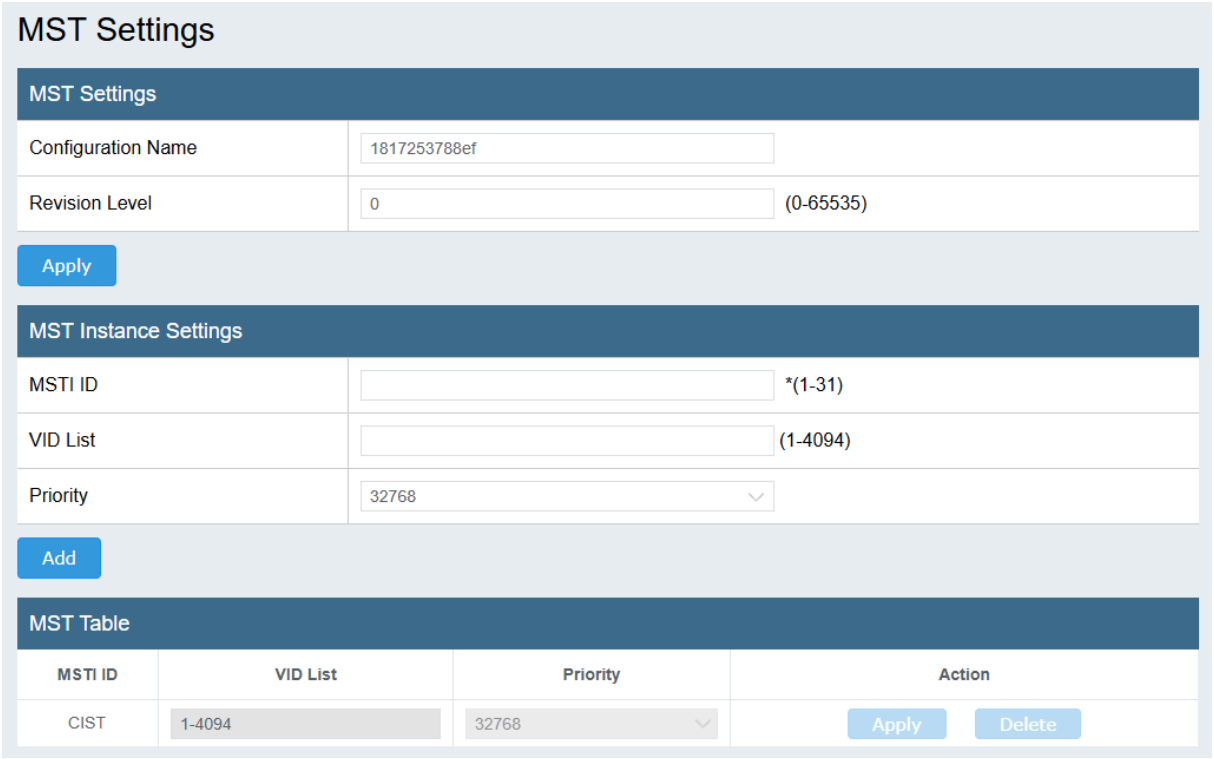
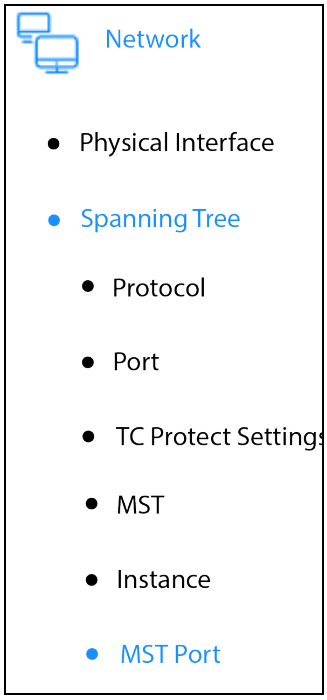


Figure 81. MST Settings Window

Configuring MST Port Settings



To configure MST port settings:

1. Select **Network** > **Spanning Tree** > **MST Port** from the menu to display the MST Port Info window in Figure 82 on page 246.
2. Configure the window parameters by referring to Table 61.

Note
Select **Save** in the menu to save your changes.

Table 61. MST Port Settings Window

Field	Description
Select MST Port	Select a switch port to view or configure from the pull-down list. You can configure only one port at a time.
MSTI ID	Displays the MSTP Instance of the port.
Designated Bridge	Displays the MAC address of the bridge that provides the least-cost path to the root bridge from a network segment.
Internal Path Cost	Displays the operating cost of the port when it is connected to a bridge in the same MSTP region.
Admin Path Cost	Enter the cost of a port to the root. The range is 0 to 200,000,000. The 0 value, the default setting, activates the Auto setting, which sets the value according to port speed. Here are the MSTP port costs with the Auto setting when a port is not a member of a trunk. - 10M - 2,000,000 - 100M - 200,000 - 1000M - 20,000 Here are the MSTP port costs with the Auto setting when a port is a member of a trunk. - 10M - 20,000 - 100M - 20,000 - 1000M - 2,000

Table 61. MST Port Settings Window (Continued)

Field	Description
Priority	Select the spanning tree port priority from the menu. The priority is used as a tie breaker when two or more ports have equal costs to the regional root bridge. The range is 0 to 255 in increments of 16. The default value is 128.
Status	Displays the MSTP state of the port. The possible states are listed here: - Disabled: The port has not established a link with a network device, or MSTP is disabled on the port or switch. - Discarding: The port is discarding received packets and is not submitting forwarded packets for transmission. - Learning: The port can receive but not forward packets. - Forwarding: Normal operations.
Role	Displays the MSTP role of the port. The possible roles are listed here: - Disabled: The port has not established a link with a network device, or MSTP is disabled on the port or switch. - Root - The port that is connected to the root switch, directly or through other switches, with the least path cost. - Alternate - The port offers an alternate path in the direction of the root switch. - Backup - The port on a designated switch that provides a backup for the path provided by the designated port. - Designated - The port on the designated switch for a LAN that has the least cost path to the root switch. This port connects the LAN to the root switch. - Master - Similar to the root port. When the port is a boundary port, the MSTI port roles follow the CIST port roles. The MSTI port role is called “master” when the CIST role is “root.”

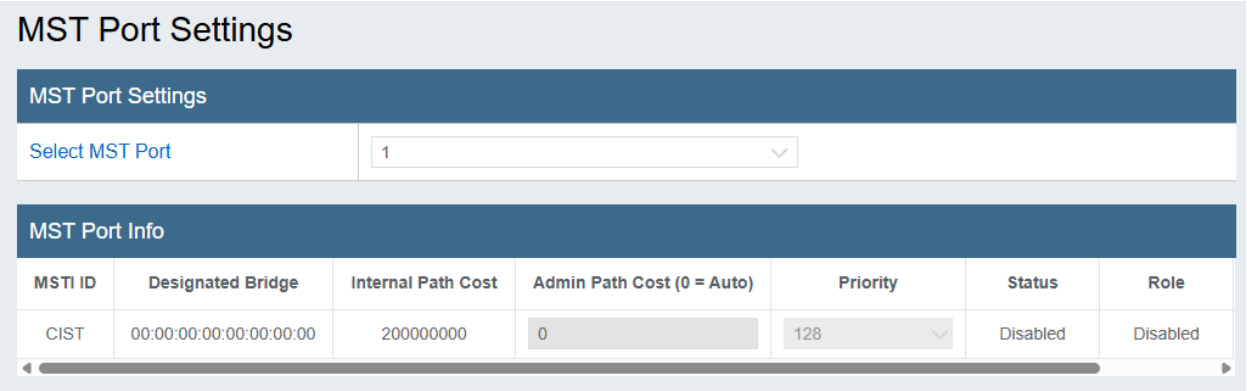
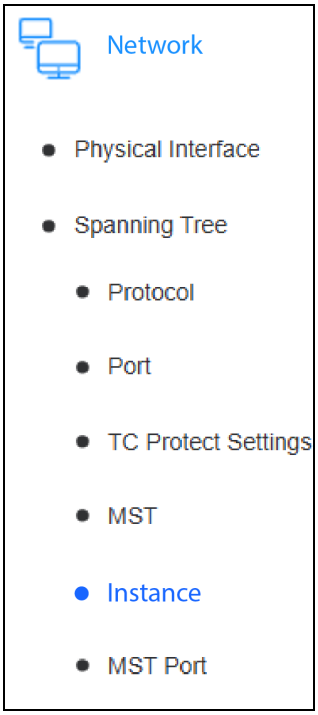


Figure 82. MST Port Settings Window

Displaying MST Instance Information



To display MST instance information on the switch, select **Network** > **Spanning Tree** > **Instance** from the menu. The Instance Information window is shown in Figure 83. The columns are described in Table 62.

Table 62. Instance Information Window

Column	Description
MSTI ID	Displays the MSTP Instance.
Internal Root Cost	Displays the internal cost of the port leading to the root bridge in the MSTP region.
Root Port	Displays the port leading to the root bridge in the MSTP region.
Regional Root Bridge	Displays the MAC address of the root bridge of the MST instance.
Designated Bridge	Displays the MAC address of the bridge providing the least-cost path to the root bridge.
Instance Priority	Displays the priority value of the port leading to the root bridge.

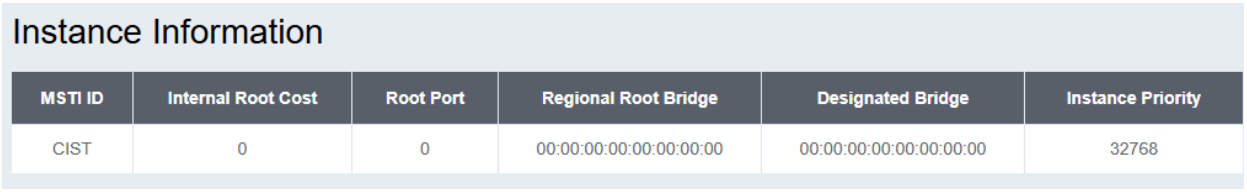


Figure 83. Instance Information Window

Chapter 23

Static Port Trunks

This chapter describes static port trunks in the following sections:

- “Static Port Trunk Overview” on page 250
- “Adding Static Port Trunks” on page 252
- “Modifying Static Port Trunks” on page 254
- “Deleting Static Port Trunks” on page 256

Static Port Trunk Overview

Static port trunks are an economical way to increase the bandwidth between the Ethernet switch and another networking device, such as a network server, router, workstation, or another Ethernet switch. They consist of two or more ports that function as a single virtual link between the switch and another device. Port trunks improve performance by distributing network traffic across multiple ports between the devices and enhance reliability by reducing the reliance on a single physical link. They are commonly used in situations where the bandwidth of a single physical link between devices is not sufficient to efficiently handle the traffic load.

The example in Figure 84 illustrates a port trunk of three links between two iGS950/10PS Switches.

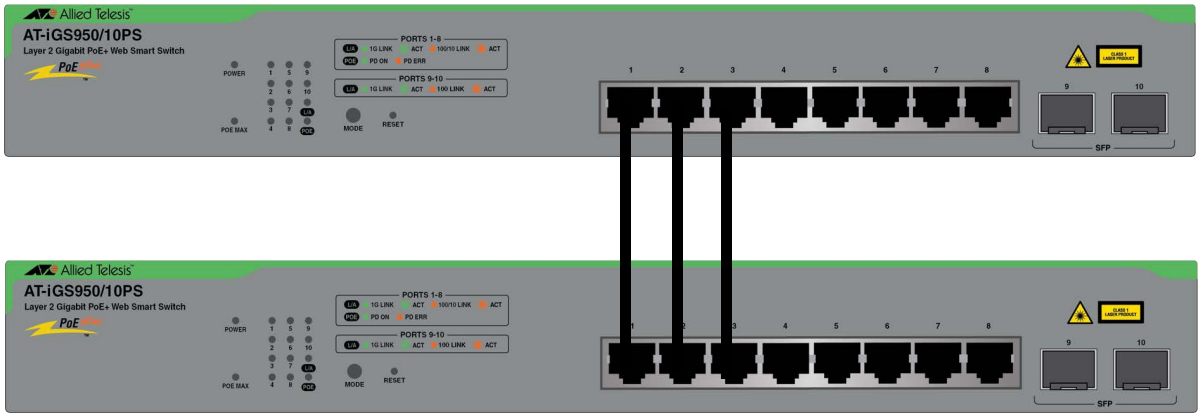


Figure 84. Static Port Trunk Example

Network equipment vendors tend to employ different techniques to implement static port trunks. Consequently, a static port trunk on one device may not be compatible with the same feature on a device from a different manufacturer. For this reason, static port trunks are typically employed only between devices from the same manufacturer.

Also, note that a static port trunk does not provide for redundancy or link backup. If a port in a static trunk loses its link, the trunk's total bandwidth is reduced. Although the traffic carried by the lost link is shifted to one of the remaining ports in the trunk, the bandwidth remains reduced until the lost link is re-established or you add another port to the trunk.

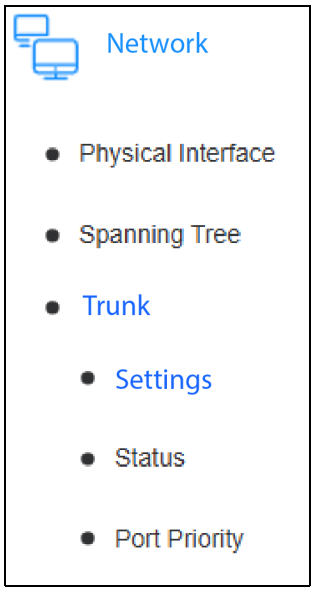
Guidelines

Here are the guidelines to static port trunks:

- Allied Telesis recommends employing static port trunks between the same Allied Telesis networking devices to ensure compatibility.
- The AT-iGS950/10PS Switch supports up to four LACP or static port trunks.

- All other AT-iGS950 Switches support up to eight LACP or static port trunks.
- A port can belong to only one static trunk at a time.
- The ports of a static trunk must be of the same medium type. They can be all copper ports or fiber optic ports, but not both.
- Trunk ports can be consecutive (for example, ports 2 through 4) or nonconsecutive (for example, ports 3, 5, and 7).
- The port settings have to be the same for all trunk ports. This includes speed, duplex mode, flow control, back pressure settings, and VLAN membership.
- A change to the speed, duplex mode, flow control, or back pressure of a port in a trunk is automatically implemented by the switch on all the other trunk ports.
- The switch selects a port in the trunk to handle broadcast packets and packets of unknown destination. The switch makes this choice based on a hash algorithm, depending on the source and destination MAC addresses.

Adding Static Port Trunks



This procedure explains how to add static port trunks.

Caution
Do not connect the cables of a port trunk until after you have configured the ports on both switches. Connecting the cables prior to configuring the ports can form loops in your network topology, which can result in broadcast storms that can reduce network performance.

To add static port trunks:

1. Select **Network** > **Trunk** > **Settings** from the menu.

   The Trunking window is shown in Figure 85 on page 253. The switch supports up to eight LACP and static port trunks, Each row represents a separate trunk. The numbers and check boxes represent the switch ports. Ports that have check marks in the check boxes are members of a trunk.

2. Click the check boxes of the ports for the trunk. Here are the guidelines:

   - A check in a box indicates the port is a member of the trunk. No check means the port is not a member.
   - The AT-iGS950/10PS Switch supports up to four LACP or static port trunks.
   - All other AT-iGS950 Switches support up to eight LACP or static port trunks.
   - A port can be a member of only one trunk at a time. To add a port that is already a member of a trunk to another trunk, you first have to remove it from its current trunk.

3. Set the trunk mode status with the pull-down menu in the right column of the corresponding Trunk ID row. The choices are listed here:

   - **Manual** - Activates the static port trunk.
   - **Disable** - Disables the static port trunk. The ports function as regular networking ports. This is the default setting.

   Note
   The Active and Passive menu settings are for LACP trunks. Refer to Chapter 24, “LACP Trunks” on page 257.

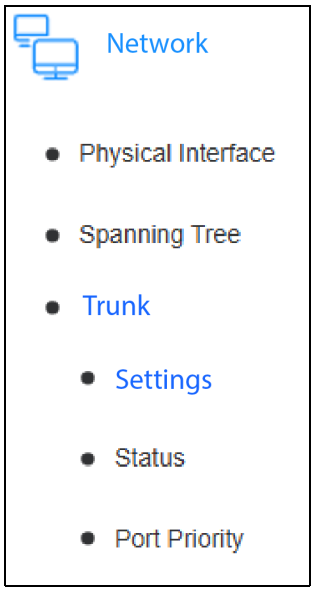
4. Click **Apply**.

> **Note**
> Select **Save** from the menu to save your changes.

5. Configure the port trunk on the other switch.
6. Connect the Ethernet cables to the trunk ports on the two switches.

Figure 85. Trunking Window

Modifying Static Port Trunks



This procedure explains how to enable or disable port trunks, or add or remove ports.

Caution
Before disabling or modifying a port trunk, disconnect all cables from its ports. Leaving the cables connected can create loops in your network topology, which can result in broadcast storms that can reduce network performance.

To add or remove ports from a trunk:

1. Disconnect all Ethernet cables from the ports of the trunk.
2. Select **Network** > **Trunk** -> **Settings** from the menu

   The Trunking window is shown in Figure 85 on page 253. The window lists the eight possible trunks on the switch. The rows of numbers and check boxes represent the switch ports.
3. To add or remove ports, click the check boxes. Here are the guidelines:
   - A check in a box indicates the port is a member of the trunk. No check means the port is not a member.
   - The AT-iGS950/10PS Switch supports up to four LACP or static port trunks.
   - All other AT-iGS950 Switches support up to eight LACP or static port trunks.
   - A port can be a member of only one trunk at a time. To add a port that is already a member of a trunk to another trunk, you first have to remove it from its current trunk.
4. To enable or disable a trunk, change the status with the pull-down menu to the right column of the corresponding Trunk ID row. The choices are listed here:
   - **Manual** - Activates the static port trunk.
   - **Disable** - Disables the static port trunk. The ports function as regular networking ports. This is the default setting.

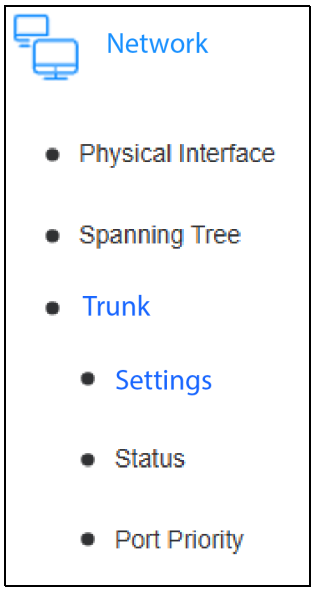
Note
The Active and Passive menu settings are for LACP trunks. Refer to Chapter 24, “LACP Trunks” on page 257.

5. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

6. If necessary, modify the port trunk on the other switch.
7. Connect the Ethernet cables to the trunk ports on the two switches.

Deleting Static Port Trunks



Caution
Before deleting a port trunk, disconnect all cables from its ports. Leaving the cables connected can create loops in your network topology, which can result in broadcast storms that can reduce network performance.

To delete static port trunks:

1. Disconnect all Ethernet cables from the trunk ports.
2. Select **Network** > **Trunk** > **Setting** from the menu. The Trunking window is shown in Figure 85 on page 253.
3. In the appropriate Trunk ID row, remove the ports from the trunk by clicking their check boxes to remove the check marks.
4. Set the status of the trunk to **Disabled** with the menu in the right column.
5. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Chapter 24

LACP Trunks

This chapter describes LACP port trunks in the following sections:

- “LACP Port Trunk Overview” on page 258
- “Displaying LACP Group Status” on page 261
- “Adding LACP Trunks” on page 262
- “Setting LACP Port Priorities” on page 264
- “Modifying LACP Trunks” on page 265
- “Deleting LACP Trunks” on page 267

LACP Port Trunk Overview

LACP (Link Aggregation Control Protocol) port trunks are used to increase the bandwidth between network devices by distributing the traffic load over multiple physical links. They are useful in situations where the bandwidth of a single physical link is not sufficient to efficiently handle the traffic load between network devices.

LACP on the iGS950 Switch is compliant with the IEEE 802.3ad standard. This makes it inter-operable with equipment from other vendors that also comply with the standard, allowing for LACP trunks between iGS950 Switches and network devices from other manufacturers.

To add an LACP trunk to the switch, you designate the ports of the trunk. A trunk can have any number of ports, but only eight ports can be active at any one time in a trunk. The other ports operate in a standby mode. Ports in the standby mode do not pass network traffic, but they do transmit and accept LACP Data Unit (LACPDU) packets, which the switch uses to search for LACP compliant devices. If a link on an active LACP trunk port goes down, the switch automatically activates a standby port so that the maximum possible bandwidth of the trunk is maintained. This adds redundancy and resiliency to the trunk. For example, an LACP trunk of ten ports will have eight active ports and two standby ports. If the link on one of the active ports fails, the switch activates one of the standby ports.

The main component of an LACP trunk is the *aggregator.* It manages a group of ports on the switch. On the iGS950 Switch, the ports assigned to a trunk group are automatically assigned to an aggregator. Only one aggregator can be assigned to each trunk group, which is referred to as an *aggregate trunk*.

Only ports on the switch that are part of an aggregator transmit LACPDU packets. If a port that is part of an aggregator does not receive LACPDU packets from its corresponding port on another device, it assumes that the other port is not part of an LACP trunk and functions as a normal Ethernet port by forwarding network traffic. However, it does continue to send LACPDU packets. If it begins to receive LACPDU packets, it automatically transitions to an active or standby mode as part of an aggregate trunk.

System Priority and ID Numbers

When two network devices form an aggregate trunk, a conflict may occur if they have different LACP implementations. For example, the two devices might not support the same number of active ports in an aggregate trunk or might not agree on which ports are to be active and which are to be in the standby mode.

If a conflict does occur, the two devices need a mechanism for resolving the conflict and deciding whose LACP settings take precedence. This is accomplished with the following values:

- System priority: This value is fixed at 32768 on the iGS950 Switch. It cannot be changed.
- System ID numbers: This is the MAC address of the iGS950 Switch. It cannot be changed.

If the two switches of an LACP trunk have different system priorities, the LACP settings on the switch with the lower value takes precedence. If the two switches have the same system priorities, as will be the case with LACP trunks between iGS950 Switches, they compare system IDs. System IDs for iGS950 Switches, are their MAC addresses. The LACP settings on the switch with the lower MAC address takes precedence.

Port Priority Value

The switch uses ports' LACP priorities to determine which ports are active and which are in the standby mode in situations where the number of ports in the aggregate trunk exceeds the maximum number of allowed active ports. This parameter has a range of 1 to 65535. The lower the number, the higher the priority. Ports with the highest priorities are designated as the active ports in an aggregate trunk. The default value is a port's number. For example, the default priority values for ports 1 and 2 are 1 and 2, respectively.

As an example, if both 802.3ad-compliant devices support up to eight active ports, and there are a total of nine or more ports in the trunk, the eight ports with the highest priorities (lowest priority values) are designated as the active ports, and the others are placed in the standby mode. If an active link goes down on a active port, the standby port with the highest priority is automatically activated to take its place.

The selections of active links in an aggregate trunk are dynamic and change as links are added, removed, lost, or re-established. For example, if an active port loses its link and is replaced by a port in the standby mode, the re-establishment of the link on the originally active port causes the port to return to the active state because it has a higher priority value than the replacement port, which returns to the standby mode.

Two conditions must be met for a port in an aggregate trunk to function in the standby mode. First, the number of ports in the trunk has to exceed the highest allowed number of active ports, and second, the port must be receiving LACPDU packets from the other device. A port functioning in the standby mode does not forward network traffic. However, it continues to send LACPDU packets. If a port that is part of an aggregator does not receive LACPDU packets, it functions as a normal Ethernet port and forwards network packets along with LACPDU packets.

Note

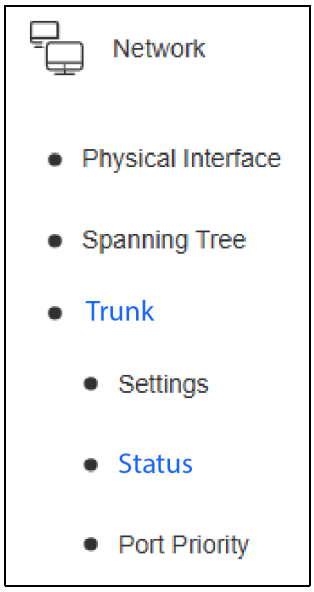
You can adjust a port's priority value.

General Guidelines

Here are LACP guidelines:

- LACP has to be activated on both the iGS950 Switch and its partner device.
- The other device has to be 802.3ad-compliant.
- iGS950 Switches support up to eight active ports in an aggregate trunk at a time.
- The ports of an aggregate trunk have to be the same medium type: all copper ports or all fiber optic ports.
- The ports of a trunk can be consecutive (for example ports 1-5) or nonconsecutive (for example, ports 2, 4, 6, 8).
- A port can belong to only one aggregator at a time.
- The ports of an aggregate trunk have to be members of the same VLAN.
- Copper ports have to be set to Auto-Negotiation or full-duplex mode. LACP trunking does not support half-duplex mode.
- 1000Base-X fiber optic ports have to be set to full-duplex mode.
- You can create an aggregate trunk of transceivers with 1000Base-X fiber optic ports.
- Only ports in an aggregator transmit LACPDU packets.
- Member ports in an aggregator function as part of an aggregate trunk only when receiving LACPDU packets from a remote device. If they do not receive LACPDU packets, they function as regular Ethernet ports, forwarding network traffic, while also continuing to transmit LACPDU packets.
- The port with the highest priority in an aggregate trunk carries broadcast packets and packets with an unknown destination.
- Prior to adding an aggregate trunk between an Allied Telesis device and another vendor's device, refer to the vendor's documentation to determine the maximum number of active ports the device can support in a trunk. If the number is less than eight, the maximum number for iGS950 Switches, you should assign the other vendor's device a higher system LACP priority than your iGS950 Switch. This can help avoid a conflict between the devices if some ports are placed in the standby mode when the devices form the trunk. For background information, refer to "System Priority and ID Numbers" on page 258.
- LACPDU packets are transmitted as untagged packets.

Displaying LACP Group Status



To display the LACP Group Status, select **Network** > **Trunk** > **Status** from the menu. The LACP Group Status window is shown in Figure 86. The fields and table columns are described in Table 63.

Table 63. LACP Group Status Window

Field or Column	Description
System Priority	Displays the switch's LACP System Priority value, 32768. You cannot change this value. Refer to "System Priority and ID Numbers" on page 258.
System ID	Displays the MAC address of the switch. You cannot change this value.
LGA Group ID	Displays the group ID number of an LACP trunk. This value is not adjustable.
Member Ports	Displays the active and standby ports of the trunk.
Active Port List	Displays the ports that are active members of the LACP trunk. The iGS950 Switch supports up to eight active trunk members per trunk.
Standby Port List	Displays the ports that are standby members of the LACP trunk. The ports transmit and accept LACPDU packets, but do not forward network traffic.

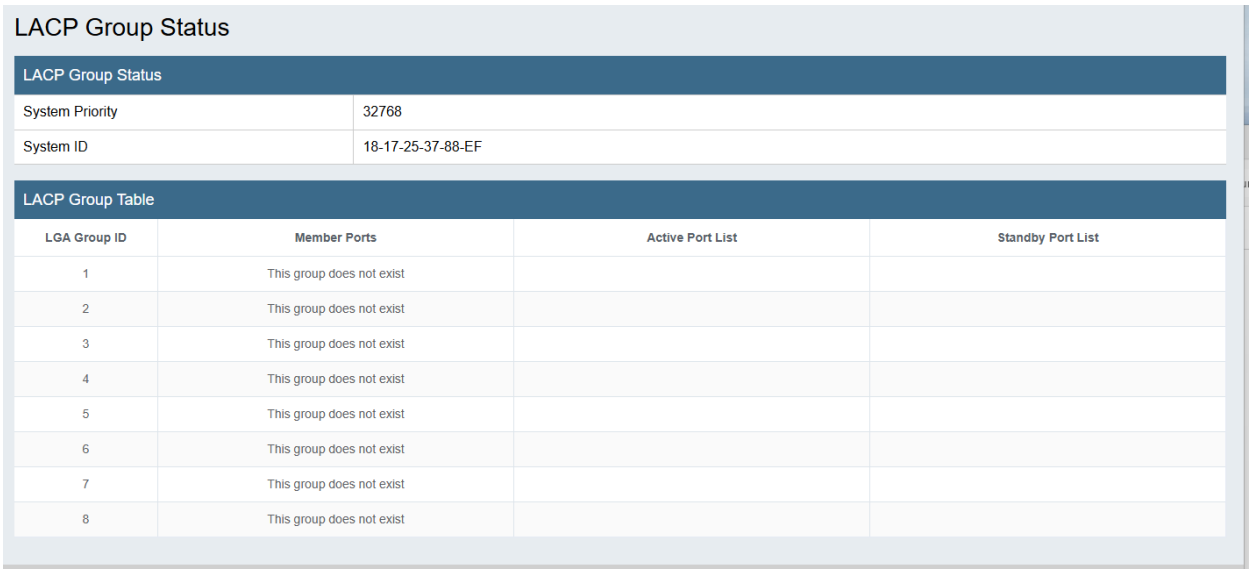
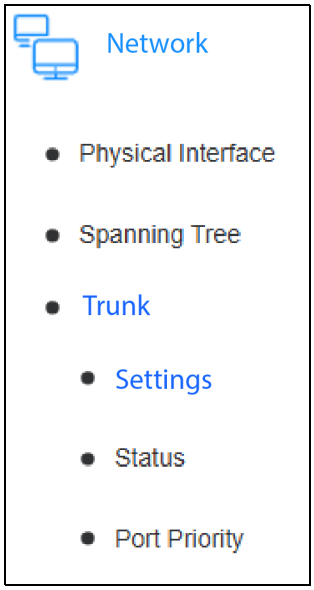


Figure 86. LACP Group Status Window

Adding LACP Trunks



Caution

Do not connect the cables of a port trunk until after you have configured the ports on both switches. Connecting the cables prior to configuring the ports can form loops in your network topology, which can result in broadcast storms that can reduce network performance.

To add LACP trunks to the switch:

1. Select **Network** > **Trunk** > **Settings** from the menu. The Trunking window is shown in Figure 85 on page 253.

   Each row represents a separate trunk. The numbers and check boxes represent the switch ports. Ports with check marks are members of a trunk. Note the following:

   - The AT-iGS950/10PS Switch supports up to four LACP or static port trunks.
   - All other AT-iGS950 Switches support up to eight LACP or static port trunks.

2. Click the check boxes of the ports for the trunk. Here are the guidelines:

   - A check in a box indicates the port is a member of the trunk. No check means the port is not a member.
   - Ports can be members of only one trunk at a time. Ports that are already members of a trunk have to be removed from their current trunk assignments before you can assign them to a different trunk.
   - An LACP trunk can have any number of ports. Up to eight ports can be active at one time.

3. Select one of the following from the menu in the right column of the Trunk ID row:

   - **Active**: Activates the ports for an LACP trunk. The ports send and respond to LACPDU packets by forming an LACP trunk.
   - **Passive**: Activates the ports for an LACP trunk. The trunk ports respond to LACPDU packets by forming an LACP trunk, but do not send LACPDU packets. You can use this setting if the other network device does not need to receive LACPDU packets to form LACP trunks.
   - **Disabled**: Disables an LACP trunk.

Note

The **Manual** setting in the menu is for static port trunks. Refer to Chapter 23, “Static Port Trunks” on page 249.

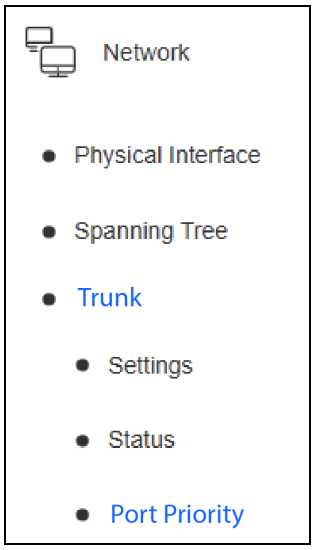
4. Click **Apply**.

Note

Select **Save** from the menu to save your changes.

5. Configure the ports on the other network device for LACP.
6. Connect the Ethernet cables between the trunk ports on the two devices.

Setting LACP Port Priorities



The switch uses LACP port priorities to select the active ports of a trunk when the number of ports exceeds the maximum number of eight active ports. For background information, refer to “Port Priority Value” on page 259.

To set a port’s priority:

1. Select the **Network** > **Trunk** > **Port Priority** from the menu. The Port Priority window is show in Figure 87.
2. Enter a value from 0 to 65535 in the Priority field for the port. The lower the number the higher the priority. The default is 0.

Note

The System Priority and System ID fields in the window are defined in Table 63 on page 261.

3. Click **Apply** at the bottom of the window.

Note

Select **Save** from the menu to save your changes.

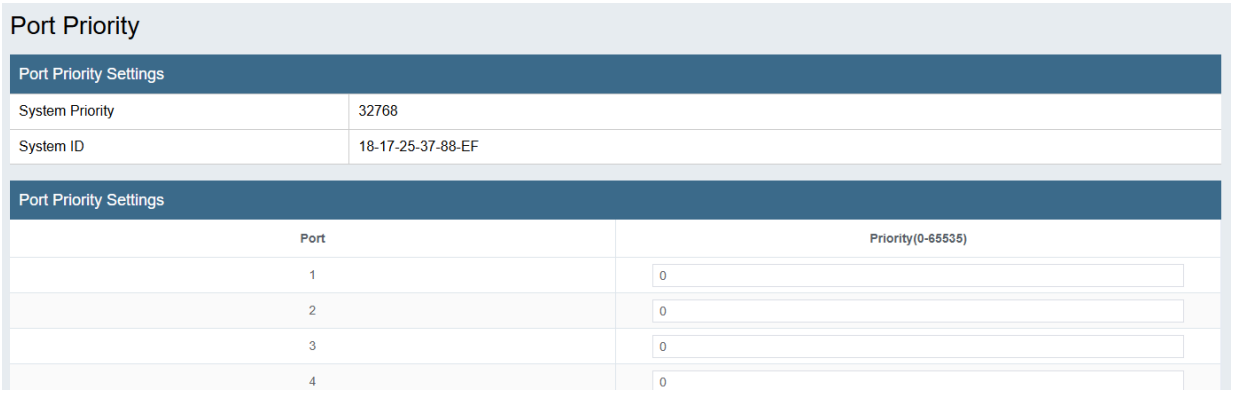
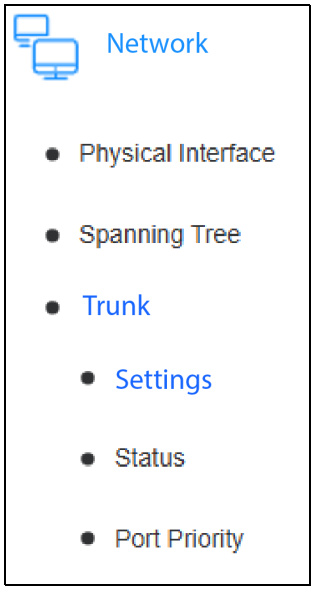


Figure 87. Port Priority Window

Modifying LACP Trunks



Caution

Before modifying a port trunk, disconnect all cables from its ports. Leaving the cables connected can create loops in your network topology, which can result in broadcast storms that can reduce network performance.

To add or remove ports from LACP trunks:

1. Disconnect all Ethernet cables from the trunk ports.
2. Select **Network** > **Trunk** > **Setting** from the menu. The Trunking window is shown in Figure 86 on page 261. The eight Trunk ID rows are the static and LACP trunks.
3. To add or remove ports from a trunk, click the port check boxes. Here are the guidelines:
   - A check in a box indicates the port is a member of the trunk. No check means the port is not a member.
   - An LACP trunk can have any number of ports. Up to eight ports can be active at one time.
   - Ports can be members of only one trunk at a time. Ports that are already members of a trunk have to be removed from their current trunk before you can add them to a different trunk.
4. To enable or disable an LACP trunk, change its status with the menu in the right column of the Trunk ID row. The choices are listed here:
   - **Active**: Activates the ports for an LACP trunk. The ports send and respond to LACPDU packets by forming an LACP trunk.
   - **Passive**: Activates the ports for an LACP trunk. The trunk ports respond to LACPDU packets by forming an LACP trunk, but do not send LACPDU packets. You can use this setting if the other network device does not need to receive LACPDU packets to form LACP trunks.
   - **Disabled**: Disables a static port or LACP trunk.

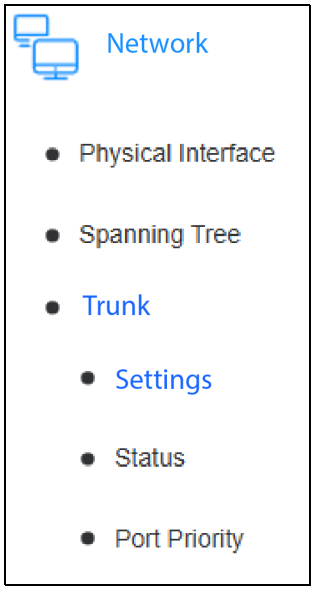
   Note

   The **Manual** setting in the menu is for static port trunks. Refer to Chapter 23, “Static Port Trunks” on page 249.
5. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

6. Configure the port trunk on the other switch.
7. Connect the Ethernet cables on the trunk ports on the switch and the other device.

Deleting LACP Trunks



Caution

Before deleting a port trunk, disconnect all cables from its ports. Leaving the cables connected can create loops in your network topology, which can result in broadcast storms that can reduce network performance.

To delete and LACP trunk:

1. Disconnect all Ethernet cables from the trunk ports.
2. Select **Network** > **Trunk** > **Setting** from the menu. The Trunking window is shown in Figure 85 on page 253.
3. Remove the ports from the trunk by clicking their check boxes to remove the check marks.
4. Set the status of the trunk to **Disabled** with the pull-down menu to the right of the trunk row.
5. Click **Apply**.

Note

Select **Save** from the menu to save your changes.

Chapter 25

Port Mirroring

This chapter describes port mirroring in the following sections:

- “Port Mirroring Overview” on page 270
- “Enabling Port Mirroring” on page 271
- “Disabling Port Mirroring” on page 273

Port Mirroring Overview

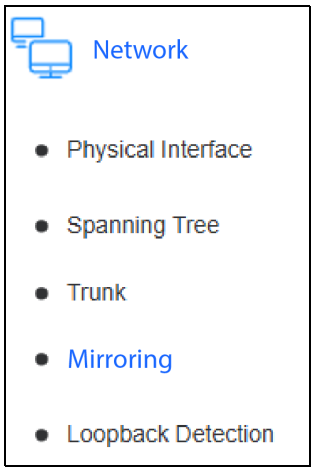
Port mirroring lets you unobtrusively monitor the traffic received or transmitted on one or more ports by copying the traffic to another switch port. By connecting a data analyzer to the port where the traffic is copied, you can monitor the traffic on the other ports without impacting network performance or speed. The feature can be used to troubleshoot network problems or investigate possible network attacks.

Port mirroring has two components. The ports whose traffic you want to mirror are called *source port(s)*. The port where the traffic will be copied is called the *mirroring port*.

Observe the following guidelines when using the port mirror:

- ❒ You can designate only one mirroring port.
- ❒ You can designate more than one source port. However, the more ports you mirror, the less likely the mirroring port will be able to handle all the traffic. For example, if you mirror the traffic of six heavily active ports, the mirroring port will likely drop packets, meaning that it will not provide an accurate mirror of the traffic of the source ports.
- ❒ The source and mirroring ports have to be located on the same switch.
- ❒ You can mirror the ingress traffic, egress traffic or both of the source ports.
- ❒ The mirroring port cannot be a member of a static or LACP trunk.
- ❒ The mirroring port is dedicated to monitoring the traffic from the source ports. It cannot be used for regular network operations.

Enabling Port Mirroring



This section explains how to activate port mirroring. You need to know the following to use the feature:

- ❒ Which port will be the mirroring port? The switch copies the traffic from the source port to this port. There can be only one mirroring port. The default is port 1.
- ❒ Which ports will be the source ports? These are the ports whose traffic you want to monitor. There can be more than one source port.
- ❒ Do you want to mirror the ingress traffic, egress traffic, or both on the source ports?

To enable port mirroring:

1. Select **Network** > **Mirroring** from the menu. The Mirroring window is shown in Figure 86.

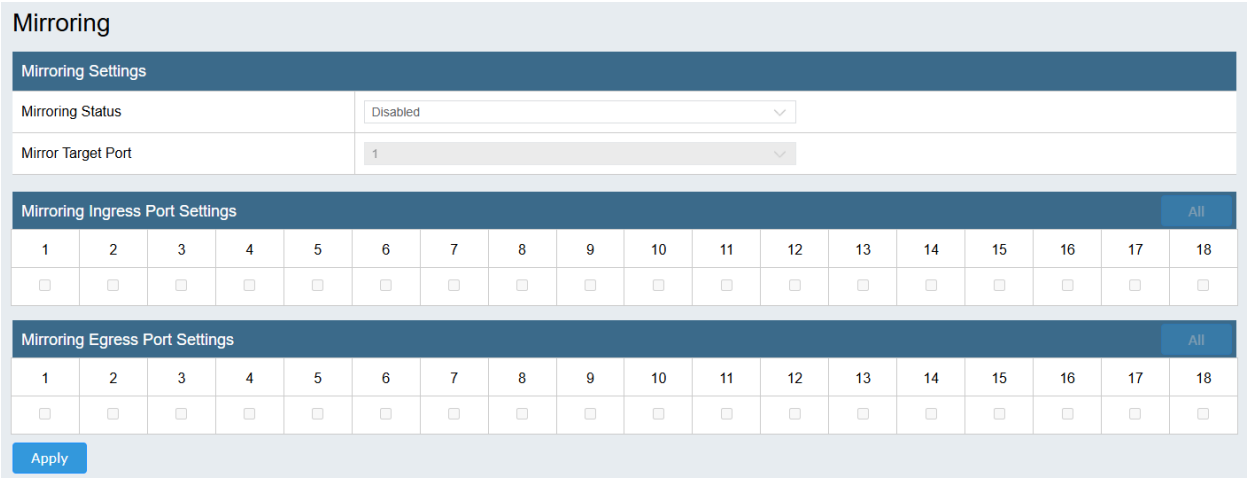


Figure 86. Mirroring Window

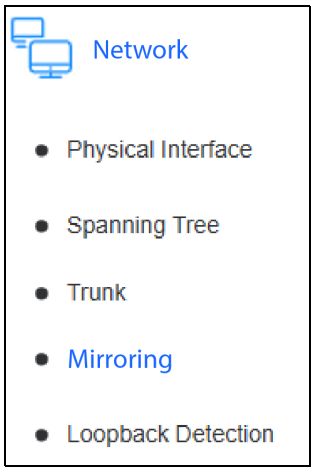
2. Select **Enabled** from the Mirroring Status menu. You have to enable the feature to configure it.
3. Select the mirroring port from the Mirror Target Port menu. You can select only one mirroring port.
4. Click the check boxes of the ports that are to be source ports:
   - ❒ Use the Mirroring Ingress Port Settings row to designate ports whose ingress traffic are to be mirrored.
   - ❒ Use the Mirroring Egress Port Settings row to designate ports whose egress traffic are to be mirrored.

5. Click **Apply**.The switch immediately activates port mirroring.

Note
Select **Save** from the menu to save your changes.

6. Connect a data analyzer to the mirroring port to monitor the Ethernet traffic on the source ports.

Disabling Port Mirroring



To disable port mirroring:

1. Select **Network** > **Mirroring** from the menu. The Mirroring window is shown in Figure 86 on page 271.
2. Select **Disabled** from the Mirroring Status field.
3. Click **Apply**.

   Port mirroring is now disabled on the switch. Traffic on the source ports are no longer copied to the mirroring port. The parameters in the window become inactive. You can now use the mirroring port for regular network operations.

Note
Select **Save** from the menu to save your changes.

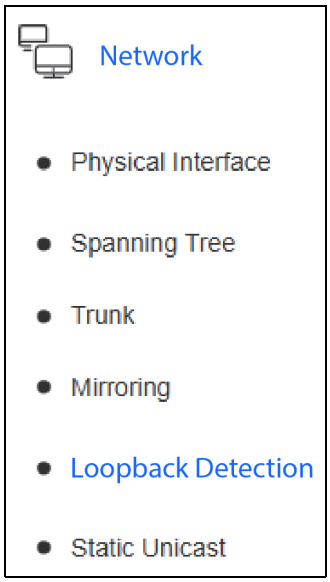
Chapter 26

Loopback Detection

This chapter describes loopback detection in the following sections:

- “Configuring Loopback Detection” on page 276
- “Disabling Loopback Detection” on page 279

Configuring Loopback Detection



The switch uses loopback detection to test for the following network problems:

- Network loops between directly connected upstream and downstream switches and the tested switch.
- Shorts or crossovers on the strands of wires in the network cables on the copper ports.

The switch automatically disables ports if it detects either of the loopback conditions.

Note
Loopback detection requires that spanning tree protocol be disabled. Refer to “Configuring STP and RSTP Global Settings” on page 206.

To activate and configure loopback detection:

1. Select **Network** > **Loopback Detection** from the menu. The Loopback Detection window is shown in Figure 87 on page 278.
2. Configure the settings in Table 63.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 63. Loopback Detection Window

Field	Description
Loopback Detection Settings	
Loopback Detection Status	Select one of the following: - **Enabled** - Enables loopback detection. You must enable the feature to configure it. - **Disabled** - Disables loopback detection. This is the default setting.

Table 63. Loopback Detection Window (Continued)

Field	Description
Loopback Detection Time Settings	
Interval	Enter the interval, in seconds, between tests. The range is 1 to 32767 seconds. The default is two seconds.
Recover Time	Enter the number of seconds ports remain disabled after a loopback condition is corrected. The range is 60 to 1000000 seconds. The default is 60 seconds.
Loopback Detection Table	
Port	Lists the individual ports on the switch.
Loopback Detection State	Select one of the following: ❒ **Enabled**: Enables the feature on the port. The switch disables the port, blocking it from forwarding traffic, if it detects a loopback condition. ❒ **Disabled**: Disables the feature on the port. This is the default state. The All row is used to apply the same setting to all ports.
Loop Status	Displays the status of the test on the individual ports. Possible states are listed here: - Normal: The test is not detecting any problems with the copper cables. - Loop: The test disabled the port after detecting a loopback condition on the copper cable. The port remains disabled until the condition is resolved and the recovery timer expires, or the switch is reset.

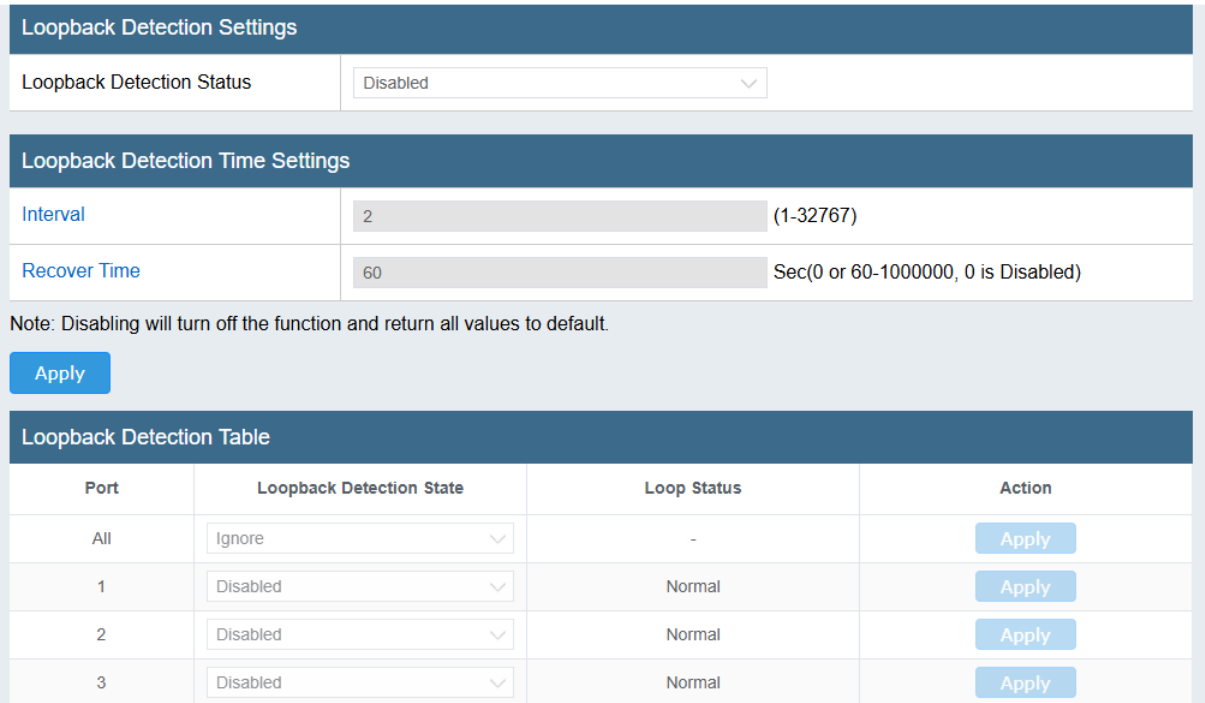
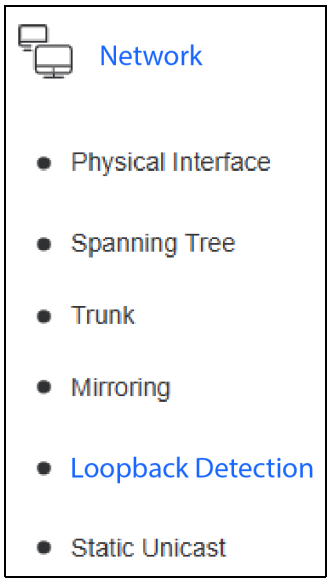


Figure 87. Loopback Detection Window

Disabling Loopback Detection



To disable loopback detection:

1. Select **Network** > **Loopback Detection** from the menu. The Loopback Detection window is shown in Figure 87 on page 278.
2. Select **Disabled** from the Loopback Detection Status menu.
3. Click **Apply**

Note
Select **Save** from the menu to save your changes.

Chapter 27

Static Unicast MAC Addresses

This chapter describes static unicast MAC addresses in the following sections:

- ❒ “Static MAC Addresses Overview” on page 282
- ❒ “Adding Static Unicast MAC Addresses” on page 284
- ❒ “Modifying Static Unicast MAC Addresses” on page 286
- ❒ “Deleting Static Unicast MAC Addresses” on page 287

Static MAC Addresses Overview

The switch has a MAC address table for storing the MAC addresses of the network devices connected to its ports. Each entry in the table consists of a MAC address, a port number where an address was learned by the switch, and an ID number of a VLAN where a port is a member.

The switch learns the MAC addresses of the network devices by examining the source addresses in the packets as they arrive on the ports. When the switch receives a packet that has a source address that is not already in the table, it adds the address, along with the port number where the packet was received and the ID number of the VLAN where the port is a member. The result is a table that contains the MAC addresses of all the network devices that are connected to the switch's ports.

The purpose of the table is to allow the switch to forward packets more efficiently. When a packet arrives on a port, the switch examines the destination address in the packet and refers to its MAC address table to determine the port where the destination node of that address is connected. It then forwards the packet to that port and on to the network device.

If the switch receives a packet with a destination address that is not in the MAC address table, it floods the packet to all its ports, excluding the port where the packet was received. If the ports are grouped into virtual LANs, the switch floods the packet only to those ports that belong to the same VLAN from which the packet originated. This prevents packets from being forwarded to inappropriate LAN segments and increases network security. When the destination node responds, the switch adds its MAC address and port number to the MAC address table.

If the switch receives a packet with a destination address that is on the same port on which the packet was received, it discards the packet without forwarding it on to any port. There is no reason for the switch to forward the packet because the source and destination nodes are located on the same port on the switch. This too increases network performance by preventing frames from being forwarded unnecessarily to other network devices.

MAC addresses learned by the switch are referred to as dynamic addresses. Dynamic MAC addresses are not stored indefinitely in the MAC address table. They are automatically deleted when they are inactive. A MAC address is considered inactive if the switch does not receive any frames from the network device after a specified period of time. The switch assumes that the node with that MAC address is no longer active and that its MAC address can be deleted from the table. This prevents the MAC address table from becoming filled with addresses of inactive nodes.

The period of time the switch waits before deleting inactive dynamic MAC addresses is called the aging time. This value is adjustable on the switch. The default value is 300 seconds (5 minutes).

You can also enter addresses manually into the table. These addresses are referred to as static addresses. Static MAC addresses remain in the table indefinitely and are never deleted, even when the network devices are inactive. Static MAC addresses are useful for addresses that the switch might not learn through its normal learning process or for addresses that you want the switch to retain, even when the end nodes are inactive.

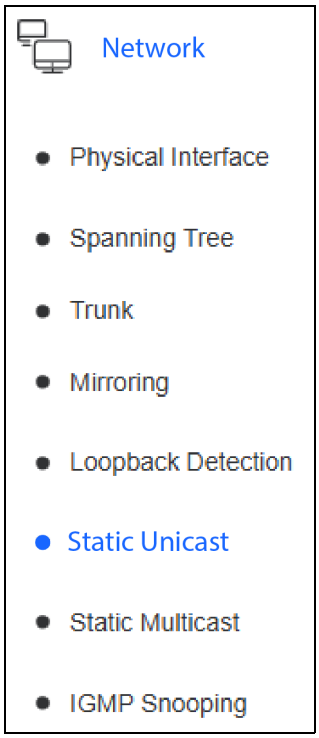
Adding Static Unicast MAC Addresses

The procedure in this section explains how to add static unicast MAC addresses to the MAC address tables for devices that are members of 802.1Q tagged VLANs. Entering a new static unicast MAC address requires the following information:

- The static unicast MAC address.
- The VID of the 802.1Q tagged VLAN.
- The switch port of the device.

Here are the guidelines:

- You can assign a static unicast MAC address to only one switch port.
- The 802.1Q tagged VLAN must already exist on the switch. For instructions, refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.
- The switch has a maximum capacity of 255 static unicast addresses.



To add static unicast addresses to the switch:

1. Select **Network** > **Static Unicast** from the menu. The Static Unicast Address Table window is shown in Figure 88 on page 285.

   The table at the bottom of the window display the current static unicast MAC addresses on the switch: The table columns are described in Table 64.

Table 64. Static Unicast Table

Column	Description
VLAN	Displays the VLAN ID of the 802.1Q tagged VLAN of the MAC address.
MAC Address	Displays the static MAC address.
Port Members	Displays the switch port number of the address.
Action	Contains Modify and Delete buttons.

2. Enter the VID of the 802.1Q VLAN in which the static unicast MAC address belongs. A static unicast MAC address can have only one VID. The VLAN must already exist on the switch.

3. Enter the static unicast MAC address in the **Group MAC Address** field. You can enter only one address at a time.

4. Designate the port of the MAC address by clicking the corresponding radio button in Port Member Settings. You can select only one port.

5. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

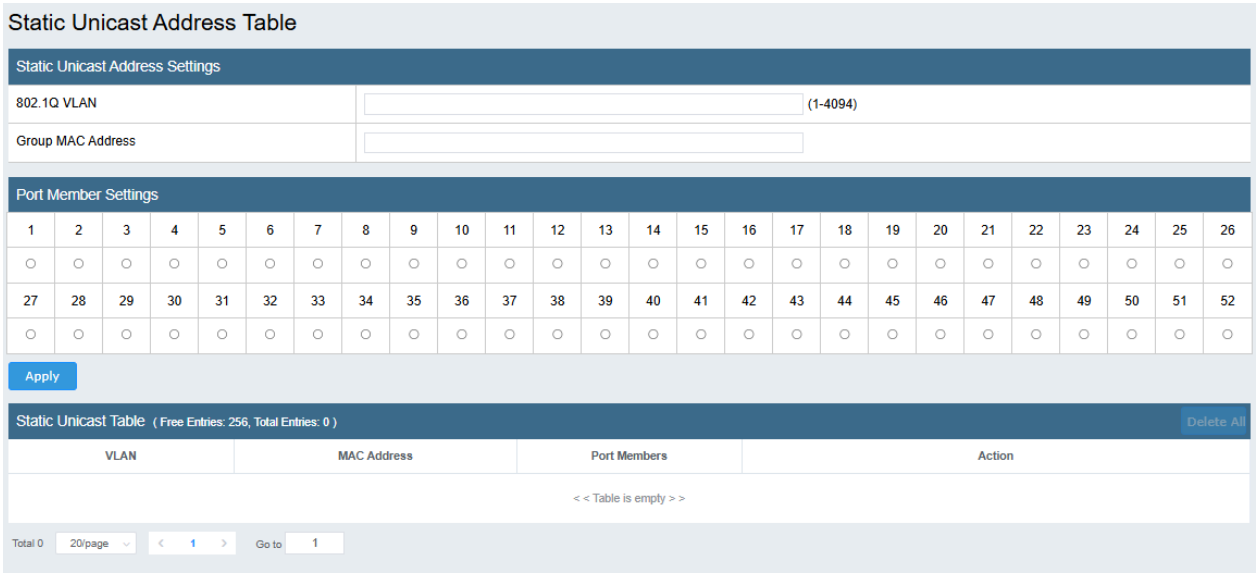
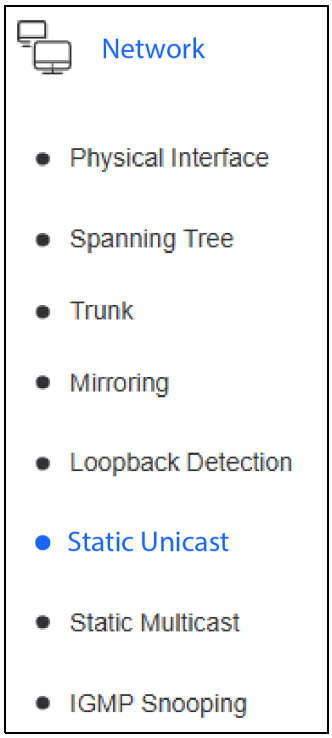


Figure 88. Static Unicast Address Table Window

Modifying Static Unicast MAC Addresses

This procedure explains how to change the port assignments of unicast MAC addresses. Here are the guidelines:

- You cannot change the VLAN or MAC address of a static address with this procedure. Instead, you must delete the entry from the switch and enter it again with the new VLAN or MAC address. Refer to “Deleting Static Unicast MAC Addresses” on page 287.
- The 802.1Q Tagged VLAN must already exist on the switch. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.

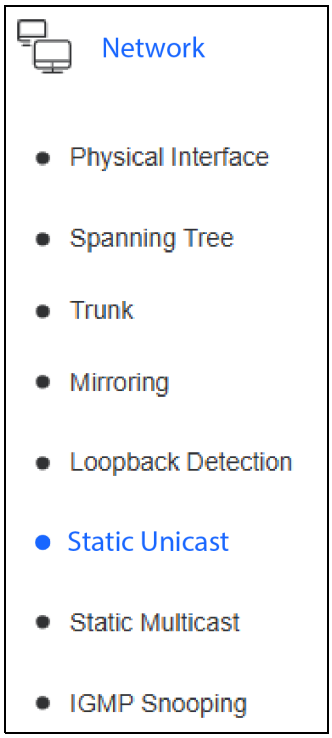


To modify the port assignment of a unicast MAC address:

1. Select **Network** > **Static Unicast** from the menu. The Static Unicast Address Table window is shown in Figure 88 on page 285.
2. Click **Modify** in the Action column of the static MAC address you want to change. You can modify only one address at a time. The Modify Static Unicast Address window changes to display the details of the selected address.
3. Select the new port of the MAC address by clicking the corresponding radio button in Port Member Settings. You can select only one port.
4. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Deleting Static Unicast MAC Addresses



To delete a static MAC addresses from the switch:

1. Select **Network** > **Static Unicast** from the menu. The Static Unicast Address Table window is shown in Figure 88 on page 285.
2. Click **Delete** in the Action column of the MAC address to be deleted. You can delete only one address at a time. The switch deletes the MAC address.

Note
Select **Save** from the menu to save your changes.

Chapter 28

Static Multicast MAC Addresses

Static multicast addresses are described in the following sections:

- “Adding Static Multicast MAC Addresses” on page 290
- “Modifying Static Multicast MAC Addresses” on page 292
- “Deleting Static Multicast Addresses” on page 293

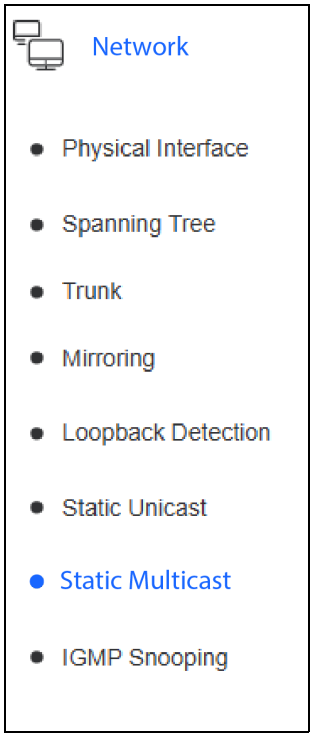
Adding Static Multicast MAC Addresses

This section contains the procedure for adding static multicast MAC addresses to the ports on the switch. The switch supports up to 256 static multicast addresses. Static multicast MAC addresses require the following information:

- The static multicast MAC address.
- For a static multicast MAC address for ports in a 802.1Q tagged VLAN, the VID of the VLAN.
- The switch ports that are connected to the host nodes and multicast router of the multicast address.

Here are the guidelines:

- You can assign static multicast MAC addresses to hosts ports and multicast router ports.
- To assign a multicast MAC address to ports in an 802.1Q tagged VLAN, you have to add the VLAN to the switch first. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.
- The switch has a maximum capacity of 255 static multicast addresses.



To add static multicast addresses to the switch:

1. Select **Network** > **Static Multicast** from the menu. The Static Multicast Address Table window is shown in Figure 89 on page 291.
2. To add a static multicast MAC address to an 802.1Q Tagged VLAN, enter in the **802.1Q VLAN** field the VID of the tagged VLAN containing the host and router ports of the multicast address. You can enter only one VID. The range is 1 to 4094. The VLAN has to already exist on the switch.
3. Enter a multicast MAC address in the **Group MAC Address** field.
4. Designate the ports of the multicast group by clicking the corresponding radio boxes in **Group Member**. The ports should include host ports and the multicast router port.
5. Click **Apply** to activate your change.

Note
Select **Save** from the menu to save your changes.

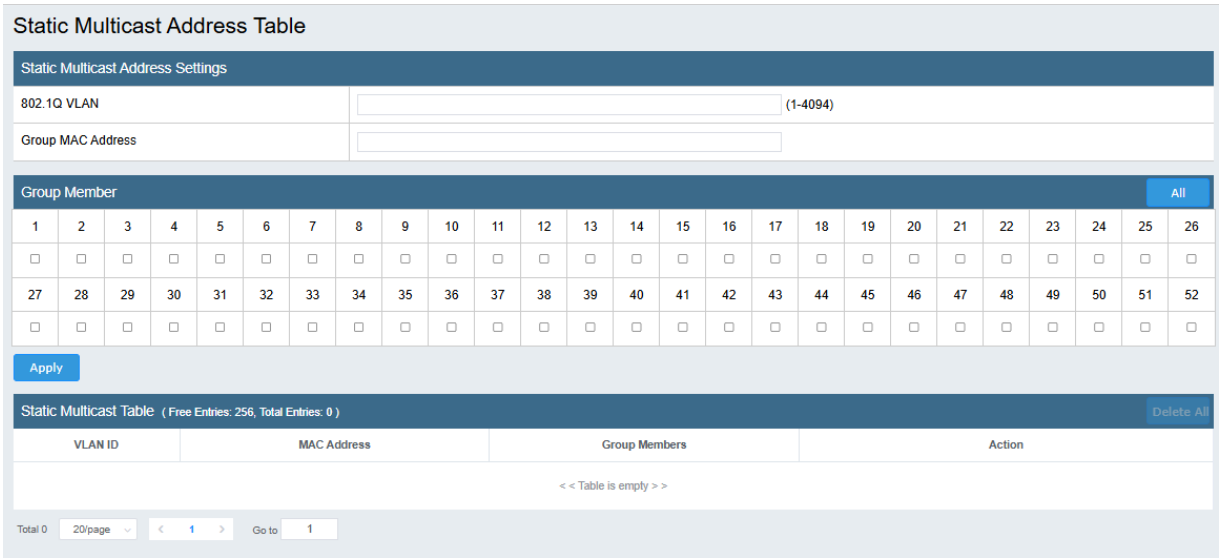


Figure 89. Static Multicast Address Table Window

The Static Multicast Table at the bottom of the window displays the current static multicast MAC addresses belonging to 802.1Q tagged VLANs. The columns in the table are explained in Table 65.

Table 65. Static Multicast Address Table

Column	Description
VLAN ID	Displays the VLAN ID of the tagged VLAN of the MAC address.
MAC Address	Displays the static multicast MAC address.
Group Members	Displays the port numbers of the host and router ports where the address is assigned.
Action	Contains Modify and Delete buttons.

Modifying Static Multicast MAC Addresses

This procedure explains how to change the port assignments of multicast MAC addresses. Here are the guidelines:

- You cannot change the VLAN or MAC address of a multicast address with this procedure. Instead, you have to delete the entry from the switch and enter it again with the new VLAN or MAC address. Refer to “Deleting Static Multicast Addresses” on page 293.
- For you to assign a MAC address to a port in an 802.1Q VLAN, the VLAN has to already exist on the switch. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.

To modify the port assignments of a multicast MAC address:

1. Select **Network** > **Static Multicast** from the menu. The Static Multicast window is shown in Figure 89 on page 291.
2. Click **Modify** in the Action column of the static MAC address you want to change. You can modify only one address at a time. The details of the address are displayed in the Modify Static Multicast Address window.
3. Add or delete ports from the MAC address by clicking the corresponding radio buttons under **Group Member**.
4. Click **Apply** to activate your change.

Note
Select **Save** from the menu to save your changes.

Deleting Static Multicast Addresses

To delete static multicast MAC addresses from the MAC address table:

1. Select **Network** > **Static Multicast** from the menu. The Static Multicast window is shown in Figure 89 on page 291.
2. Do one of the following:
   - ❒ To delete a single entry, click **Delete** in the Action column.
   - ❒ To delete all 802.1Q address entries, click **Delete All** above the table.
3. Click **Apply** to activate your change.

Note
Select **Save** from the menu to save your changes.

Chapter 29

IGMP Snooping

This chapter explains the IGMP snooping feature in the following sections:

- ❒ “IGMP Snooping Overview” on page 296
- ❒ “Configuring IGMP Snooping” on page 298
- ❒ “Adding or Deleting Static Multicast Router Ports” on page 302

IGMP Snooping Overview

The switch uses IGMP snooping to improve network performance of multicast groups by directing multicast traffic to only those ports in VLANs that have multicast hosts. The switch monitors the transmissions of queries from multicast routers, and reports and leave requests from hosts, to build its own multicast membership lists. It uses the lists to forward multicast packets only to ports with host nodes. Without IGMP snooping, the switch has to flood multicast traffic to all VLAN ports, including ports without host nodes.

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

Nodes that want to become members of multicast groups respond to queries by sending *reports*. Nodes that join multicast groups are referred to as *host nodes*. After joining multicast groups, host nodes have to periodically issue new reports to remain group members.

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

There are three versions of IGMP— versions 1, 2, and 3. A difference between the versions is how a host node signals that it no longer wants to be a member of a multicast group. In version 1, it stops sending reports. If a router does not receive a report from a host node after a pre-defined length of time, referred to as a *time-out value*, it assumes that the host node no longer wants to receive multicast frames and removes it from the membership list of the multicast group. If there are no additional member hosts on the port, the switch stops forwarding multicast packets from it.

In version 2, a host node exits from a multicast group by sending a *leave request*. After receiving a leave request from a host node, the router removes the node from the appropriate membership list. It also stops sending multicast packets from the port if it determines there are no additional host nodes on the port.

Version 3 adds the ability of host nodes to join or leave specific sources in multicast groups. It also enables the switch to build membership reports of the host nodes, and to send the reports in lien of individual report and

leave requests to multicast routers, thereby reducing traffic overhead.

Note
The iGS950 Switch do not support IGMPv3 snooping.

The IGMP snooping feature on the iGS950 Switch supports IGMP versions 1 and 2. The switch monitors the flow of queries from routers and checks report and leave messages from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets only to ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by restricting the flow of multicast packets only to those ports connected to host nodes. The switch can support up to 256 multicast addresses.

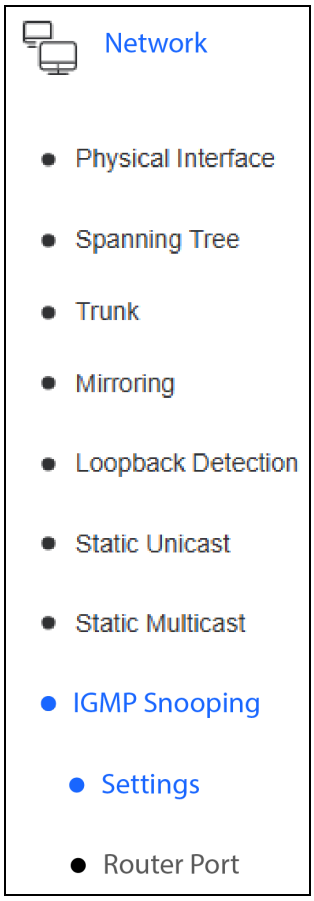
Without IGMP snooping, a switch has to flood multicast packets on all VLAN ports, except the port on which it received the packet. Such flooding of packets can reduce network performance.

The switch also has IGMP snooping querier. You can use this feature if your network has multicast traffic, but no multicast routers. When the feature is enabled, the switch sends out queries, searching for host nodes in VLANs on its ports wanting to join multicast groups.

The iGS950 Switch maintains a list of multicast groups through an adjustable time-out value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Note
The default setting for IGMP snooping is disabled.

Configuring IGMP Snooping



To configure IGMP snooping:

1. Select **Network** > **IGMP Snooping** > **Settings** from the menu. The IGMP Snooping Settings window is shown in Figure 90 on page 301.
2. Configure the parameters in Table 66.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 66. IGMP Snooping Settings Window

Setting	Description
IGMP Snooping Status	Select one of the following options: - **Enabled**: Enables IGMP snooping on the switch. You have to enable IGMP snooping to configure the settings. - **Disabled**: Disables IGMP snooping. This is the default setting.
Aging Timeout	Enter the maximum time in seconds the switch should wait for reports from hosts wanting to remain members of multicast groups. Hosts are removed from multicast groups if they do not send reports before the age-out timer expires. The range is 130 to 153025 seconds. The default is 260 seconds.
Querier Status	Select the status of the IGMP snooping querier on the switch. The querier can be used in networks where there is multicast traffic but no multicast router. The switch uses the querier to send its own multicast queries to search for host nodes. The settings are: - **Enabled**: The multicast querier is enabled. The switch transmits its own queries for host nodes. - **Disabled**: The querier is disabled. This is the default setting.

Table 66. IGMP Snooping Settings Window (Continued)

Setting	Description
Fast Leave Status	Select whether the switch is to implement the fast leave feature after receiving an IGMP leave message from a host. Here are the settings: - Enabled: Upon receiving an IGMP leave message from a host, the switch immediately deletes the corresponding port from the multicast group. - Disabled: Disables the fast leave feature.
Query Interval	Enter the interval in seconds for the transmission of multicast queries for host nodes by the switch. Here are the guidelines: - Querier Status has to be enabled. - The query interval has to be less than the age-out timer. Otherwise, hosts might not receive multicast traffic. - The range is 60 to 600 seconds. The default is 125 seconds.
Max Response Time	Enter the maximum response time the switch adds to the query packets that it transmits to hosts. This is the maximum amount of time hosts have to respond to the queries. Here are the guidelines. - Querier Status has to be enabled. - The range is 10 to 25 seconds. The default is 10 seconds.
Robustness Variable	Enter the number of times hosts can fail to respond to consecutive snooping queries before the switch deletes them from multicast groups. For example, when set to 4, the switch deletes hosts from multicast groups if they fail to respond to four consecutive queries. The range is 2 to 255 times. The default is 2 times.

Table 66. IGMP Snooping Settings Window (Continued)

Setting	Description
Last Member Query Interval	Enter the maximum time in seconds the switch should wait before deleting multicast groups from VLAN ports when no hosts respond to IGMP query messages. The range is 1 to 25 seconds. The default is 1 second.
Router Timeout	Enter the maximum time the switch should wait for queries from multicast routers before removing them from its multicast tables. The range is 120 to 1200 seconds. The default is 250 seconds.

The Multicast Group Entries table at the bottom of the window lists the multicast addresses and ports with active host nodes in 802.1Q tagged VLANs. The tables do not include ports with inactive hosts. The columns in the table are described in Table 67.

Table 67. Multicast Group Entries Table in the IGMP Snooping Settings Window

Columns	Description
VLAN Index	Displays the VID of a tagged 802.1Q VLAN.
Multicast Group Address	Displays active dynamic multicast addresses in the VLAN. Also displays active and inactive static multicast addresses.
Member Ports	Displays active multicast routers and host ports.

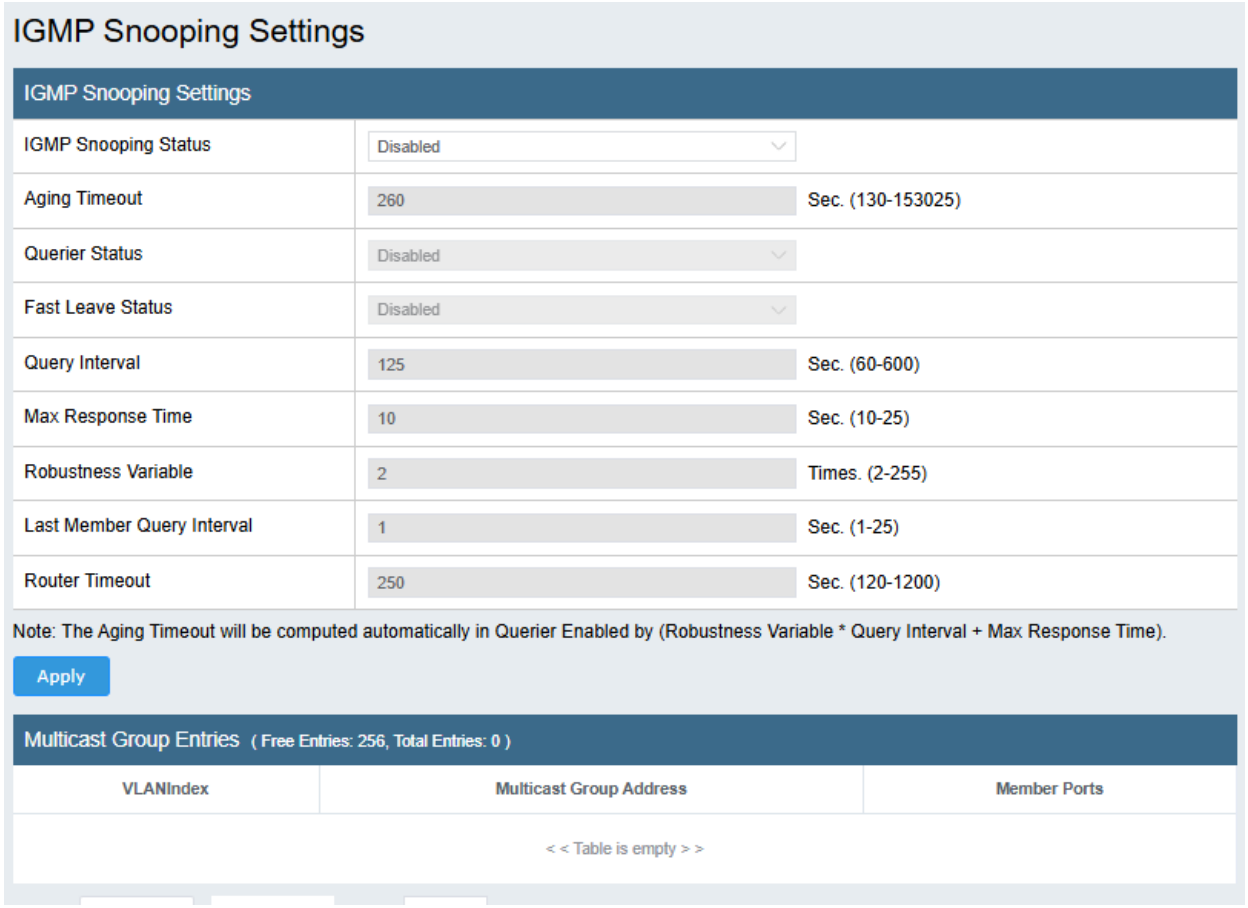
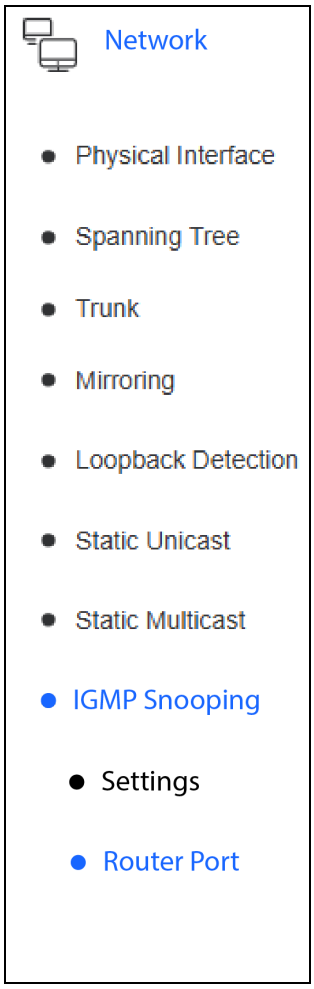


Figure 90. IGMP Snooping Settings Window

Adding or Deleting Static Multicast Router Ports



To support IGMP snooping, the switch needs to know which ports are connected to multicast routers. The switch receives queries from multicast routers on these ports, transmits reports from host nodes to routers, and receives multicast traffic streams. The switch can learn the ports automatically by watching for multicast queries on its ports from the routers, or you can designate the ports manually. The latter ports are referred to as static multicast router ports. You might add static router ports for multicast routers that the switch might not learn automatically or for routers the switch should never unlearn.

Static multicast router ports must belong to 802.1Q tagged VLANs. Thus, the first step to designating ports as static multicast router ports is to add the appropriate VLANs to the switch and add the ports to the VLANs. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.

To add or delete static multicast router ports:

1. Select **Network** > **IGMP Snooping** > **Router Port** from the menu. The switch displays the IGMP Snooping Router Port window in Figure 91 on page 303.The columns in the tables are described in Table 68.

Table 68. IGMP Snooping Router Port Window

Column	Description
VLAN ID	Displays the VIDs of tagged VLANs with a static or dynamic router port. The VLANs are listed individually.
Static Router Port	Displays ports that were manually designated as static multicast router ports in the VLAN.
Dynamic Router Port	Displays ports that the switch automatically learned as multicast router ports because it received queries from multicast routers on the ports.
Action	Displays the Modify button for adding or removing static multicast router ports to the VLAN.

2. To add or remove static multicast router ports from a VLAN, click the corresponding **Modify** button. The Modify IGS Static Router Port window is displayed. Refer to Figure 92 on page 303.

3. Click the check boxes of ports to be designated or removed as static multicast router ports. A check mark designates a port as a static multicast router port. VLANs can have more than one static multicast router port. The window includes these options:
   - ❒ To select all ports, click **All** in the left margin.
   - ❒ To restore the original settings, click **Restore** in the right margin.
4. Click **Apply** to activate your change.

Note
Select **Save** from the menu to save your changes.

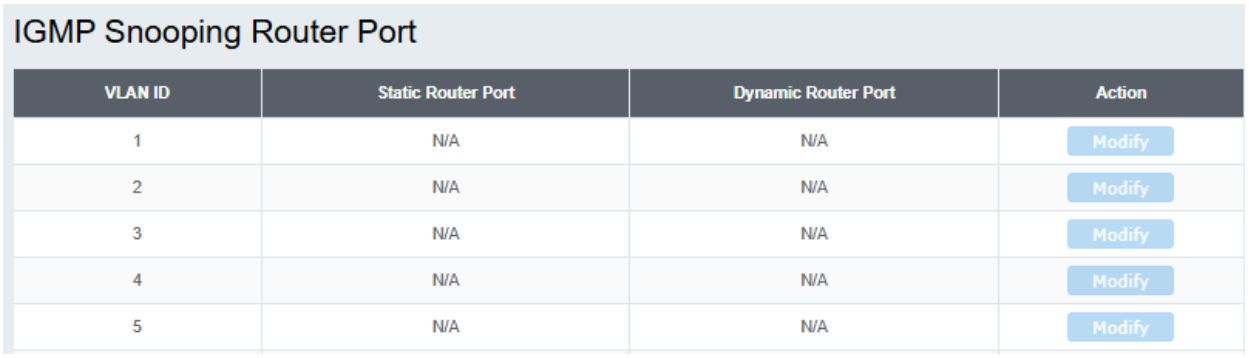


Figure 91. IGMP Snooping Router Port Window

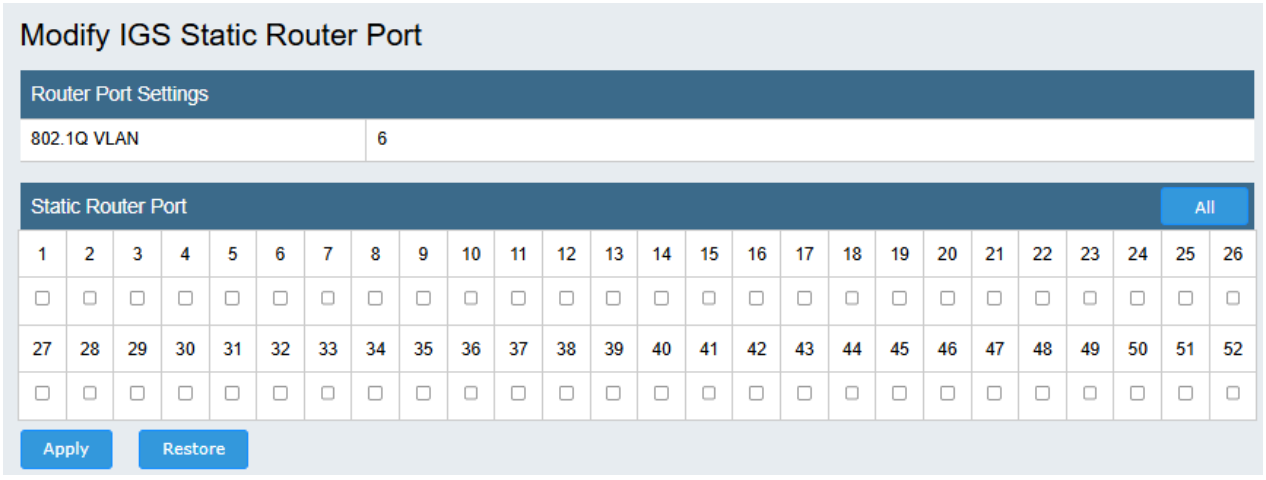


Figure 92. Modify IGS Static Router Port Window

Chapter 30

MLD Snooping

This chapter explains the MLD Snooping feature in the following sections:

- “MLD Snooping Overview” on page 306
- “Configuring MLD Snooping” on page 307
- “Adding or Deleting Static Multicast Router Ports” on page 311

MLD Snooping Overview

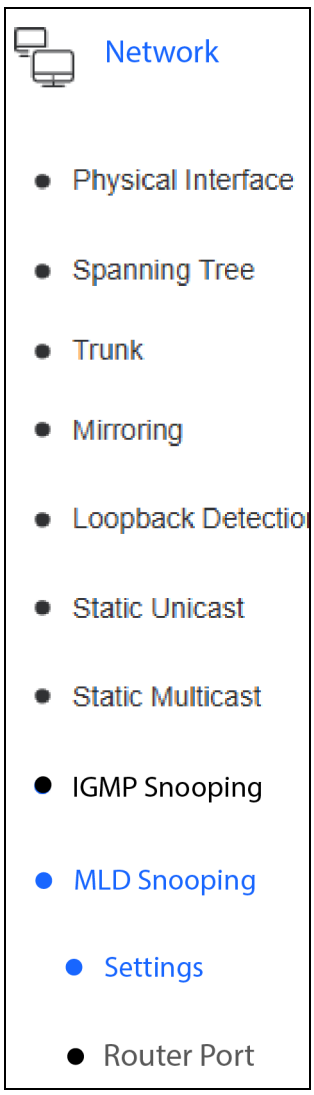
Layer 2 switches use MLD Snooping to listen to or "snoops" the MLD messages passing through them or from member hosts and multicast routers. The purpose of MLD Snooping is to provide efficient Layer 2 multicast forwarding, by sending only to hosts that have expressed an interest in receiving the multicast data.

Hosts express an interest in receiving multicast data for a given multicast group by sending an MLD join message. Without MLD Snooping, if one host expresses an interest in getting multicast data for a given group, by sending an MLD join for the multicast group, then all hosts connected to the same VLAN will also receive the multicast data. This wastes bandwidth on the switch ports connected to the host that are not interested in receiving the multicast data. Snooping takes note of exactly which ports have received joins for a given group, and send that group only to those ports.

The default setting for MLD Snooping is disabled.

MLD Snooping makes a distinction between Member ports, which are ports connected to members hosts, and Router ports, which are ports connected to, or directed towards, a Layer 3 router or a Layer 3 switch.

Configuring MLD Snooping



To configure MLD Snooping:

1. Select **Network** > **MLD Snooping** > **Settings** from the menu. The MLD Snooping Settings window is shown in Figure 93 on page 310.
2. Configure the parameters in Table 69.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 69. MLD Snooping Settings Window

Setting	Description
MLD Snooping Status	Select one of the following options: - **Enabled**: Enables MLD Snooping on the switch. You have to enable MLD Snooping to configure the settings. - **Disabled**: Disables MLD Snooping. This is the default setting.
Aging Timeout	Enter the maximum time in seconds the switch should wait for reports from hosts wanting to remain members of multicast groups. Hosts are removed from multicast groups if they do not send reports before the age-out timer expires. The range is 130 to 153025 seconds. The default is 260 seconds.
Querier Status	Select the status of the MLD snooping querier on the switch. The querier can be used in networks where there is multicast traffic but no multicast router. The switch uses the querier to send its own multicast queries to search for host nodes. The settings are: - **Enabled**: The multicast querier is enabled. The switch transmits its own queries for host nodes. - **Disabled**: The querier is disabled. This is the default setting.

Table 69. MLD Snooping Settings Window (Continued)

Setting	Description
Fast Leave Status	Select whether the switch is to implement the fast leave feature after receiving an MLD leave message from a host. Here are the settings: - Enabled: Upon receiving an MLD leave message from a host, the switch immediately deletes the corresponding port from the multicast group. - Disabled: Disables the fast leave feature.
Query Interval	Enter the interval in seconds for the transmission of multicast queries for host nodes by the switch. Here are the guidelines: - Querier Status has to be enabled. - The query interval has to be less than the age-out timer. Otherwise, hosts might not receive multicast traffic. - The range is 60 to 600 seconds. The default is 125 seconds.
Max Response Time	Enter the maximum response time the switch adds to the query packets that it transmits to hosts. This is the maximum amount of time hosts have to respond to the queries. Here are the guidelines. - Querier Status has to be enabled. - The range is 10 to 25 seconds. The default is 10 seconds.
Robustness Variable	Enter the number of times hosts can fail to respond to consecutive snooping queries before the switch deletes them from multicast groups. For example, when set to 4, the switch deletes hosts from multicast groups if they fail to respond to four consecutive queries. The range is 2 to 255 times. The default is 2 times.

Table 69. MLD Snooping Settings Window (Continued)

Setting	Description
Last Member Query Interval	Enter the maximum time in seconds the switch should wait before deleting multicast groups from VLAN ports when no hosts respond to MLD query messages. The range is 1 to 25 seconds. The default is 1 second.
Router Timeout	Enter the maximum time the switch should wait for queries from multicast routers before removing them from its multicast tables. The range is 120 to 1200 seconds. The default is 250 seconds.

The Multicast Group Entries table at the bottom of the window lists the multicast addresses and ports with active host nodes in 802.1Q tagged VLANs. The tables do not include ports with inactive hosts. The columns in the table are described in Table 70.

Table 70. Multicast Group Entries Table in the MLD Snooping Settings Window

Columns	Description
VLAN Index	Displays the VID of a tagged 802.1Q VLAN.
Multicast Group Address	Displays active dynamic multicast addresses in the VLAN. Also displays active and inactive static multicast addresses.
Member Ports	Displays active multicast routers and host ports.

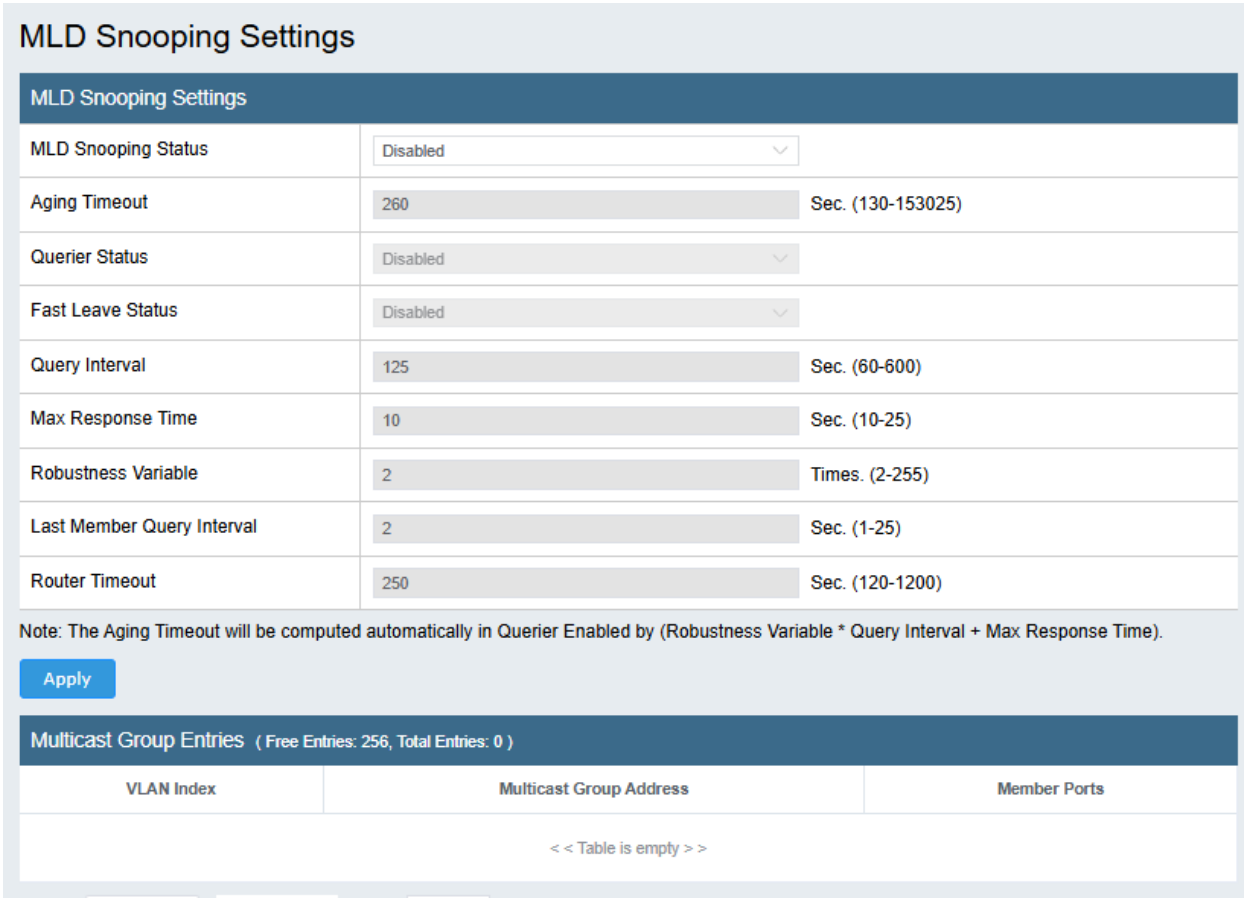
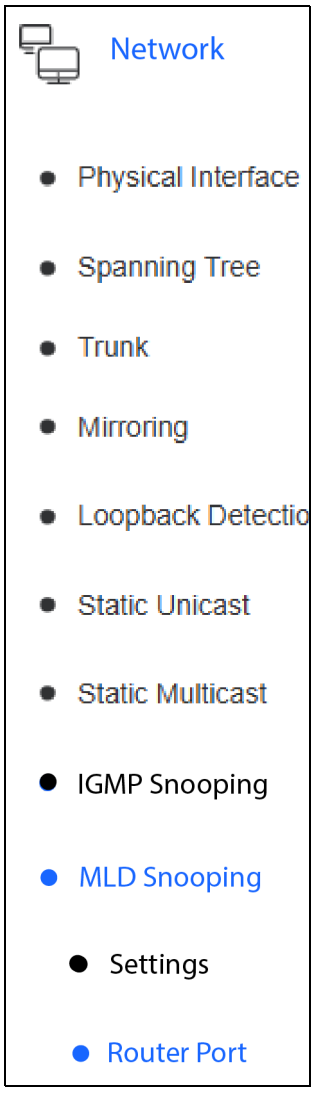


Figure 93. MLD Snooping Settings Window

Adding or Deleting Static Multicast Router Ports



To support MLD Snooping, the switch needs to know which ports are connected to multicast routers. The switch receives queries from multicast routers on these ports, transmits reports from host nodes to routers, and receives multicast traffic streams. The switch can learn the ports automatically by watching for multicast queries on its ports from the routers, or you can designate the ports manually. The latter ports are referred to as static multicast router ports. You might add static router ports for multicast routers that the switch might not learn automatically or for routers the switch should never unlearn.

Static multicast router ports must belong to 802.1Q tagged VLANs. Thus, the first step to designating ports as static multicast router ports is to add the appropriate VLANs to the switch and add the ports to the VLANs. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.

To add or delete static multicast router ports:

1. Select **Network** > **MLD Snooping** > **Router Port** from the menu. The switch displays the MLD Snooping Router Port window in Figure 94 on page 312.The columns in the tables are described in Table 71.

Table 71. MLD Snooping Router Port Window

Column	Description
VLAN ID	Displays the VIDs of tagged VLANs with a static or dynamic router port. The VLANs are listed individually.
Static Router Port	Displays ports that were manually designated as static multicast router ports in the VLAN.
Dynamic Router Port	Displays ports that the switch automatically learned as multicast router ports because it received queries from multicast routers on the ports.
Action	Displays the Modify button for adding or removing static multicast router ports to the VLAN.

2. To add or remove static multicast router ports from a VLAN, click the corresponding **Modify** button. The Modify IGS Static Router Port window is displayed. Refer to Figure 95 on page 312.

3. Click the check boxes of ports to be designated or removed as static multicast router ports. A check mark designates a port as a static multicast router port. VLANs can have more than one static multicast router port. The window includes these options:
   - ❒ To select all ports, click **All** in the left margin.
   - ❒ To restore the original settings, click **Restore** in the right margin.
4. Click **Apply** to activate your change.

Note
Select **Save** from the menu to save your changes.

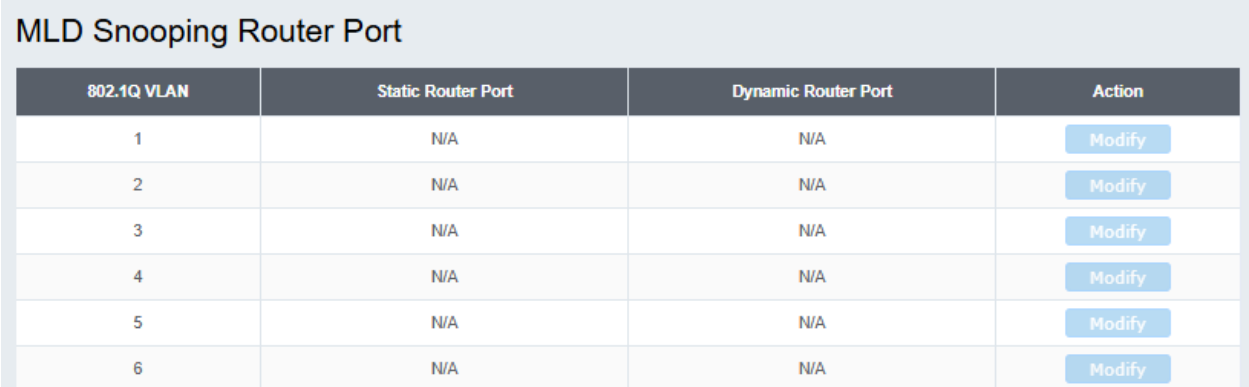


Figure 94. MLD Snooping Router Port Window

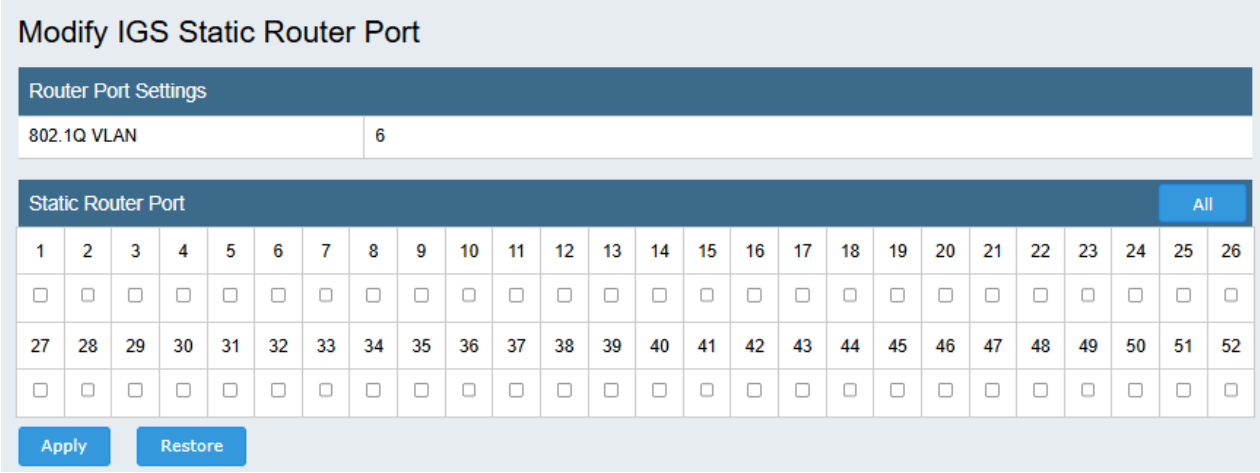


Figure 95. Modify IGS Static Router Port Window

Chapter 31

Multicast VLANs

This chapter describes multicast VLANs in the following sections:

- “Introduction” on page 314
- “Managing Multicast VLANs” on page 315
- “Viewing Multicast VLANs” on page 320
- “Managing Multicast Address Profiles” on page 322
- “Managing Associations of Multicast VLANs with Multicast Address Profiles” on page 325

Introduction

Multicast VLANs are employed in network environments where multiple destination devices need to receive the same traffic stream from a single source. The VLANs improve network efficiency and performance by allowing one source to provide a single traffic stream to multiple destinations. The alternative, where a source device delivers individual traffic streams to each destination device, would result in reduced network performance from avoidable consumption of network bandwidth by identical traffic streams.

Adding multicast VLANs has three main steps:

- Step 1: “Adding Multicast VLANs” on page 315 - The multicast VLAN defines the VLAN name, ID number, source ports, and destination ports of the multicast stream.
- Step 2: “Adding Multicast Address Profiles” on page 322 - Multicast address profiles define the IPv4 or IPv6 multicast address ranges of the multicast traffic from the source device.
- Step 3: “Adding Associations” on page 325 - Associations join the multicast VLAN with the multicast profile.

To view the existing multicast VLANs on the switch, display the Multicast VLAN Table window by selecting **Network** > **Multicast VLAN** > **VLAN Table** from the menu. An example of the window is shown in Figure 97 on page 320 and Table 72 on page 320.

Managing Multicast VLANs

This section contains the following procedures:

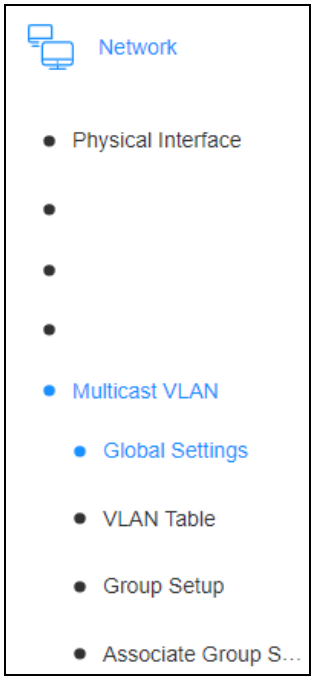
- “Adding Multicast VLANs,” next
- “Editing Multicast VLANs” on page 317
- “Deleting Multicast VLANs” on page 319

Adding Multicast VLANs

This procedure contains instructions for adding multicast VLANs to the switch. Adding a multicast VLAN requires the following information:

- IPv4 or IPv6 address type of the source traffic
- VLAN ID in the range 1 to 52.
- VLAN name
- Source port: This port is connected to the device generating the source traffic flow. This can be any port on the switch.
- Destination ports: These ports are connected to the destination devices that are to receive the traffic flow. This can be all of the ports on the switch, minus the source port.

To add a multicast VLAN:



1. Select **Network** > **Multicast VLAN** > **Global Settings** from the menu to display the Multicast Global Settings window. Refer to Figure 96 on page 317.
2. Under the Multicast Global Settings section at the top of the window, set the following two parameters to designate whether the source device will use IPv4 or IPv6 addressing for the multicast traffic:
   - Multicast IPv4 State
   - Multicast IPv6 State

   Settings are:
   - Disabled: The source device is not using IPv4 or IPv6 addressing to transmit the multicast stream. This is the default setting.
   - Enabled: The source device is using IPv4 or IPv6 addressing to transmit the multicast stream.
3. Click **Apply**.
4. Under the Multicast VLAN Settings section in the window, configure these two settings:
   - VLAN ID: Enter an ID number for the multicast VLAN. The range is 2 to 4094. The selected value must be unique from the ID numbers

of all current VLANs on the switch. To view the existing VLANs and their VIDs, refer to “Viewing All 802.1Q Tagged VLANs” on page 352.

- ❒ VLAN Name: Enter a name for the VLAN. The name can be up to 32 characters. Spaces are allowed, but not special characters. The name must be unique from all other VLAN names on the switch.

5. Click **Add**.

Note
At this point, the switch adds the multicast VLAN to its VLAN database, but without the source and destination ports.

6. To designate the destination ports of the multicast VLAN, perform the following steps:

   a. Under The Port Setting of Multicast section of the window, click the **Edit** button under **Receiver Ports**. This displays the Receiver Ports Settings window.

   b. Select the tagged and/or untagged ports that will be connected to destination devices of the multicast VLAN by clicking on the corresponding dialog circles under the port numbers. The destination ports can be all ports on the switch, minus the source port. There are no default destination ports.

   c. Click the **Apply** button at the bottom of the Receiver Ports Settings window to implement your change.

   d. Click the **Previous Page** button at the bottom to the window to return to the Multicast Global Settings window.

   e. Click the **Apply** button under Action in The Port Setting of Multicast section of the window.

7. To designate the source ports of the multicast VLAN, perform these steps:

   a. Under The Port Setting of Multicast section of the window, click the **Edit** button under **Source Ports**. This displays the Source Ports Settings window.

   b. Select the tagged and/or untagged ports that will be connected to the source device of the multicast VLAN by clicking on the corresponding dialog circles under the port numbers. There are no default source ports.

   c. Click the **Apply** button at the bottom of the Receiver Ports Settings window to implement your change.

d. Click the **Previous Page** button at the bottom to the window to return to the Multicast Global Settings window.

e. Click the **Apply** button under Action in The Port Setting of Multicast section of the window.

8. In The Port Setting of Multicast section of the Multicast Global Settings window, check the State of the new multicast VLAN and adjust, if necessary. Possible states are:

   - Enabled: The multicast VLAN is enabled. This is the default setting.
   - Disabled: The multicast VLAN is disabled.

9. To save your changes, refer to “Saving Your Changes” on page 63.

10. To view the details on the multicast VLANs on the switch, refer to “Viewing Multicast VLANs” on page 320.

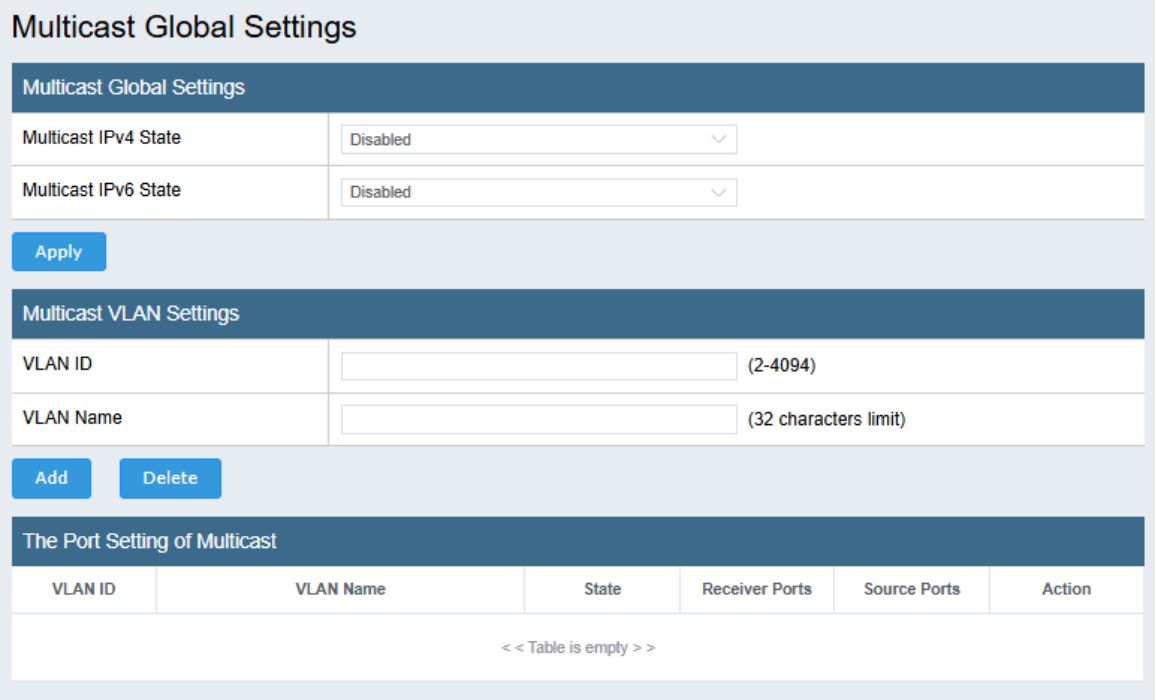


Figure 96. Multicast Global Settings Window

Editing Multicast VLANs

This procedure explains how to edit the following parameters of a multicast VLAN:

- Destination ports
- Source ports
- State (enabled or disabled)

Note
Changing the VLAN ID or name of a multicast VLAN requires deleting and recreating a VLAN.

To edit a multicast VLAN:

1. Select **Network** > **Multicast VLAN** > **Global Settings** from the menu to display the Multicast Global Settings window, shown in Figure 96 on page 317.

2. To change the destination ports of a multicast VLAN, perform the following steps:

    a. Under The Port Setting of Multicast section of the window, click the **Edit** button under **Receiver Ports**. This displays the Receiver Ports Settings window.

    b. Select the tagged and/or untagged ports that will be connected to destination devices of the multicast VLAN by clicking on the corresponding dialog circles under the port numbers. The destination ports can be all ports on the switch, minus the source ports.

    c. Click the **Apply** button at the bottom of the Receiver Ports Settings window to implement your changes.

    d. Click the **Previous Page** button at the bottom to the window to return to the Multicast Global Settings window.

    e. Click the **Apply** button under Action in The Port Setting of Multicast section of the window.

3. To change the source ports of a multicast VLAN, perform these steps:

    a. Under The Port Setting of Multicast section of the window, click the **Edit** button under **Source Ports**. This displays the Source Ports Settings window.

    b. Select the tagged and/or untagged ports that are connected to the source device of the multicast VLAN by clicking on the corresponding dialog circles under the port numbers.

    c. Click the **Apply** button at the bottom of the Receiver Ports Settings window to implement your change.

    d. Click the **Previous Page** button at the bottom of the window to return to the Multicast Global Settings window.

    e. Click the **Apply** button under Action in The Port Setting of Multicast section of the window.

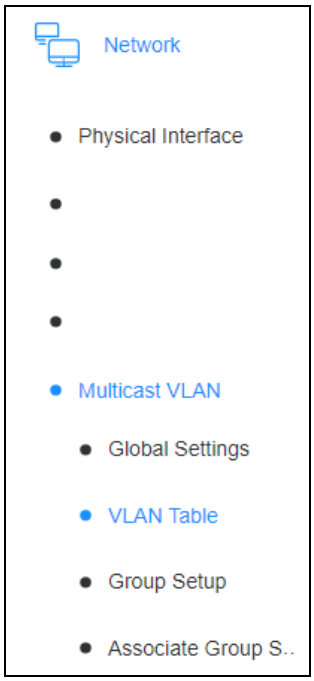
4. In The Port Setting of Multicast section of the Multicast Global Settings window, check the State of the new multicast VLAN and adjust, if necessary. Possible states are:
   - ❒ Enabled: The multicast VLAN is enabled. This is the default setting.
   - ❒ Disabled: The multicast VLAN is disabled.
5. To save your changes, refer to “Saving Your Changes” on page 63.

Deleting Multicast VLANs

To delete multicast VLANs:

1. Select **Network** > **Multicast VLAN** > **Global Settings** from the menu. This displays the Multicast Global Settings window, shown in Figure 96 on page 317.
2. In the Multicast VLAN Settings section of the window, enter in the **VLAN ID** field the VLAN ID of the VLAN to be deleted. You can delete only one VLAN at a time.
3. Click the **Delete** button. The switch deletes the multicast VLAN.
4. To save your changes, refer to “Saving Your Changes” on page 63.

Viewing Multicast VLANs



To view the details of the multicast VLANs on the switch, display the Multicast VLAN Table window by selecting **Network** > **Multicast VLAN** > **VLAN Table** from the menu. An example of the window is shown in Figure 97. The columns in the window are described in Table 72.

Table 72. Multicast VLAN Table Window

Column	Description
VLAN ID	Displays the ID number for the multicast VLAN. The range is 1 to 52. The value must be unique from the ID numbers of the current VLANs on the switch. Review to “Viewing All 802.1Q Tagged VLANs” on page 352.
VLAN Name	Displays the name of the multicast VLAN. Here are the guidelines: - The name can be up to 32 characters. - Spaces are allowed, but not special characters. - The name should be unique from the names of all other VLANs on the switch.
State	Displays whether the multicast VLAN is enabled or disabled.
Tagged Receiver Ports	Lists the switch tagged ports connected to destination devices who may receive the multicast stream.
Untagged Receiver Ports	Lists the switch untagged ports connected to destination devices of clients receiving the multicast stream.
Tagged Source Ports	Lists the switch tagged ports connected to the source device of the multicast stream.
Untagged Source Ports	Lists the switch untagged ports connected to the source device of the multicast stream.

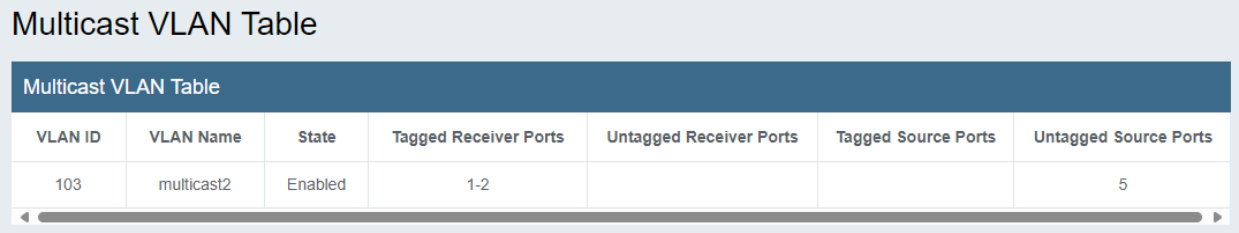


Figure 97. Multicast VLAN Table Window

Managing Multicast Address Profiles

Managing multicast address profiles is the second step to adding support for multicast traffic to the switch. Multicast address profiles define the IPv4 or IPv6 multicast address ranges of the source traffic of multicast VLANs. Here are the procedures:

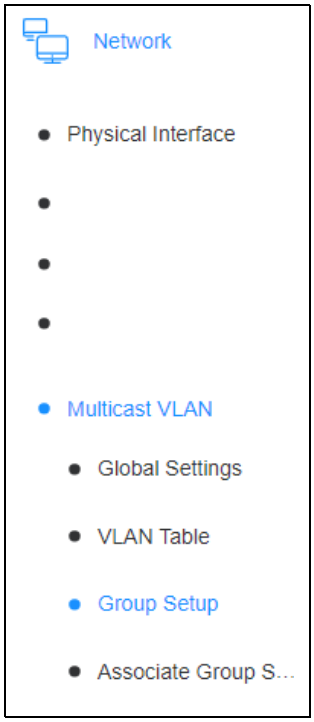
- ❒ “Adding Multicast Address Profiles”
- ❒ “Editing Multicast Profiles”
- ❒ “Deleting Multicast Profiles”

Adding Multicast Address Profiles

This procedure explains how to add multicast address profiles that define the IPv4 or IPv6 multicast address ranges of multicast source traffic. There are two steps:

Step 1: Creating a Profile

Note
You must first assign the new profile a name in the Profile Create section of the window before designating the multicast IP address range.



1. Select **Network** > **Multicast VLAN** > **Group Setup** from the menu. The Multicast Group Setup Window is shown in Figure 98 on page 323.
2. In the Profile Name field in the Profile Create section of the window, enter a name for the new group. The name can contain a maximum of thirty two alphanumeric characters.
3. Click the **Add** button. The name is added to the Multicast Profile Table at the bottom of the window.

Step 2: Designating the Multicast Address Range

1. In the Group Profile Settings section of the window, enter in the Profile Name field the name of an existing profile that is to be assigned an address range. The name is case-sensitive. The names are listed in the Multicast Profile Table in the window.
2. In the IP Address Range of the window, click either the IPv4 or IPv6 dialog circle to indicate the address format of the source multicast traffic. The default is IPv4.
3. In the two IPv4 or IPv6 fields, enter the beginning and ending addresses of the multicast address range. Note the following:

- ❒ An IPv4 multicast address range must be within 224.0.0.0 to 239.255.255.255.
- ❒ An IPv6 multicast cast address range must contain the prefix ff00::/8.

4. Click **Add** The profile is added to the Multicast Profile Table at the bottom of the window.

5. To save your changes, refer to “Saving Your Changes” on page 63.

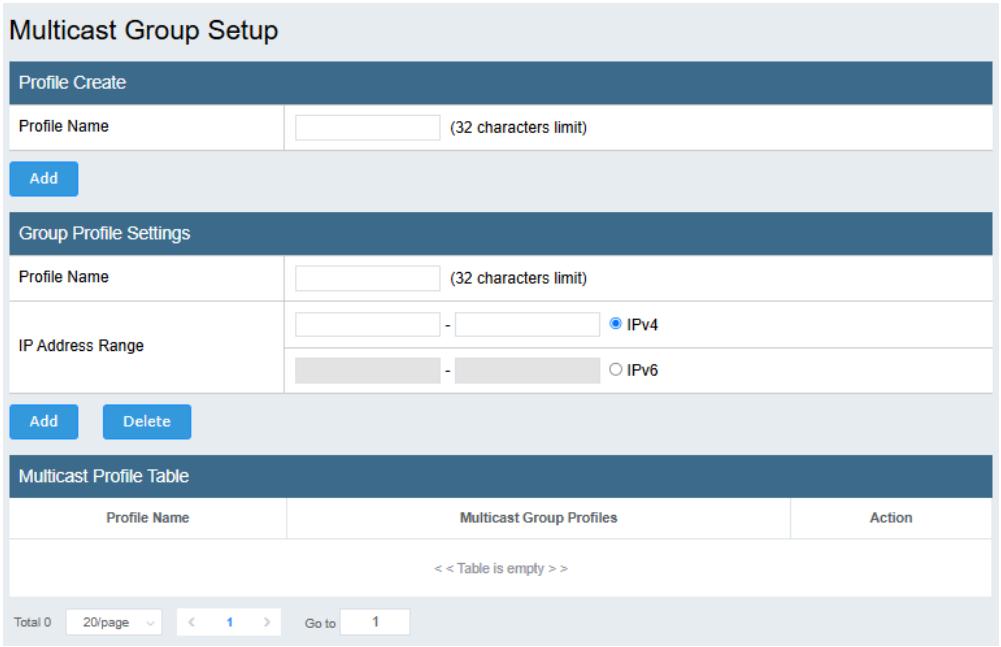


Figure 98. Multicast Group Setup Window

Editing Multicast Profiles

To change the IPv4 or IPv6 address range of a multicast profile:

1. Select **Network** > **Multicast VLAN** > **Group Setup** from the menu. The Multicast Group Setup Window is shown in Figure 98.

2. In the Group Profile Settings section of the window, enter in the Profile Name field the name of the profile you want to change. The name is case-sensitive.

3. In the IP Address Section of the window, click either the IPv4 or IPv6 dialog circle to indicate the address to be changed.

4. In the two IPv4 or IPv6 fields, adjust the beginning and ending addresses of the multicast address range, as needed. Note the following:

   - ❒ An IPv4 multicast address range must be within 224.0.0.0 to 239.255.255.255.

- An IPv6 multicast cast address range must have the prefix ff00::/8.

5. Click the **Add** button. The profile is updated in the Multicast Profile Table at the bottom of the window.

6. To save your changes, refer to “Saving Your Changes” on page 63.

Deleting Multicast Profiles

To delete a multicast profile:

1. Select **Network** > **Multicast VLAN** > **Group Setup** from the menu. The Multicast Group Setup Window is shown in Figure 98.

2. In the Group Profile Settings section of the window, enter in the Profile Name field the name of the profile you want to delete. The name is case-sensitive.

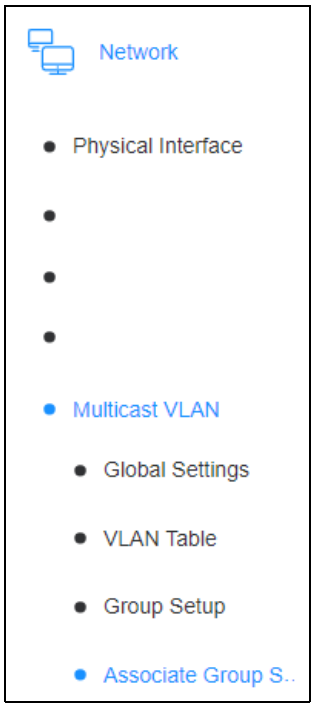
3. Click the **Delete** button. The profile is delete from the Multicast Profile Table at the bottom of the window.

4. To save your changes, refer to “Saving Your Changes” on page 63.

Managing Associations of Multicast VLANs with Multicast Address Profiles

After adding a multicast VLAN with the source and destination ports, and defining the multicast address range in a multicast profile, you may join the two together. This is called associating the VLAN with its profile. Once a multicast VLAN is joined with its profile, the VLAN is complete.

Adding Associations



To associate a multicast VLAN with its multicast address profile:

1. Select **Network** > **Multicast VLAN** > **Associate Group Setup** from the menu. The Multicast Associate Group Setup Window is shown in Figure 99.
2. In the VLAN ID field, enter the ID number of the multicast VLAN that you want to associate with a profile. You can enter only one VLAN ID and the ID must already exist. To view the VLAN ID numbers, refer to “Editing Multicast VLANs” on page 317.
3. In the Profile Name field in the window, enter the name of the multicast address profile you want to associate with the VLAN. You can enter only one profile. The name is case-sensitive.
4. Click the **Add** button. The Multicast Associate Group Table is updated with the new association.

   The multicast VLAN is complete. You may connect the source and destination devices to the ports on the switch and activate the multicast stream on the source device.

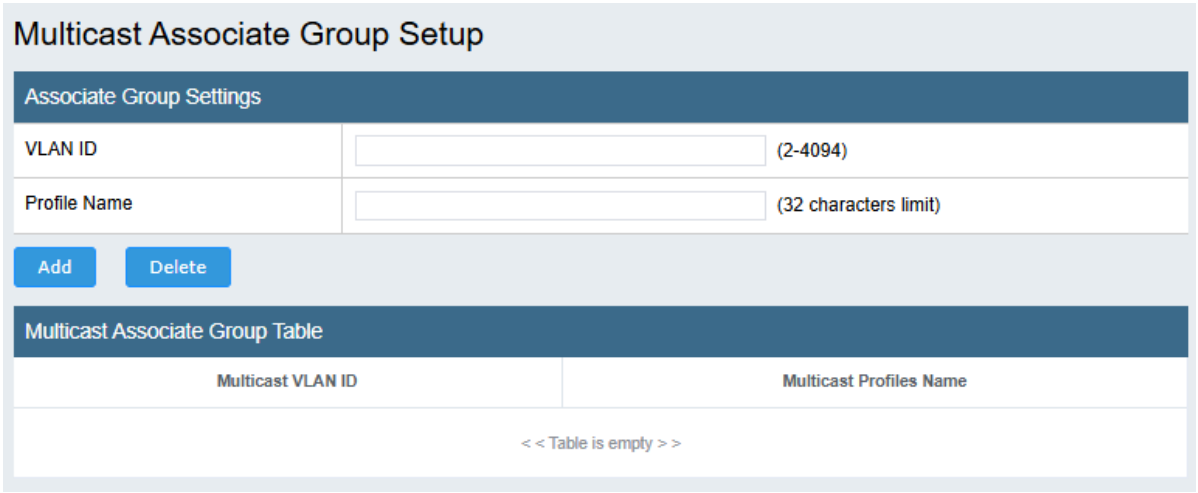


Figure 99. Multicast Associate Group Setup Window

Deleting Associations

To delete associations so as to remove the connection between a multicast VLAN and its multicast address profile:

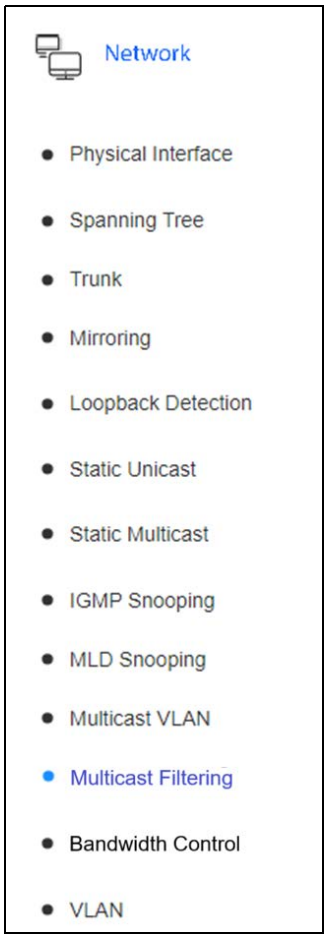
Caution
Deleting an association breaks the link between the multicast VLAN and its profile, thus terminating the multicast stream.

1. Select **Network** > **Multicast VLAN** > **Associate Group Setup** from the menu. The Multicast Associate Group Setup Window is shown in Figure 99.
2. In the **VLAN ID** field, enter the VLAN ID of the association you want to delete.
3. Click the **Delete** button. The association is deleted from the switch. The switch stops forwarding any multicast traffic from the multicast VLAN.

Chapter 32

Multicast Filtering

Description and Procedure



The Multicast Filtering option in the Network menu allows you to block all ingress multicast packets from source devices on ports. When activated on a port, the switch discards all ingress multicast packets on the designated port, but continues to forward egress multicast packets.

To enable or disable ingress multicast filtering on ports:

1. Select **Network** > **Multicast Filtering** from the menu to display the Multicast Filtering window shown in Figure 100.
2. Select the port settings from the Multicast Filter Mode pull-down menus. Refer to Table 73.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 73. Multicast Filtering Window

Action	Description
Forward	The switch forwards all ingress multicast packets on the port.
Filter multicast traffic	The switch blocks all ingress multicast packets on the port.

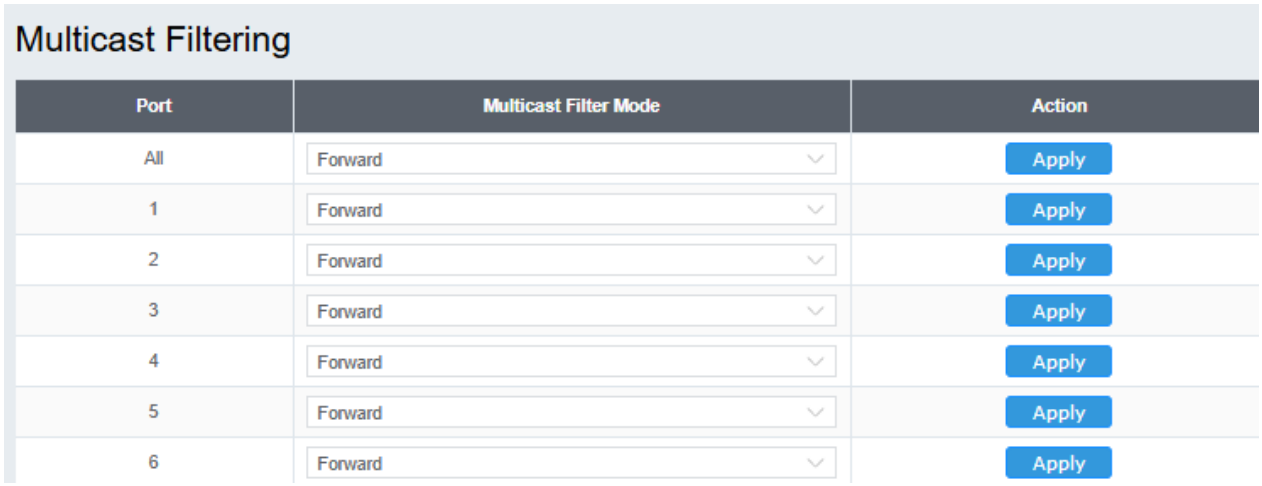


Figure 100. Multicast Filtering Window

Chapter 33
Bandwidth Control

This chapter describes bandwidth control in the following sections:

- “Setting Threshold Limits for Ingress Unknown Unicast, Broadcast, and Multicast Packets” on page 330
- “Setting Ingress Bandwidth Limits” on page 332
- “Setting Egress Traffic Rate Limits” on page 334

Setting Threshold Limits for Ingress Unknown Unicast, Broadcast, and Multicast Packets

You can set maximum threshold limits for the number of ingress packets that ports will accept per second. Ingress packets that exceed the thresholds are discarded by the switch. You can set maximum thresholds for the following types of traffic:

- ❒ Unicast packets (destination lookup failures)
- ❒ Broadcast packets
- ❒ Multicast packets

The feature supports packet sizes from 64 to 16384 bytes. The formula for calculating the bandwidth limit for copper ports is as follows:

Bandwidth = 64pps x increment

The increment is an integer value ranging from 1 to 4096.

To set threshold limits for ingress packets:

1. Select **Network** > **Bandwidth Control** > **Storm Control** from the menu to display the Storm Control window shown in Figure 101 on page 331.
2. Configure the port settings by referring to Table 74.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 74. Storm Control Window

Column	Description
DLF	Select one of the following: - Enabled: Enables storm control for ingress unicast packets. - Disabled: Disables storm control for ingress unicast packets. This is the default setting.

Table 74. Storm Control Window (Continued)

Column	Description
Broadcast	Select one of the following: - Enabled: Enables storm control for ingress broadcast packets. - Disabled: Disables storm control for ingress broadcast packets. This is the default setting.
Multicast	Select one of the following: - Enabled: Enables storm control for ingress multicast packets. - Disabled: Disables storm control for ingress multicast packets. This is the default setting.
Threshold	Enter the increment used to calculate the threshold value. Here are guidelines: - Thresholds are calculated by multiplying 64 packets per second (pps) by the increment. For example, an increment of 1 results in a threshold of 64pps, an increment of 2 results in a threshold of 128pps, and so on. - The increment range is 1 to 4096. - A port has to have at least one enabled filter for you to set the threshold.

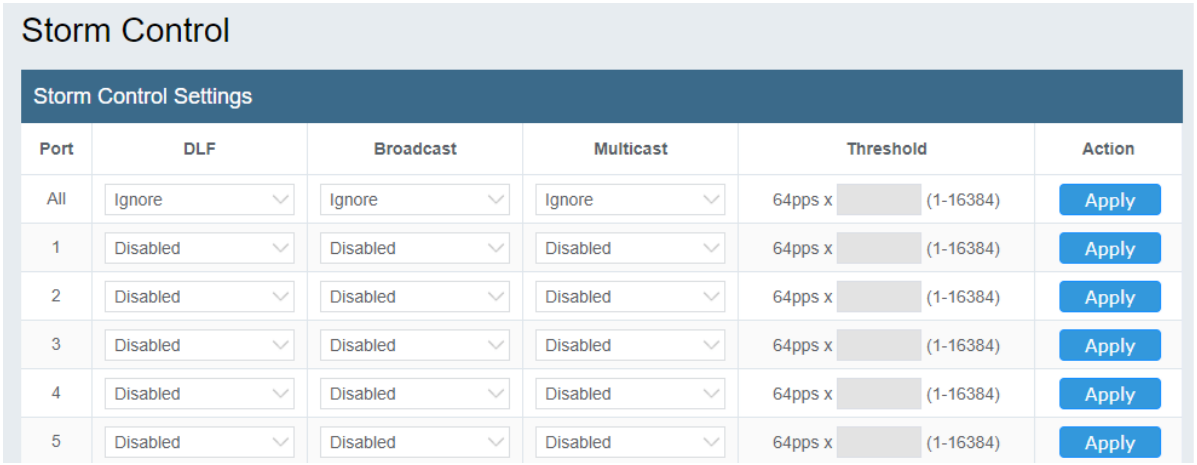
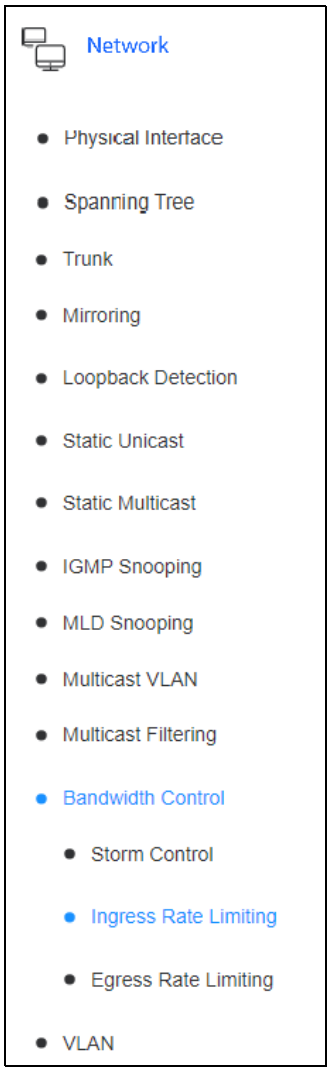


Figure 101. Storm Control Window

Setting Ingress Bandwidth Limits



This section explains how to set ingress bandwidth limits on the individual switch ports. The ports discard ingress traffic from their network counterparts that exceed the bandwidth limits. You might use the feature to protect the port ingress queues from being overwhelmed or saturated during periods of heavy traffic from other network devices.

The traffic is defined as kilobits per second (Kbps). The range is from 64Kbps to 1000M, in increments of 64Kbps. The formula for calculating the bandwidth limit for 10/100/1000Base-T ports is as follows:

- Bandwidth = 64Kbps x increment
- The increment is an integer ranging from 1 to 15625.

To configure ingress bandwidth limits on the ports:

1. Select **Network** > **Bandwidth Control** > **Ingress Rate Limiting** from the menu. The Ingress Rate Limiting window is shown on Figure 102 on page 333.
2. Configure the settings for the individual ports by referring to Table 75.

Table 75. Ingress Rate Limiting Window

Column	Description
Bandwidth	Enter the increment for calculating the bandwidth value. Here are guidelines: - Thresholds are calculated by multiplying 64 kilobits per second (Kbps) by the increment. For example, an increment of 1 results in a threshold of 64Kbps, an increment of 2 results in a bandwidth threshold of 128Kbps, and so on. - You have to enable the bandwidth on a port to set its threshold increment. - The increment range is 1 to 15625. - Ports can have different thresholds.
Status	Select one of the following: - Enabled: Enables bandwidth threshold on the port. - Disabled: Disables bandwidth threshold on the port. This is the default setting.
Action	Click **Apply** to activate your change.

Note
Select **Save** from the menu to save your changes.

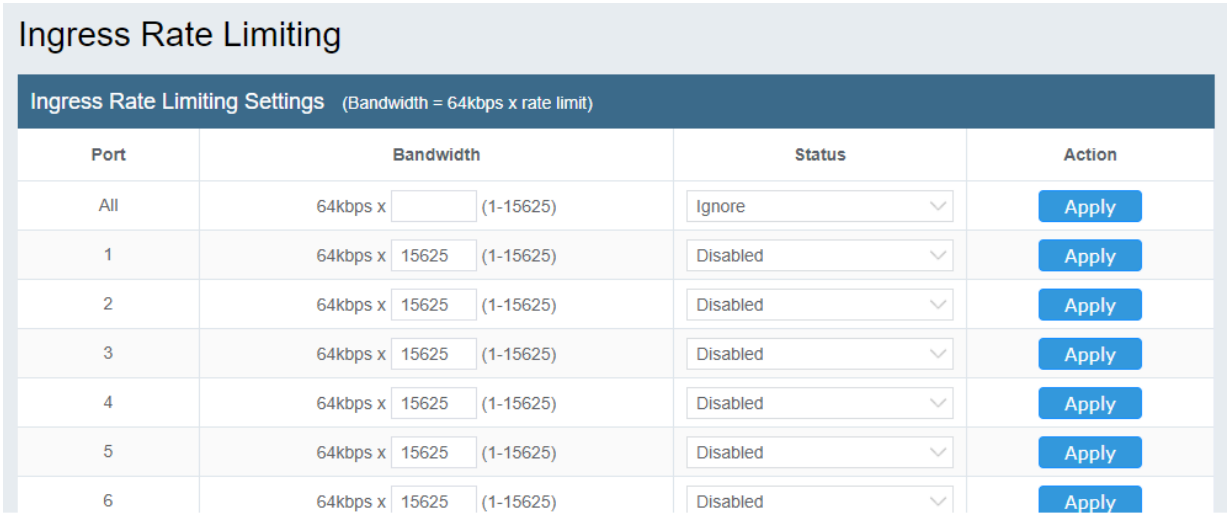
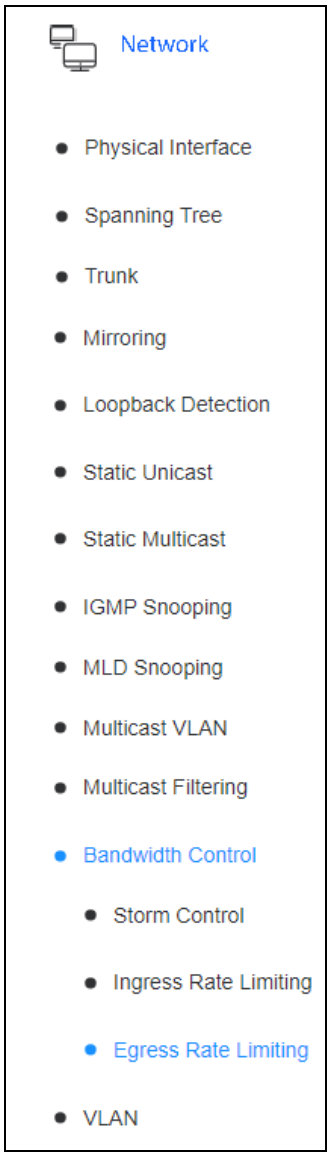


Figure 102. Ingress Rate Limiting Window

Setting Egress Traffic Rate Limits



This section explains how to set limits on the egress traffic that ports transmit to their local or remote network counterparts. The feature can prevent switch ports from overwhelming their network counterparts during periods of heavy traffic.

The traffic is defined as kilobits per second (Kbps). The range is from 64Kbps to 1000M, in increments of 64Kbps. The formula for calculating the bandwidth limit for 10/100/1000Base-T ports is as follows:

- Bandwidth = 64Kbps x increment
- The increment is an integer ranging from 1 to 15625.

To configure egress traffic rate limits on the ports:

1. Select **Network** > **Bandwidth Control** > **Egress Rate Limiting** from the menu. The Egress Rate Limiting window is shown in Figure 103 on page 335.
2. Configure the settings for the individual ports by referring to Table 76.

Table 76. Egress Rate Limiting Window

Column	Description
Bandwidth	Enter the increment for calculating the bandwidth value. Here are guidelines: - Thresholds are calculated by multiplying 64 kilobits per second (Kbps) by the increment. For example, an increment of 1 results in an egress bandwidth threshold of 64Kbps, an increment of 2 results in an egress bandwidth threshold of 128Kbps, and so on. - You have to enable the bandwidth on a port to set its threshold increment. - The increment range is 1 to 15625. - Ports can have different thresholds.
Status	Select one of the following: - Enabled: Enables egress bandwidth threshold on the port. - Disabled: Disables egress bandwidth threshold on the port. This is the default setting.
Action	Click **Apply** to activate your change.

Note
Select **Save** from the menu to save your changes.

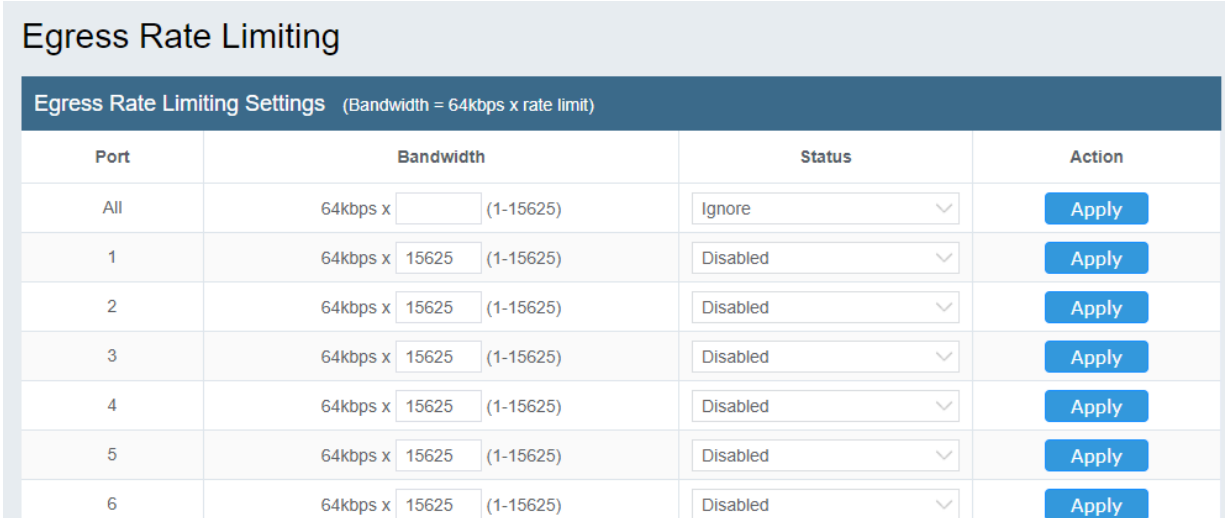


Figure 103. Egress Rate Limiting Window

Chapter 34

802.1Q Tagged Virtual LANs

This chapter describes 802.1Q Tagged VLANs in the following sections:

- ❒ “802.1Q Tagged VLAN Overview” on page 338
- ❒ “Adding or Viewing 802.1Q Tagged VLANs” on page 344
- ❒ “Configuring PVIDs and Filters for Tagged and Untagged Ports” on page 348
- ❒ “Modifying 802.1Q Tagged VLANs” on page 350
- ❒ “Deleting 802.1Q Tagged VLANs” on page 351
- ❒ “Viewing All 802.1Q Tagged VLANs” on page 352

802.1Q Tagged VLAN Overview

A VLAN consists of a group of ports that form an independent traffic domain on an Ethernet switch. The ports of a VLAN forward ingress traffic only to those ports that are part of the same VLAN. An interconnection device, such as a router or Layer 3 switch, is commonly added to permit traffic between different VLANs.

The switch supports several types of VLANs. This chapter describes 802.1Q Tagged VLANs. Tagged VLANs commonly consist of two types of switch ports: tagged and untagged.

Tagged Ports

Tagged ports are connected to network devices that support 802.1Q tagged packets. Tagged packets contain in the headers, following the source and destination addresses, the VLAN identifiers (VIDs) of the virtual LANs to which the frames belong (IEEE 802.3ac standard). When the switch receives frames with VLAN tags, referred to as tagged frames, on tagged ports, it forwards them only to those ports that share the same VID.

Network devices connected to tagged ports should be IEEE 802.1Q compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

The benefit of tagged ports is that they can belong to more than one VLAN at one time, which can simplify the task of adding shared devices to the network. For example, an 802.1Q-compliant server connected to a tagged port on the switch can be configured to accept and return packets from different VLANs, simultaneously.

Tagged VLANs are also useful where multiple VLANs span across switches. You can use one port per switch to connect the different parts of VLANs together.

The IEEE 802.1Q standard describes how this tagging information is used to forward the traffic throughout the switch. The handling of frames tagged with VIDs coming into a port is straightforward. If the incoming frame's VID tag matches one of the VIDs of a VLAN of which the port is a tagged member, the frame is accepted and forwarded to the appropriate ports. If the frame's VID does not match any of the VLANs in which the port is a member, the frame is discarded.

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

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

Untagged Ports

Untagged ports in Tagged VLANs are for network devices that do not support 802.1Q tagged packets. The packets they transmit and receive do not contain VIDs in the headers. VLAN memberships of untagged ports are controlled by port VLAN identifiers (PVIDs). These are values that you assign to the individual switch ports to identify which VLANs the ports, and the devices connected to the ports, belong to. Ports can have only one PVID.

The PVIDs of untagged ports should match the VID of their Tagged VLANs. For example, the untagged ports of a Tagged VLAN with the VID 56 should be assigned the PVID 56. Refer to “Configuring PVIDs and Filters for Tagged and Untagged Ports” on page 348.

802.1Q Tagged VLAN Components

The components of Tagged VLANs are described Table 77.

Table 77. Components of 802.1Q Tagged VLANs

Item	Description
VLAN Identifier	A tagged VLAN has to have a unique identification number (VID). The VID has to match the VID in the tagged packets transmitted by the 802.1Q-compliant network devices in the VLAN. Tagged VLANs that span multiple switches should be assigned the same VID on each switch. The range is 2 to 4093. The VID 1 is reserved for the default Tagged VLAN.
Name	A tagged VLAN has to have a name. VLANs will be easier to identify if you give them names that reflect the functions of the member devices, such as Sales, Production, or Engineering.

Table 77. Components of 802.1Q Tagged VLANs (Continued)

Item	Description
Tagged Ports	A tagged VLAN will have one or more tagged ports. These are ports that are connected to 802.1Q-compliant network devices that transmit tagged packets containing the VIDs that identify their VLAN memberships. Here are the guidelines: - A tagged VLAN can have any number of tagged ports, up to all the ports on the switch. - Tagged ports can belong to more than one tagged VLAN at a time. - Tagged ports cannot also be members of other types of VLANs, such as voice or private VLANs.
Untagged Ports	A tagged VLAN can have one or more untagged ports. These are ports that are connected to network devices that do not support 802.1Q tagged packets. VLAN memberships of untagged ports are identified by the PVIDs assigned to the individual ports. Here are the guidelines: - A tagged VLAN can have any number of untagged ports. - Untagged ports can belong to only one VLAN at a time. - Untagged ports should be assigned PVIDs that match the VIDs of their tagged VLANs. For example, untagged ports in a tagged VLAN with the VID 11 should be assigned the PVID 11. Refer to “Configuring PVIDs and Filters for Tagged and Untagged Ports” on page 348.
VLAN Mode	The VLAN mode identifies the ports as members of tagged VLANs.
PVID	PVIDs mainly apply to untagged ports. They identify the VLAN memberships of the untagged packets that arrive on untagged ports. However, PVIDs are applicable on tagged ports as well. As explained earlier, VLAN membership on tagged ports is typically controlled by the tag information in the header portion of the ingress frames themselves. But tagged ports do use PVIDs for any ingress untagged packets they might receive.

Guidelines to Adding Tagged VLANs

Here are the guidelines to adding tagged VLANs.

- Tagged VLANs can contain both tagged and untagged ports.
- Network devices connected to tagged ports must support 802.1Q tagged packets.
- A tagged VLAN needs to have a unique VID. If a VLAN spans multiple switches, you should assign the same VID to the various parts of the VLAN on the different switches.
- Tagged ports can be members of more than one tagged VLAN at a time.
- Untagged ports can be untagged members of only one VLAN at a time.
- You have to assign PVIDs to the untagged ports that match the VLAN's identifier. For example, untagged ports in the VLAN with the VID45 should be assigned PVID 45. Refer to "Configuring PVIDs and Filters for Tagged and Untagged Ports" on page 348.
- You should also assign PVIDs to tagged ports. The PVIDs will identify the VLAN memberships of any ingress untagged packets on tagged ports.

Tagged VLAN Example

Figure 104 illustrates how tagged ports can be used to interconnect IEEE 802.1Q-based products.

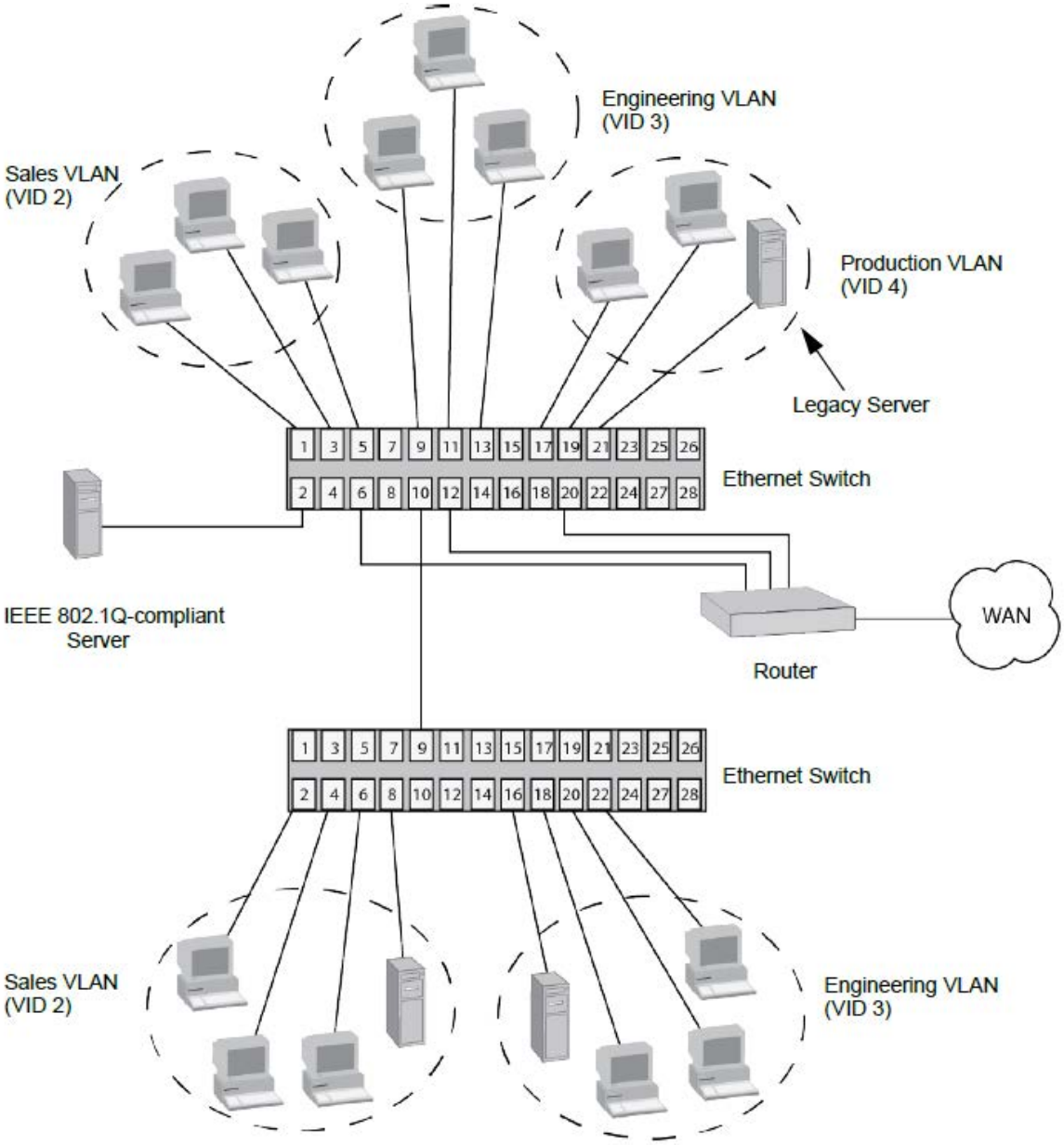


Figure 104. Example of a Tagged VLAN

The port assignments of the VLANs are described in Table 78.

Table 78. Example of Tagged VLANs

	Sales VLAN (VID 2)		**Engineering VLAN (VID 3)**		**Production VLAN (VID 4)**	
	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports	Untagged Ports	Tagged Ports
Top Ethernet Switch	1, 3 to 5 (PVID 2)	2, 10	9, 11 to 13 (PVID 3)	2, 10	17, 19 to 21 (PVID 4)	2
Bottom Ethernet Switch	2, 4, 6, 8 (PVID 2)	9	16, 18, 20, 22 (PVID 3)	9	none	none

The switches employ tagged ports to simplify network implementation and management. One of the tagged ports is port 2 on the top switch. It is a tagged member of the three VLANs. It is connected to an IEEE 802.1Q-compliant server, meaning the server can handle frames from multiple VLANs. The port makes it possible for the three VLANs to access the server without going through a router or other interconnection device. It is important to note that even though the server is accepting frames from and transmitting frames to more than one VLAN, data separation and security remain.

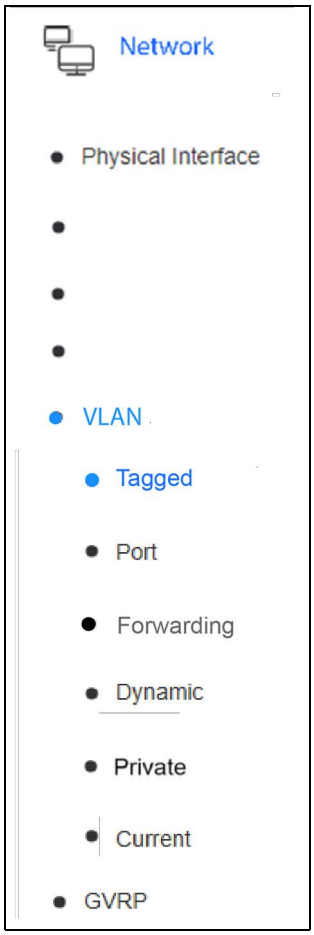
Two other tagged ports are used to simplify network design in the example. They are port 10 on the top switch and port 9 on the lower switch. These ports are tagged members of the Sales and Engineering VLANs so that they can carry traffic from both VLANs, simultaneously. They provide a common connection that enables different parts of the same VLAN to communicate with each other while maintaining data separation between the VLANs.

Adding or Viewing 802.1Q Tagged VLANs

This section contains the procedure for adding or viewing 802.1Q Tagged VLANs on the switch. Here are the basic steps to adding Tagged VLANs:

1. Add the VLAN by defining its name, VID, and tagged and untagged ports. The procedure is explained in this section.
2. Set the PVIDs of the untagged ports to match the VID of the VLAN. Refer to “Configuring PVIDs and Filters for Tagged and Untagged Ports” on page 348.
3. Set the PVID on tagged ports to control the VLAN assignment of ingress untagged packets.

This section contains the first step to adding 802.1Q Tagged VLANs to the switch. A new Tagged VLAN requires the following information:



- ❒ VID number
- ❒ Name
- ❒ Tagged ports
- ❒ Untagged ports

To add a new 802.1Q Tagged VLAN:

1. Select **Network** > **VLAN** > **Tagged** from the menu. The Tagged VLAN window is shown in Figure 105 on page 347.

   The table at the bottom of the window lists the current 802.1Q Tagged VLANs on the switch. However, the table does not include the VLAN ports. For that, refer to “Viewing All 802.1Q Tagged VLANs” on page 352. The switch comes with one default Tagged VLAN, with the VLAN ID 1. You cannot delete it or change its VID.

2. Configure the fields in Table 79 on page 345 and click **Apply** to add the new VLAN to the switch.

   Note
   Select **Save** from the menu to save your changes.

3. After adding a new VLAN, set the PVIDs of the tagged and untagged ports to match the VID of the VLAN. Refer to “Configuring PVIDs and Filters for Tagged and Untagged Ports” on page 348.

Table 79. Tagged VLAN Window

Field	Description
VLAN ID	Enter a VLAN ID. The guidelines are listed here: - A VLAN can have only one VID. - The VID has to be unique from all other Tagged VLANs on the switch. - The range is 2 to 4094. - VID 1 is reserved for the default Tagged VLAN. - A tagged VLAN that spans more than one switch should be assigned the same VID on all the switches.
VLAN Name	Enter a name for the VLAN. The guidelines are listed here: - The name can be up to 32 characters. - Spaces are allowed, but not special characters. - The name should be unique from the names of all other VLANs on the switch. - A VLAN that spans more than one switch should be given the same name on all the switches.
Static Tagged	Click the radio buttons of ports that are to be tagged members of the VLAN. Ports can be tagged members of more than one tagged VLAN at a time. The devices connected to these ports should be 802.1Q-compliant. Refer to “Tagged Ports” on page 338.
Static Untagged	Click the radio buttons of ports that are to be untagged members of the VLAN. Untagged ports can be members of only one VLAN at a time. These ports should be connected to network devices that do not supported tagged packets and 802.1Q. Refer to “Untagged Ports” on page 339.
Not Member	Click the radio buttons of ports that are not to be members of the VLAN. This is the default port setting. These ports are members of the Default 802.1Q Tagged VLAN or other VLANs.

The window buttons are described in Table 80.

Table 80. Tagged VLAN Window Buttons

Button	Description
All	Clicking the All button in the Static Tagged section designates all ports as static tagged. Clicking the All button in the Static Untagged section designates all ports as static untagged. Clicking the All button in the Not Member section removes all ports from the VLAN. This is the default.
Apply	Activates your changes on the switch.
Clear	Discards your current changes.
Reset to Default	Removes all static tagged and untagged ports from the VLAN.

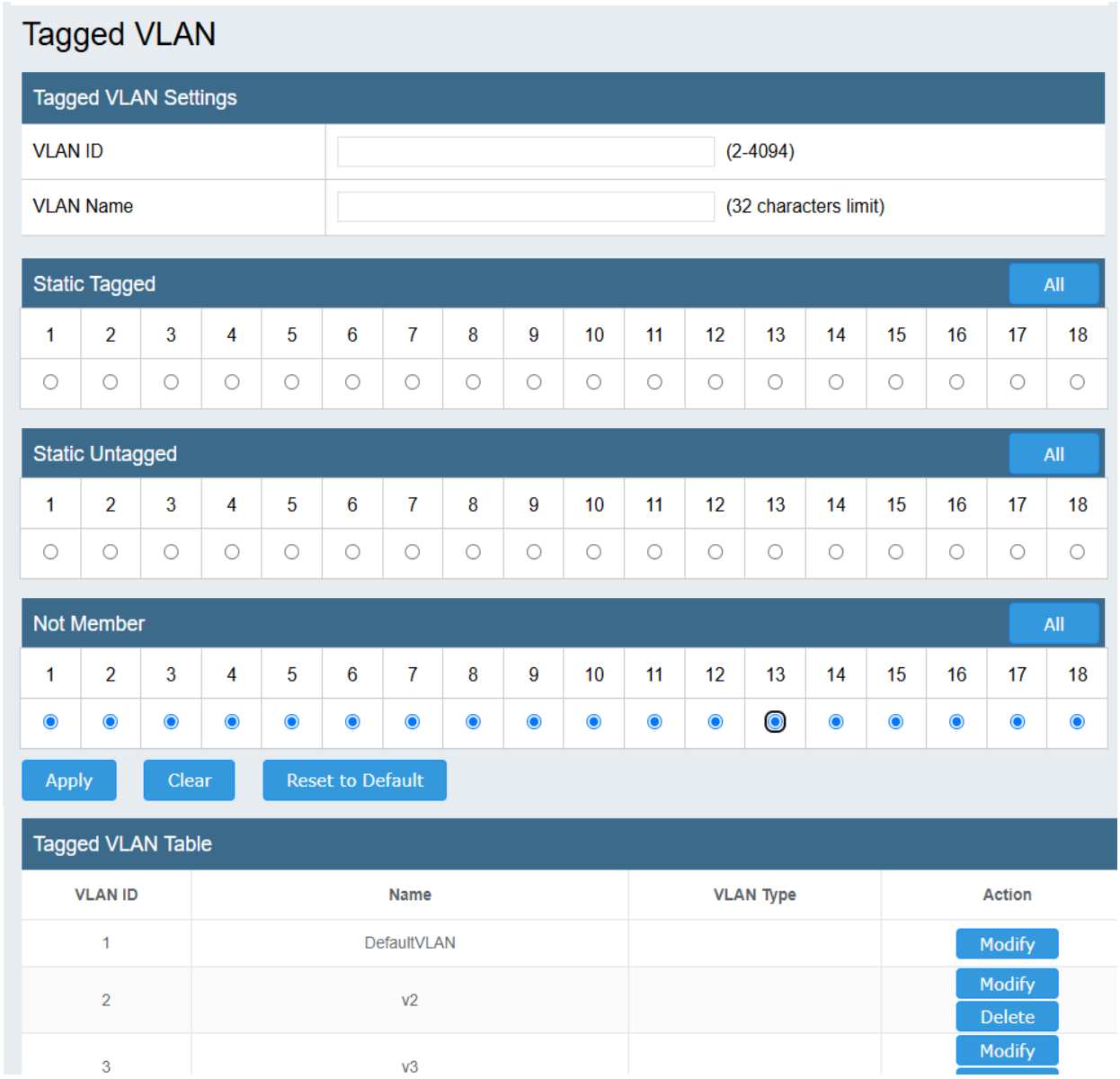
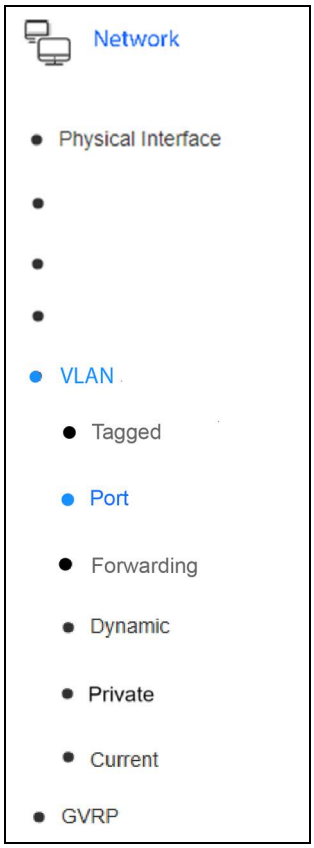


Figure 105. Tagged VLAN Window

Configuring PVIDs and Filters for Tagged and Untagged Ports



This section explains how to set the PVIDs on tagged and untagged ports in 802.1Q Tagged VLANs. The switch uses PVIDs to identify the VLAN memberships of ingress untagged packets on the ports. For background information, refer to “802.1Q Tagged VLAN Components” on page 339.

This section also explains how to set packet filters for tagged or untagged packets and enable or disable destination MAC address filtering.

Note
This procedure does not apply to private or voice VLANs.

To set port PVID and filters:

1. Select **Network** > **VLAN** > **Port** from the menu. The Port Settings window is shown in Figure 106 on page 349.
2. Configure the fields for each port. Refer to Table 81.
3. Click **Apply**.

Note
Select **Save** in the menu to save your changes.

Table 81. Port Settings Window

Field	Description
PVID	Enter a PVID value for the port. Here are the guidelines: - Ports can have only one PVID. - PVIDs of untagged ports should be the same as the VIDs of their VLANs. For example, untagged ports in an 802.1Q Tagged VLAN with the VID 87 should be assigned PVID 87. - PVIDs of tagged ports should designate which VLAN will handle ingress untagged packets. - The default is PVID 1. Refer to “802.1Q Tagged VLAN Components” on page 339.

Table 81. Port Settings Window (Continued)

Field	Description
Acceptable Frame Types	Select one of the following from the menu: - **All**: The port accepts all ingress packets. This is the default. - **Tagged**: The port accepts only tagged packets and discards untagged packets. - **Untagged and Priority Tagged**: The port accepts untagged packets and priority tagged packets, and discards all other tagged packets.
Ingress Filtering	Select one of the following from the menu: - **Enabled**: Enables destination MAC address ingress filtering on the port. Refer to Chapter 49, “Destination MAC Address Filters” on page 483. This is the default setting. - **Disabled**: Disables ingress filtering on the port.

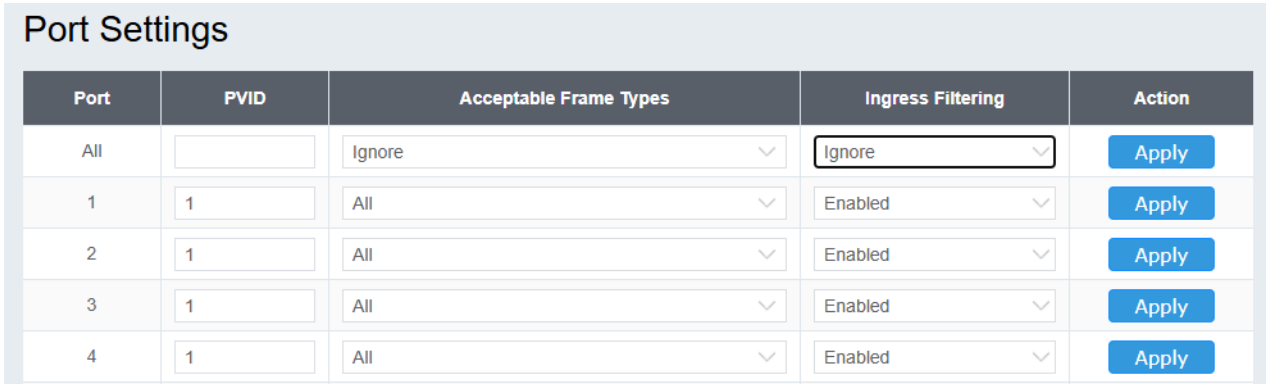
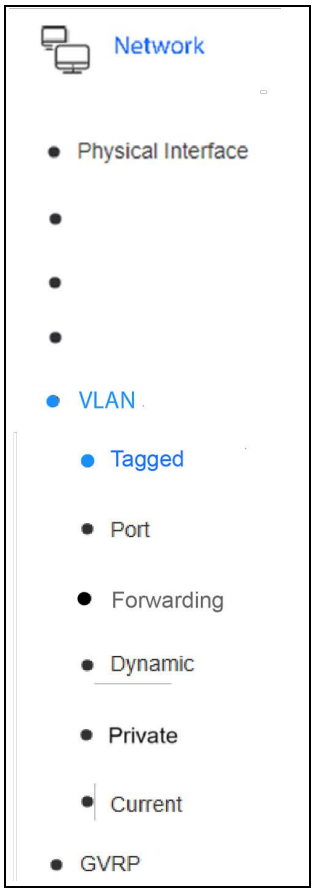


Figure 106. Port Settings Window

Modifying 802.1Q Tagged VLANs



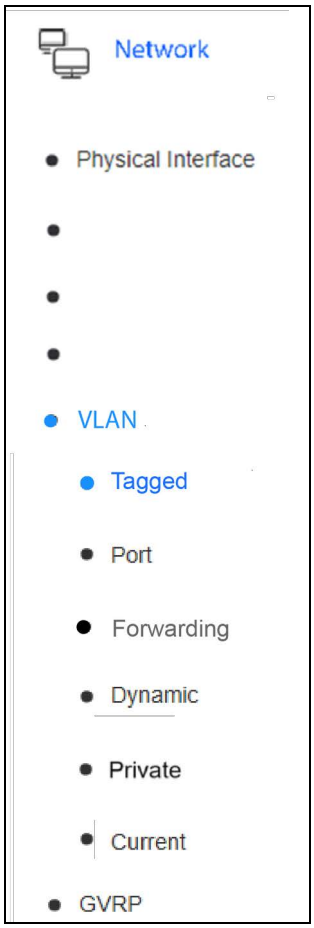
Perform the following procedure to modify 802.1Q Tagged VLANs:

1. Select **Network** > **VLAN** > **Tagged** from the menu. An example of the Tagged VLAN window is shown in Figure 105 on page 347.
2. In the **VLAN Action** column of the table, click **Modify** of the VLAN you want to modify. You can modify only one VLAN at a time.

   The current settings of the VLAN are displayed in the Modify VLAN window.
3. Modify the VLAN settings by referring to Table 79 on page 345. Review the following:
   - ❒ You cannot change the VID. Changing the VID requires deleting a VLAN and adding It again with the new VID.
   - ❒ Untagged ports removed from a VLAN are automatically returned to the Default VLAN.
   - ❒ Tagged ports removed from a VLAN retain their other VLAN assignments.
4. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Deleting 802.1Q Tagged VLANs



Here are the guidelines to deleting 802.1Q Tagged VLANs from the switch:

- ❒ You cannot delete the Default VLAN with the VID 1.
- ❒ Untagged ports of deleted VLANs are automatically returned to the Default VLAN.
- ❒ Tagged ports of deleted VLANs retain their current tag.

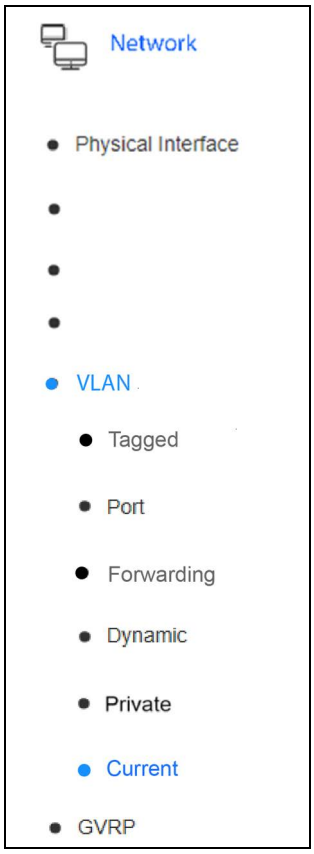
To delete 802.1Q Tagged VLANs:

1. Select **Network** > **VLAN** > **Tagged** from the menu. An example of the Tagged VLAN window is shown in Figure 105 on page 347.
2. In the **VLAN Action** column of the table, click **Delete** of the VLAN to delete. You can delete only one VLAN at a time.

   The switch displays a confirmation prompt.
3. Click **OK** to delete the VLAN or **Cancel** to cancel the deletion.

Note
Select **Save** in the main menu to save your changes.

Viewing All 802.1Q Tagged VLANs



To view all 802.1Q Tagged VLANs on the switch in one window, select **Network** > **VLAN** > **Current** from the menu to display the VLAN Current Database window. Refer to Figure 107 for an example. The columns are defined in Table 82.

Table 82. VLAN Current Database Window

Column	Description
802.1Q Tagged VLAN	
VLAN ID	Displays the VLAN identification number.
VLAN Name	Displays the VLAN name.
VLAN FDB ID	Displays the VLAN FDB identification number.
Member Ports	Displays the tagged and untagged ports of the VLAN.
Untagged Ports	Displays only the untagged ports.
Status	Permanent (static) or dynamic.

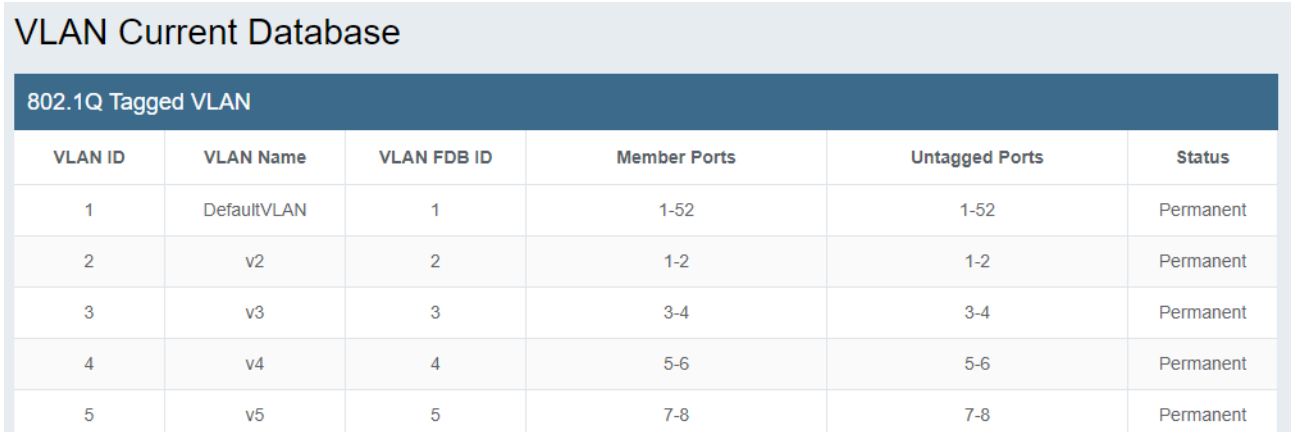


Figure 107. VLAN Current Database Window

Chapter 35

Private Virtual LAN

This chapter describes the private VLAN in the following sections:

- “Private VLAN Overview” on page 354
- “Configuring the Private VLAN” on page 355
- “Disabling the Private VLAN” on page 357

Private VLAN Overview

The private VLAN creates a special broadcast domain on the switch in which the traffic of its member ports are restricted to a single source port. Ports in the VLAN are only allowed to forward traffic to and receive traffic from the designated source port, and are prohibited from forwarding traffic to each other.

An example application of the private port VLAN would be user booths in a library. The private VLAN could enable the computers in the booths to access the Internet or a library server through the source port, but would block communications between the computers.

Another application for the private port VLAN is to simplify IP address assignments. Ports can be isolated from each other while still belonging to the same subnet.

The switch supports only one private VLAN, The switch can support private and tagged VLANs simultaneously.

Source Port

The private VLAN has one source port. The switch permits the other ports in the VLAN to forward traffic only to the source port, and not to each other. Here are the source port guidelines:

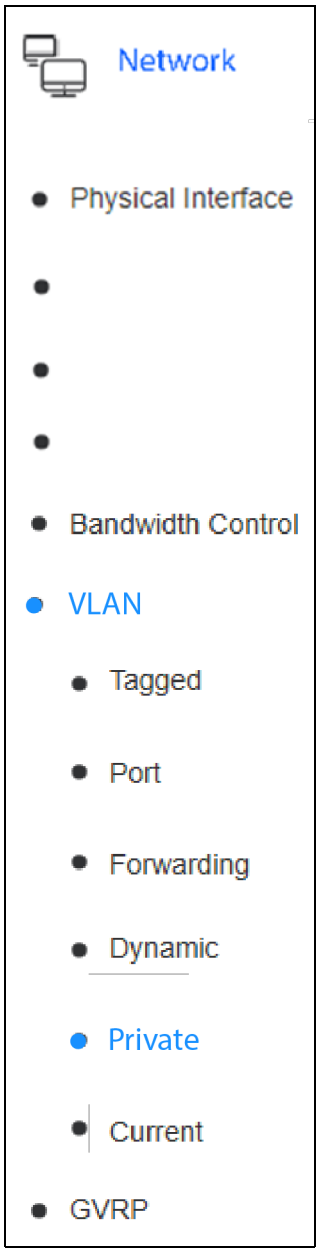
- The private VLAN can have only one source port.
- The source port can be any port on the switch.
- It cannot be a member of a static or LACP trunk.
- It cannot be a member of another VLAN.
- It is an untagged VID port and should be connected to a device that sends untagged packets.

Forwarding Ports

The other ports of the private VLAN are referred to as forwarding ports. The switch allows them to forward traffic only to the source port. Here are the guidelines:

- The private VLAN can have any number of forwarding ports, up to all the switch ports minus the source port.
- They cannot be members of static or LACP trunks.
- They cannot be members of other VLANs.
- They are untagged ports. They should be connected to devices that send untagged packets. To set the PVID, refer to “Configuring PVIDs and Filters for Tagged and Untagged Ports” on page 348.

Configuring the Private VLAN



To configure the private VLAN:

1. Select **Network** > **VLAN** > **Private** from the menu. The Private VLAN window is shown in Figure 108 on page 356.
2. Select **Enabled** from Private VLAN Status and click **Apply**. You must enable the feature to configure it. If the feature is enabled without any changes, port 1 is designated as the source port and all other ports are forwarding ports of the private VLAN.
3. Configure the private VLAN parameters and click **Apply**. Refer to Table 83.

Note
Select **Save** from the menu to save your changes.

Table 83. Private VLAN Window

Parameter	Description
Private VLAN Setting	
Private VLAN Status	Select one of the following from the pull-down menu and click **Apply**. - **Enabled**: Activates the private VLAN. You have to enable the VLAN to configure the settings. - **Disabled**: Disables the private VLAN. This is the default setting.
Port Select	
Source Port	Select the source port for the private VLAN from the pull-down menu. You can select only one source port. The default is port 1.
Forwarding Ports	
	Designate the forwarding ports of the VLAN by clicking the check boxes and click **Apply**. Here are the guidelines: - Ports with check marks are forwarding ports of the private VLAN. - The default is all ports are forwarding ports, except for the source port. - The source port cannot be a forwarding port.

Table 83. Private VLAN Window (Continued)

Parameter	Description
Port List	Lists the ports on the switch and indicates whether they are members of the private VLAN. The columns in the table are defined here: - Port: Lists the ports on the switch. - Port Map: If the private VLAN is disabled, this column lists all ports. - Indicates the source and forwarding ports of the private VLAN. The source port is listed first, followed by a comma and the forwarding ports. For example, if port 2 is the source port, and ports 6 to 13 are forwarding ports, the port map would be 2,6-13. - This column is empty for ports that are not members of the private VLAN.

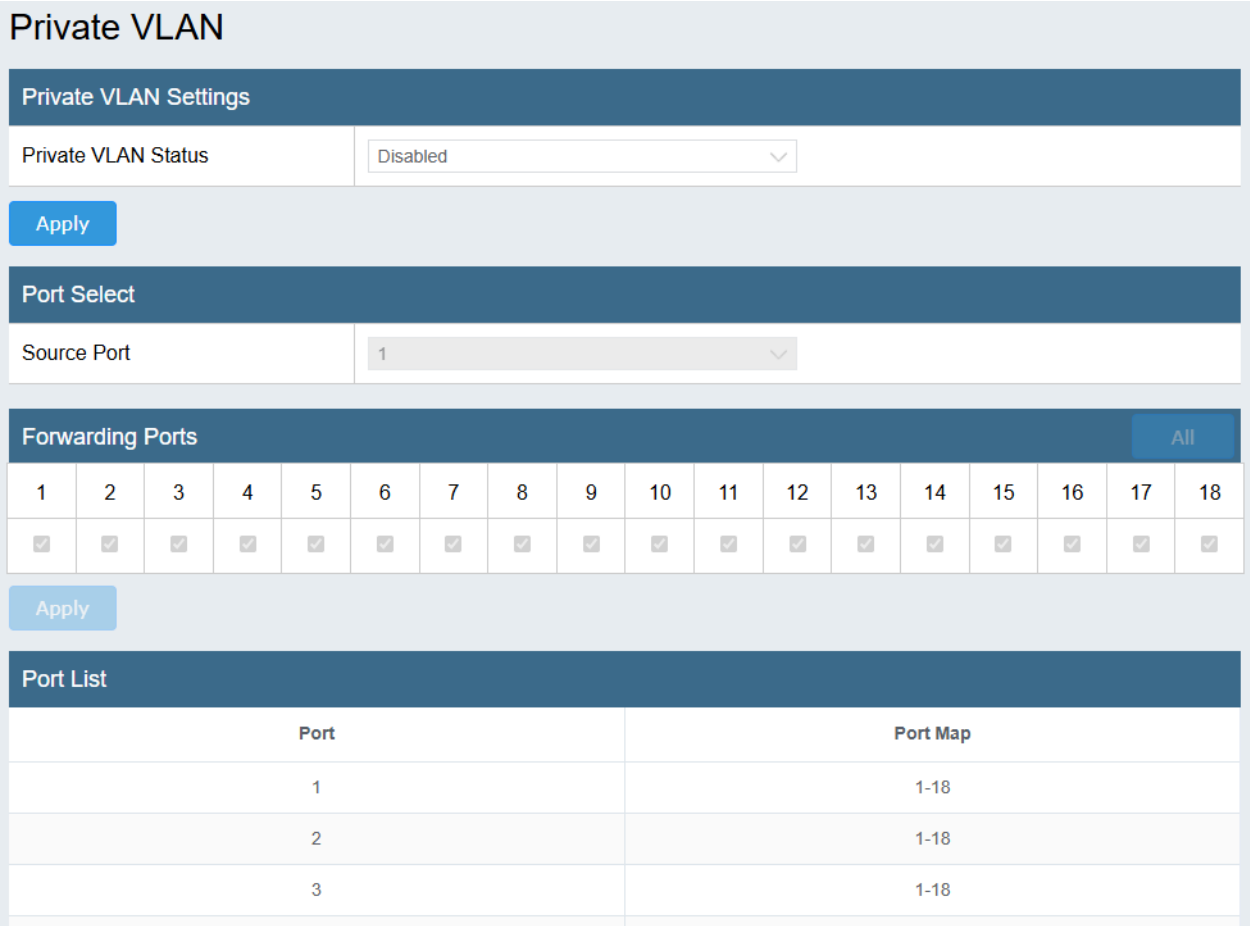
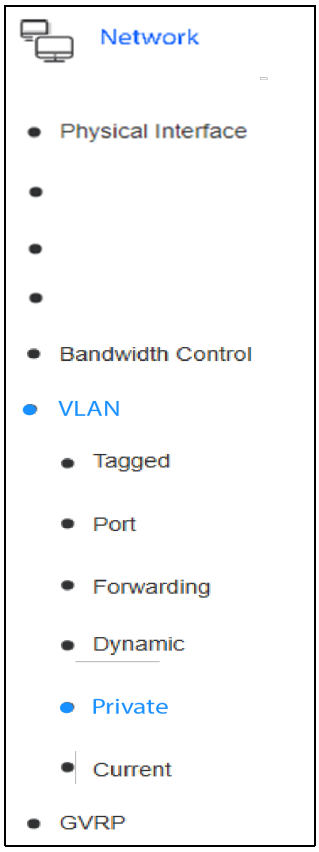


Figure 108. Private VLAN Window

Disabling the Private VLAN



To disable the private VLAN:

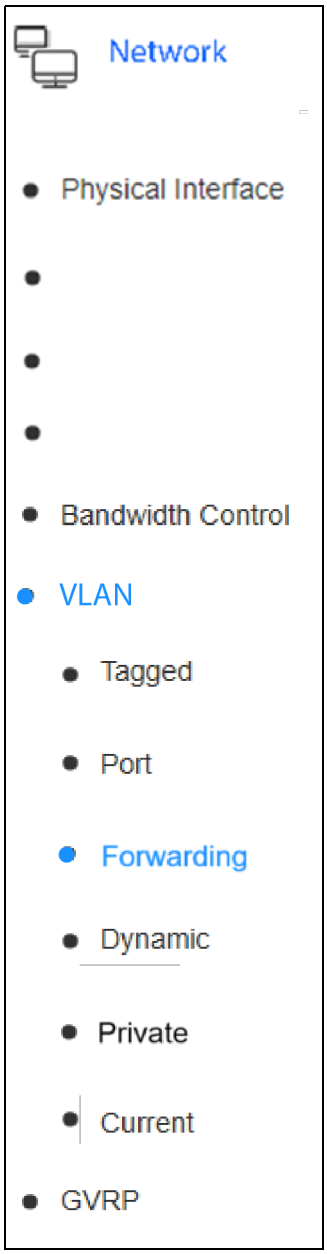
1. Select **Network** > **VLAN** > **Private** from the menu. The Private VLAN window is shown in Figure 108 on page 356.
2. Select **Disabled** from Private VLAN Status and click **Apply** to activate your change.

Note
Select **Save** from the menu to save your change.

Chapter 36

VLAN Forwarding Modes

Description and Procedure



The switch supports the following VLAN forwarding modes:

- Standard 802.1Q VLAN Mode (IVL) - This is the default mode and the recommended mode.
- Asymmetric VLAN Mode (SVL) - This mode permits the formation of overlapping untagged VLAN ports to form VLAN groups.

Changing the VLAN mode clears the entries from these tables:

- Forwarding database (FDB) table
- Static unicast address table
- Static multicast address table
- 802.1x authentication records table
- IGMP snooping multicast group table

Here are the SVL guidelines:

- Voice VLAN is not supported.
- The VID field in 802.1Q VLAN mode is displayed as “N/A”.

To change the VLAN forwarding table mode on the switch:

1. Select **Network** > **VLAN** > **Forwarding** from the menu to display the Forwarding Table Mode Settings window. Refer to Figure 109.
2. From the Learning Mode pull-down menu, select one of the following:
   - IVL - This is the default.
   - SVL
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

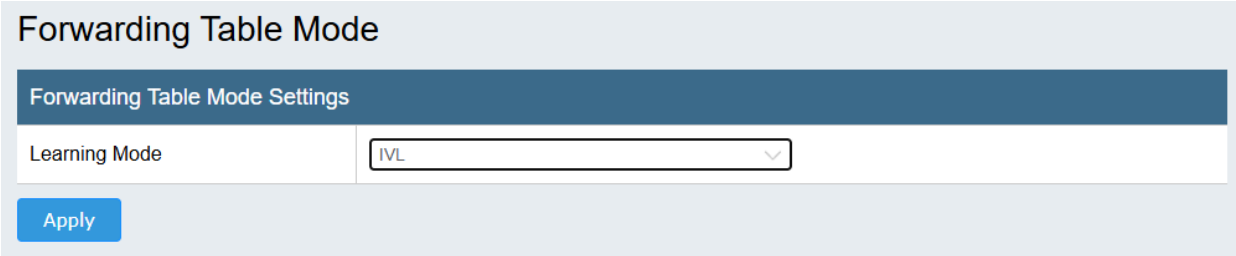


Figure 109. Forwarding Table Mode Window

Chapter 37

GARP VLAN Registration Protocol

This chapter contains the following sections:

- “GVRP Overview” on page 362
- “Enabling or Disabling GVRP” on page 366
- “Configuring GVRP Port Settings” on page 367
- “Configuring GVRP Time Settings” on page 369

GVRP Overview

The GARP VLAN Registration Protocol (GVRP) allows network devices to share VLAN information and modify existing VLANs or add new VLANs, automatically. This makes managing VLANs that span multiple switches easier. Without GVRP, you have to manually configure the switches to ensure that the various parts of VLANs can communicate with each other across different switches. With GVRP, an application of the Generic Attribute Registration Protocol (GARP), this is done automatically.

The switch uses GVRP protocol data units (PDUs) to share VLAN information among GVRP-active devices. The PDUs contain the VID numbers of the VLANs on the switch. When the switch receives a GVRP PDU on a port, it examines the PDU to determine the VIDs of the VLANs on the device that sent it. It then does the following:

- If the PDU contains a VID of a VLAN that does not exist on the switch, it adds the designated VLAN and adds the port that received the PDU as a tagged member of the VLAN. A VLAN added by GVRP is called a dynamic GVRP VLAN.
- If the PDU contains a VID of a VLAN that already exists on the switch but the port is not a member of it, the switch adds the port as a tagged member of the VLAN. A port that has been added by GVRP to a static VLAN (that is, a VLAN added by the manager) is called a dynamic GVRP port.

Only GVRP can modify or delete dynamic GVRP VLANs. Dynamic GVRP VLANs exist only so long as there are active nodes in the VLANs. If all the nodes of a dynamic GVRP VLAN stop transmitting traffic and there are no active links, GVRP deletes it from the switch.

Dynamic GVRP ports in static VLANs remain members of the VLANs as long as there are active VLAN members. If all members of a VLAN become inactive or there are no active links, GVRP removes the dynamic ports from the VLAN, but does not delete the VLAN if it is a static VLAN.

Figure 110 on page 363 is an example of how GVRP works.

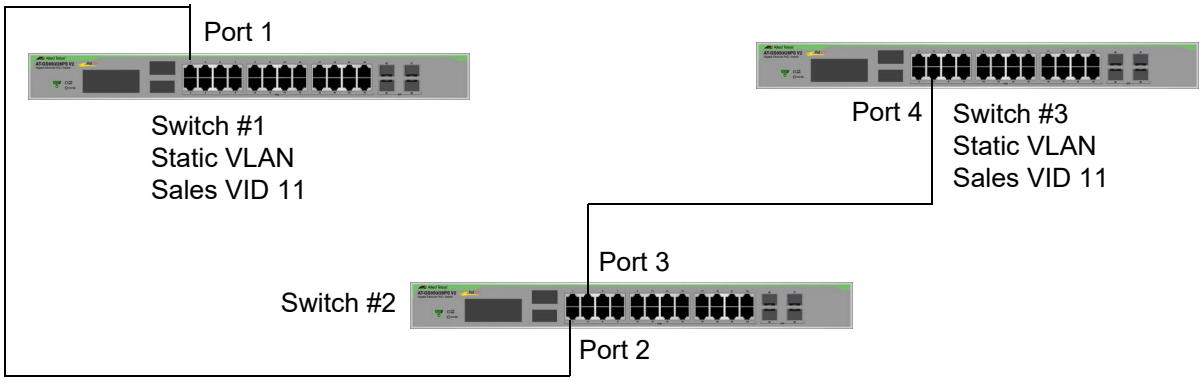


Figure 110. GVRP Example

The example consists of three switches. Switches #1 and #3 have the Sales VLAN, but switch #2 does not. Consequently, the end nodes of the two parts of the Sales VLANs cannot communicate with each other.

Without GVRP, you would have to manually add the Sales VLAN to switch #2. But with GVRP, the switch adds the VLAN automatically. Here is how GVRP resolves the example.

1. Port 1 on switch #1 sends to port 2 on switch #2 a PDU containing the VIDs of all the VLANs on the switch, including VID 11 for the Sales VLAN.

2. Switch #2 examines the PDU it receives on port 2 and notes that it does not have a VLAN with a VID 11. In response, it creates the VLAN as a dynamic GVRP VLAN, assigning it a VID 11 and the name GVRP_VLAN_11. (The name of a dynamic GVRP VLAN has the prefix “GVRP_VLAN_”, followed by the VID number.) The switch then adds port 2, the port that received the PDU, as a tagged member of the VLAN.

3. Switch #2 sends a PDU from port 3 containing all the VIDs of the VLANs on the switch, including the new GVRP_VLAN_11 with its VID of 11. (Note that port 3 is not yet a member of the VLAN. Ports are added to VLANs when they receive PDUs from other network devices, not when they transmit PDUs.)

4. Switch #3 receives the PDU on port 4 and, after examining it, notes that one of the VLANs on switch #2 has the VID 11, which matches the VID of an already existing VLAN on the switch. So it does not add the VLAN because it already exists. It then determines whether the port that received the PDU, in this case port 4, is a member of the VLAN. If it is not a member, it automatically adds the port to the VLAN as an tagged dynamic GVRP port. If the port is already a member of the VLAN, then no change is made.

5. Switch #3 sends a PDU out port 4 to switch #2.
6. Switch #2 receives the PDU on port 3 and adds the port as a tagged dynamic GVRP port to the dynamic GVRP_VLAN_11 VLAN.

There is now a communications path for the end nodes of the Sales VLAN on switches #1 and #3. GVRP created the new GVRP_VLAN_11 dynamic GVRP VLAN with a VID of 11 on switch #2 and added ports 2 and 3 to the VLAN as tagged dynamic GVRP ports.

Guidelines

Here are the GVRP guidelines:

- ❒ GVRP is supported with STP or RSTP or without spanning tree.
- ❒ Both ports of a network link between switches have to be running GVRP.
- ❒ You cannot modify or delete dynamic GVRP VLANs.
- ❒ You cannot remove dynamic GVRP ports from static or dynamic VLANs.
- ❒ To be detected by GVRP, a VLAN needs to have at least one active node or have at least one port with a valid link to an end node. GVRP cannot detect VLANs that do not have any active nodes or valid port links.
- ❒ Resetting the switch erases all dynamic GVRP VLANs and dynamic GVRP port assignments. The dynamic assignments are relearned by the switch as PDUs arrive on the ports from other switches.
- ❒ GVRP has three timers: join timer, leave timer, and leave all timer. The values for these timers have to be set the same on all switches running GVRP. Timers with different values on different switches can result in GVRP compatibility problems.
- ❒ You can convert dynamic GVRP VLANs and dynamic GVRP port assignments to static VLANs and static port assignments.
- ❒ The default port settings on the switch for GVRP is active, meaning that the ports participate in GVRP. For security purposes. Allied Telesis recommends disabling GVRP on those ports that are connected to GVRP-inactive devices, meaning devices that do not feature GVRP.
- ❒ PDUs are transmitted from only those switch ports where GVRP is enabled.

GVRP and Network Security

GVRP should be used with caution because it can expose your network to unauthorized access. If a network intruder connects to a switch port running GVRP and transmits a bogus GVRP PDU containing VIDs of restricted VLANs, GVRP makes the port a member of the VLANs, giving the intruder access to restricted areas of your network.

Here are a suggestions on how to protect your network against this type of intrusion:

- Activating GVRP only on those switch ports connected to other GVRP devices. Do not activate GVRP on ports that are connected to non-GVRP devices.
- After the switches have used GVRP to form the VLANs and VLAN links, you should convert all dynamic GVRP VLANs and dynamic GVRP ports to static assignments, and then turn off GVRP on all switches. This preserves the new VLAN assignments while protecting against network intrusion.

GVRP-inactive Intermediate Switches

If two GVRP devices are separated by a non-GVRP switch, the GVRP devices may not be able to share VLAN information. There are two issues involved.

The first is whether the intermediate switch forwards GVRP PDUs that it receives from the GVRP switches. GVRP PDUs are management frames, intended for the switch's CPU. In all likelihood, a non-GVRP switch will discard the PDUs because it will not recognize them.

The second issue is that even if a non-GVRP switch forwards GVRP PDUs, it will not automatically add the VLANs. Consequently, even if GVRP switches receive the PDUs and add the necessary VLANs, an intermediate switch may block the VLAN traffic, unless you manually modify its VLANs and port assignments.

Enabling or Disabling GVRP

To enable or disable GVRP on the switch:

1. Select **Network** > **GVRP** > **Global Settings** from the menu to display the GVRP Global Settings. Refer to Figure 111.
2. Select one of the following options from the GVRP Status menu:
   - ❒ **Disabled** - Disables GVRP on the switch. This is the default setting.
   - ❒ **Enabled** - Enables GVRP. The switch transmits GVRP PDUs from the ports and processes ingress PDUs.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

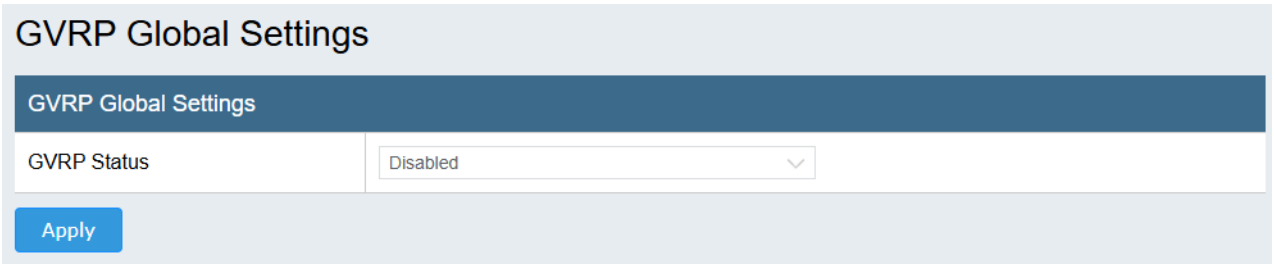


Figure 111. GVRP Global Settings Window

Configuring GVRP Port Settings

To configure the GVRP port settings:

1. Select **Network** > **GVRP** > **Port Settings** from the menu. The GVRP Port Settings window is shown in Figure 112 on page 368.
2. Configure the GVRP settings in Table 84.

Table 84. GVRP Port Settings Window

Field	Description
Port	Lists the switch ports.
Dynamic VLAN Status	Choose one of the following: - **Enabled**: Activates GVRP on a port. The switch transmits PDUs from it and processes ingress PDUs. This is the default setting. - **Disabled**: Deactivates GVRP on a port.
Restricted VLAN Registration	Choose one of the following: - **Enabled**: Adds a port only to static VLANs on the switch. When a port receives PDUs containing VLANs to which it is not a member, the switch adds it only if the VLANs are static VLANs. A port is not added to dynamic or unknown VLANs. - **Disabled**: Adds a port to static, dynamic, or unknown VLANs. When a port receives PDUs with VLANs to which it is not a member, the switch adds it to the VLANs regardless of VLAN type. This is the default setting.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

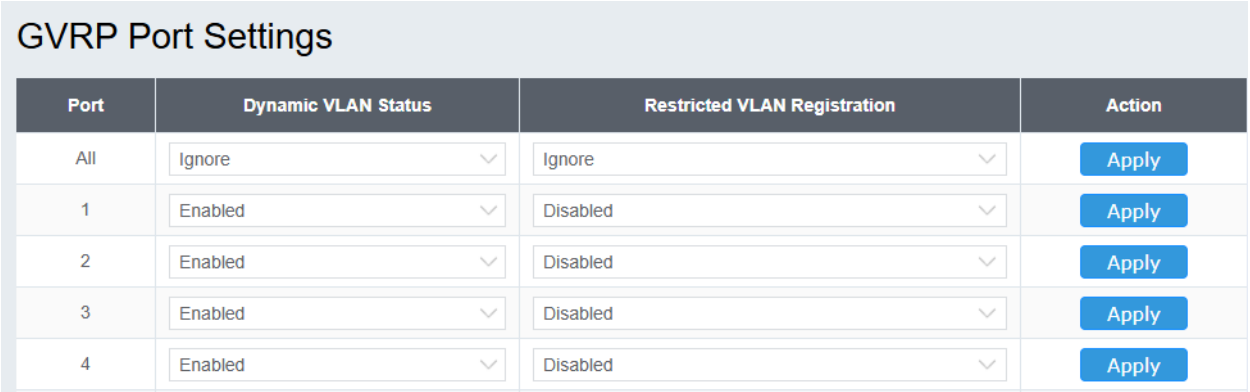


Figure 112. GVRP Port Settings Window

Configuring GVRP Time Settings

To configure the GVRP time settings:

1. Select **Network** > **GVRP** > **Time Settings** from the menu to display the GVRP Time Settings window in Figure 113.
2. Configure the fields in Table 85 for each port.

Note
Do not change the timers if you are not familiar with their functions. Refer to IEEE 802.1p standard for definitions.

Table 85. GVRP Time Settings Window

Column	Description
Port	Lists the switch ports.
JoinTime	Enter the GARP Join Timer. The range is 10 to 1073741810 milliseconds.
LeaveTime	Enter the GARP Leave Timer. The range is 30 to 2147483630 milliseconds. The timer has to be set in relation to the GVRP Join Timer according to the following equation: GARPLeaveTimer >= (GARPJoinTimer X 2) + 10
LeaveAllTime	Enter the GARP Leave All Timer. The range is 40 to 2147483640 milliseconds. The timer must be set in relation to the GVRP Leave Timer according to the following equation: GARPLeaveAllTimer > (GARPLeaveTimer + 10)

Review the following:

- The GARPLeaveTimer must be greater than (GARPJoinTimer x2 + 10) and the GARPLeaveAllTimer must be greater than (GARPLeaveTimer + 10). The acceptable input values are multiples of 10. The switch rounds down values that are not multiples of 10.
- To ensure compatibility between network devices, you have to configure the same values for the GARP Join Timer, GARP Leave Timer, and GARP Leave All Timer on all participating GVRP devices in your network.

3. Click **Apply** for ports where the settings were changed.

Note
Select **Save** from the menu to save your changes.

Figure 113. GVRP Time Settings Window

Chapter 38
Voice VLAN

This chapter describes the voice VLAN feature in the following sections:

- ❒ “Voice VLAN Overview” on page 372
- ❒ “General Guidelines” on page 374
- ❒ “Configuring the Voice VLAN” on page 375
- ❒ “Managing the OUI Table” on page 378

Voice VLAN Overview

The voice VLAN is intended for Voice over IP (VoIP) phones. It enables the switch to provide high-quality, uninterrupted voice traffic from phone users on its ports. The voice VLAN provides these basic functions:

- Identify IP phone traffic on an 802.1Q tagged VLAN by Organization Unique Identifiers (OUIs).
- Assign traffic a high Class of Service value.
- Direct traffic to a high traffic queue on the egress port.

These actions help minimize interruptions to phone conversations and increases voice quality.

802.1Q VLAN

The first step to implementing the voice VLAN is to add an 802.1Q tagged VLAN to the switch. The VLAN will form the base of the voice VLAN. The VLAN has to have one or more tagged or untagged ports that will serve as the voice VLAN ports. The VLAN has an upstream port leading to the phone system and downstream ports leading to the individual IP phones or other voice VLAN network nodes, such as other Ethernet switches or a DHCP server. The voice VLAN can have only one 802.1Q VLAN. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.

Organization Unique Identifier (OUI)

The switch identifies IP phone traffic by examining the OUIs in the source MAC addresses of the packets. Each IP phone manufacturer has one or more unique OUIs. An OUI is three bytes long and is usually expressed in hexadecimal format. It is incorporated into the first part of the MAC address of an Ethernet network device. You can find the OUI of an IP phone in the first three complete bytes of its MAC address. IP phones from the same manufacturer typically have the same OUI.

To identify voice data packets, the switch compares the OUI information in the source MAC addresses in the packets against entries in its OUI table. To configure the table, you enter the complete MAC address of one of your IP phones. An “OUI Mask” is automatically generated and applied by the switch to produce the manufacturer’s OUI. The switch supports up to ten OUI entries.

If all your phones have the same OUI, then you only have to enter the MAC address from one phone in the OUI table. If your phones have more than one OUI, then you have to enter one MAC address for each OUI.

CoS with Voice VLAN

The Voice VLAN has a CoS parameter to maintain the voice quality between the ingress and egress ports of the switch. You have to enable CoS for the Voice VLAN CoS priority to take effect. The CoS priority level you designate is applied to voice traffic on all ports of the voice VLAN.

Normally, most (non-Voice) Ethernet traffic traverses the switch through lower-order egress queues. To avoid delays and interruptions in the voice data flow, you should assign a high-order queue to the CoS priority level of the voice VLAN, and set the scheduling algorithm to Strict Priority. These settings ensure that the voice data packets are processed before other types of data so that the voice quality is maintained as the switch forwards voice data. For more information, refer to “Mapping CoS Priorities to Egress Queues” on page 414 and “Setting the Queue Scheduling Algorithm” on page 418.

Dynamic Port Auto-Detection

The switch has two ways to learn which ports are connected to IP phones in the voice VLAN. One way is for you to identify the ports yourself when adding the 802.1Q tagged VLAN that serves as the base of the voice VLAN. Another way is to let the switch discover them with its auto-detection feature. When the switch detects an ingress packet with an OUI on an ingress port that is not already part of the voice VLAN, it moves the port into the VLAN. The switch can also remove ports from the voice VLAN after a predefined timeout period, when IP phones are inactive.

Here are the guidelines for the auto-detection feature:

- Ports cannot be members of any VLAN. They have to be designated as “Not Member” ports in all VLANs. The switch will not examine packets for OUIs on ports that are members of other VLANs. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.
- IP phones have to support 802.1Q VID packets with imbedded VLAN ID tags. You have to manually set their VLAN IDs to be the same as the voice VLAN ID. This enables the switch to identify the packets from the IP phones as part of the voice VLAN, and so automatically move the ports into the VLAN. For example, if the voice VLAN has the VID 20, you have to set the VIDs on the IP phones to 20.
- Auto-detection is not supported on switch ports connected to IP phones that do not support 802.1Q VIDs. Those ports have to be configured as static tagged ports in the voice VLAN.

Note
The port VLAN IDs (PVID) of static tagged members of the voice VLAN have to be the same as the voice VLAN ID. This is to ensure that all untagged packets entering the ports are switched within the voice VLAN as the voice data pass through the switch. Refer to “Configuring PVIDs and Filters for Tagged and Untagged Ports” on page 348.

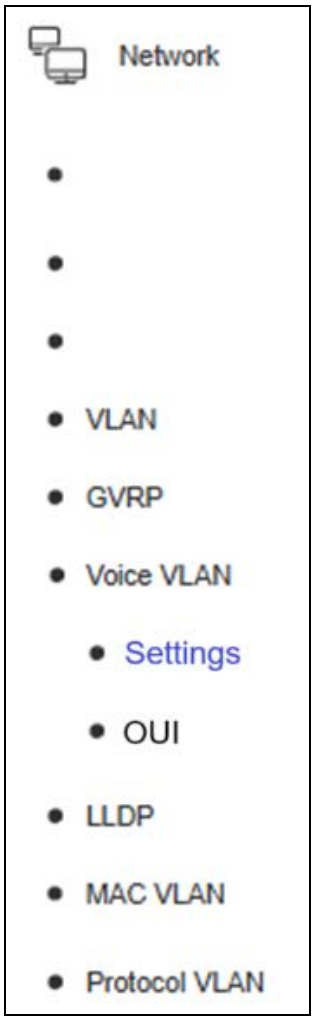
Note
The switch does not support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED). It cannot set the VIDs on IP phones that support 802.1Q VID.

General Guidelines

Here are the voice VLAN guidelines:

- The switch supports one voice VLAN.
- The voice VLAN has to be an 802.1Q tagged VLAN.
- The switch port connected to the phone system at the network core has to be a static member of the voice VLAN.
- You have to configure the port VLAN IDs (PVID) of static tagged members of the voice VLAN to be the same as the voice VLAN ID. Refer to “Configuring PVIDs and Filters for Tagged and Untagged Ports” on page 348.
- You have to enter the OUIs of the IP phones into the OUI table. Refer to “Managing the OUI Table” on page 378.
- Only one MAC address for each unique OUI is required.
- The switch supports up to ten OUIs.
- The switch does not support Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED).

Configuring the Voice VLAN



To configure a voice VLAN on the switch:

Note
A voice VLAN must be an 802.1Q tagged VLAN. For instructions, refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.

1. Select **Network** > **Voice VLAN** > **Settings**. The Voice VLAN Setting window is shown in Figure 114 on page 377.
2. Configure the settings in Table 86.

Table 86. Voice VLAN Settings Window

Field	Description
Voice VLAN Status	
Voice VLAN	Enables and disables the VLAN. The default is disabled.
Voice VLAN Global Settings	
VLAN ID	Select the VID of the 802.1Q tagged VLAN to be the voice VLAN. You can select only one VLAN. If you have not added the VLAN, go to “Adding or Viewing 802.1Q Tagged VLANs” on page 344.
Aging Time	Enter the amount of elapsed time, in hours, after which the switch removes ports with inactive IP phones from the voice VLAN. This applies only to ports discovered with auto-detection. For example, when the Aging Time is set to 1 hour, the default setting, the switch removes ports from the voice VLAN when IP phones discovered with auto-detection are inactive for one hour. The range is 1 to 120 hours.

Table 86. Voice VLAN Settings Window (Continued)

Field	Description
CoS	Select from the menu the CoS priority level the switch is to assign to voice data packets received on voice VLAN ports. The range is 0 to 7. The default is 7. You need to enable CoS on the switch and map this CoS value to the CoS “Highest” egress queue on the ports. Refer to “Mapping CoS Priorities to Egress Queues” on page 414. You should also set the scheduling algorithm to Strict Priority, as explained in “Setting the Queue Scheduling Algorithm” on page 418.
Voice VLAN Port Settings Table	
Auto Detection	To configure auto-detection on the ports in the table, select one of the following: - **Enabled** - Enables the voice VLAN auto-detection feature on the port. - **Disabled** - Disables the auto-detection feature. For a description, refer to “Dynamic Port Auto-Detection” on page 373
Status	Display whether the switch has detected an active IP phone on the phone that is participating in the voice VLAN.

3. Click **Apply** to activate your changes.

Note
Select **Save** from the menu to save your changes.

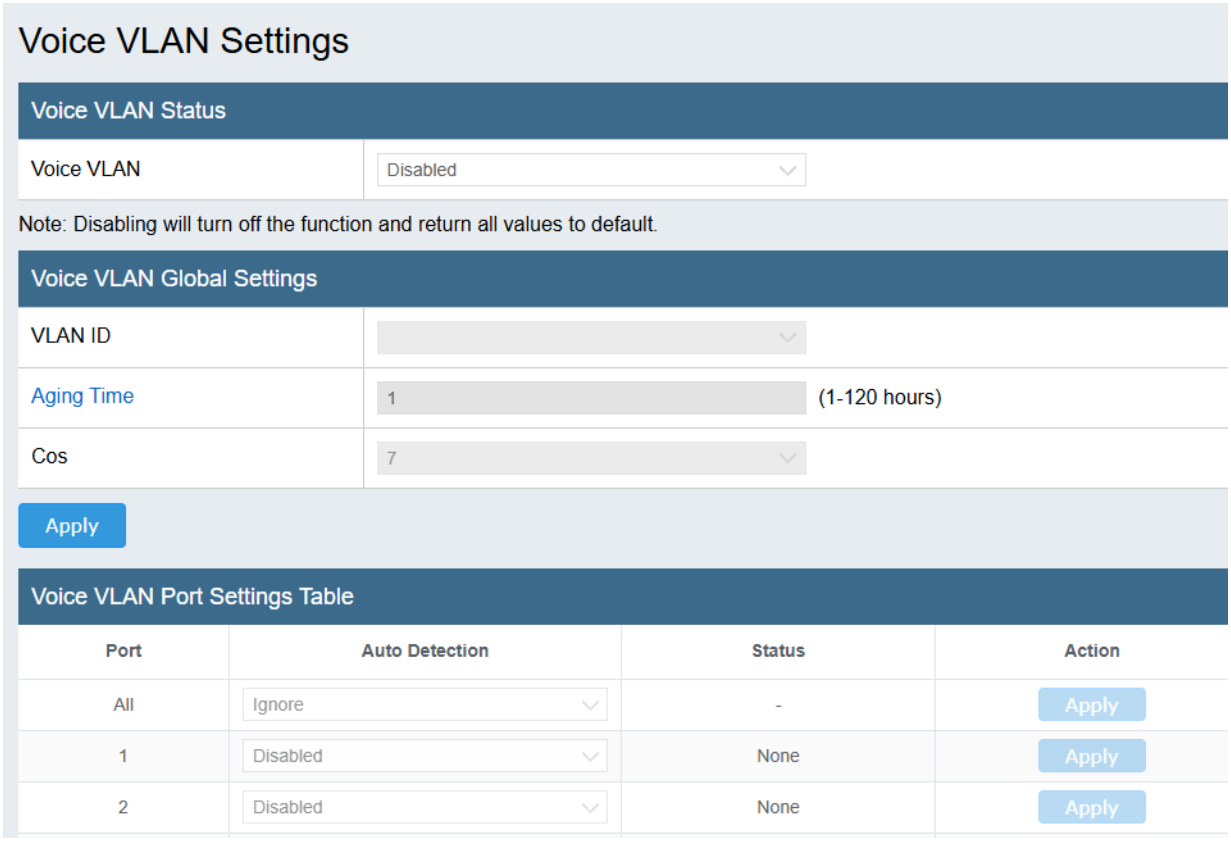


Figure 114. Voice VLAN Settings Window

Managing the OUI Table

The OUI table can contain up to ten OUIs entries of IP phone manufacturers. The switch uses the table to identify voice packets on its ports. You have to enter the MAC address from one phone for each unique OUI. Refer to “Organization Unique Identifier (OUI)” on page 372.

To add or delete OUI entries from the table:

1. Select **Network** > **Voice VLAN** > **OUI** from the menu to display the Voice VLAN OUI Settings window in Figure 115 on page 379.
2. To add an OUI entry, configure the settings in Table 87.
3. Click **Add**.
4. To delete OUI entries, click **Delete** in the Action column of the table.

Note
Click **Save** in the menu to save your changes.

Table 87. Voice VLAN OUI Settings Window

Field	Description
Description	Enter the name of the phone manufacturer and phone model. The description can be up to 20 characters.
Telephony OUI	Enter the MAC address of one of the phones.

Note
You cannot modify OUIs in the table. If you need to edit an OUI, you must delete and reenter it.

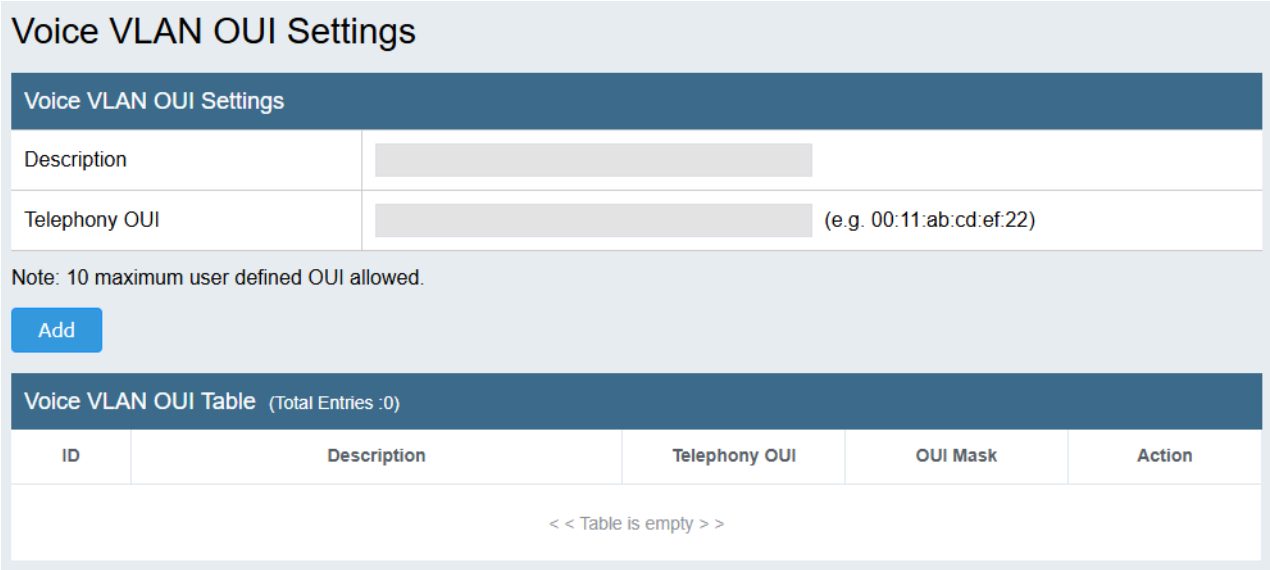


Figure 115. Voice VLAN OUI Settings Window

Chapter 39

Link Layer Discovery Protocol

This chapter describes Link Layer Discovery Protocol (LLDP) in the following sections:

- ❒ “LLDP Overview” on page 382
- ❒ “Configuring LLDP” on page 383
- ❒ “Displaying Neighbor Information” on page 395

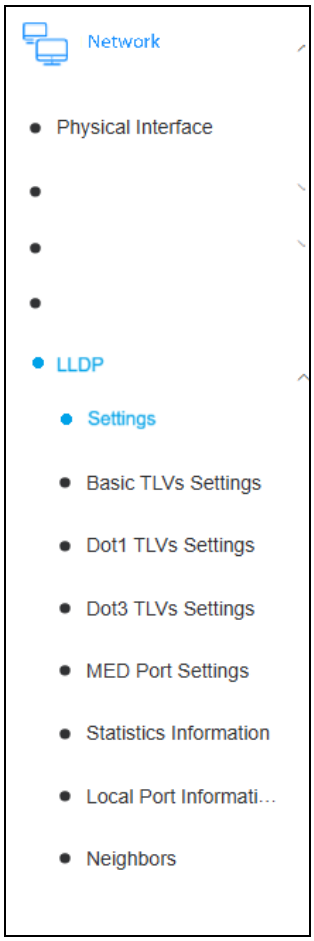
LLDP Overview

Link Layer Discovery Protocol (LLDP) allows Ethernet network devices, such as switches and routers, to share and store device-related information with each other. Neighboring devices that use LLDP can advertise parts of their Layer 2 configuration to each other, which allows you to identify several types of incorrect configurations more easily.

LLDP is a “one-hop” protocol. LLDP information can only be sent to and received by devices that are directly connected to each other, or connected via a hub or repeater. Devices that are directly connected to each other are called neighbors. Advertised information is not forwarded on to other devices on the network. Also, LLDP is a one-way protocol. That is, the information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors, and the communication ends there. Transmitted advertisements do not solicit responses, and received advertisements do not solicit acknowledgments. LLDP cannot solicit any information from other devices. LLDP operates over physical ports only. For example, you can configure it on switch ports that belong to static port trunks or LACP trunks, but not on the trunks themselves, and on switch ports that belong to VLANs, but not on the VLANs themselves.

Each port can be configured to transmit local information, receive neighbor information, or both. LLDP transmits information in packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains a particular type of information about the device or port transmitting it.

Configuring LLDP



Perform the following procedure to configure LLDP:

1. Select **Network** > **LLDP** > **Settings** from the menu.
2. To enable or disable LLDP on the switch, perform the following:
   a. Select **Enabled** or **Disabled** from the LLDP Status pull-down menu in LLDP Global Settings, to enable or disable the feature. The default is disabled. You have to enable LLDP to configure the settings.
   b. Click **Apply**.
3. To view or configure the global and port settings, refer to Table 88.
4. After completing your changes, select **Save** from the menu to save your changes.

Table 88. LLDP Global Settings

Field	Description
LLDP Global Settings	
LLDP Status	Options are: – Enabled: Enables LLDP. – Disabled: Disables LLDP. This is the default setting.
LLDP-MED Parameter Settings	
Fast Start Repeat Count	Enter the fast count start count for LLDP-MED. This parameter controls the number of fast start advertisements a port sends when initiating LLDP-MED advertisements. The range is 1 to 10 times. The default is 3 times.

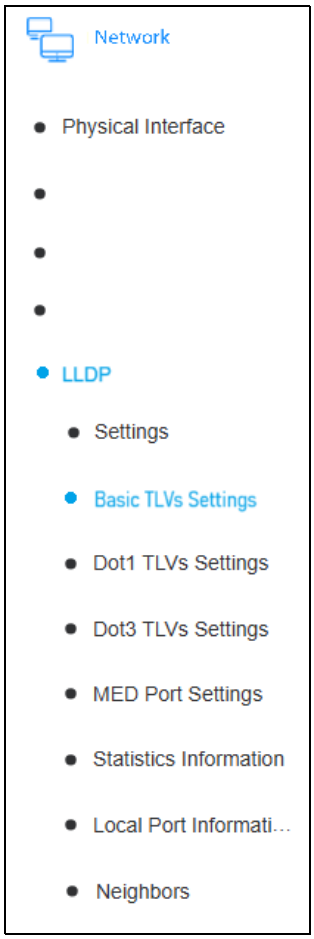
Table 88. LLDP Global Settings (Continued)

Field	Description
LLDP Parameter Settings	
Message TX Hold Multiplier	Enter the multiplier value for the Message TX Interval. This is used to calculate the Time To Live (TTL) that the switch advertises to neighbors. TTL controls the length of time in seconds that advertisements are valid. The range is 2 to 10. The default is 4.
Message TX Interval	Enter the interval between regular transmissions of LLDP advertisements. The interval must be a least four times the LLDP TX Delay. The range is from 5 to 32768 seconds. The default is 30 seconds.
LLDP Reinit Delay	Enter the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized. The range is from 1 to 10 seconds. The default is 2 seconds.
LLDP TX Delay	Enter the minimum time interval between transmissions of LLDP advertisements from changes to LLDP local information. The transmission delay timer cannot be greater than a quarter of the Message TX Interval. The range is from 1 to 8192 seconds. The default is 2 seconds.
LLDP System Information	
Chassis ID Subtype	Displays “MAC Address” as the Chassis ID subtype. This value is not adjustable.
Chassis ID	Displays the switch’s MAC address. This value is not adjustable.
System Name	Displays the system name of the switch. Refer to Chapter 3, “System Name, Location, and Administrator” on page 69.
System Description	Displays the description of the switch. Refer to Chapter 3, “System Name, Location, and Administrator” on page 69.
LLDP-MED System Information	
Device Class	Displays Network Connectivity as the device class. This value is not adjustable.

Table 88. LLDP Global Settings (Continued)

Field	Description
Hardware Revision	Displays the hardware revision. This value is not adjustable.
Firmware Revision	Displays the firmware revision. This value is not adjustable.
Software Revision	Displays the software revision. This value is not adjustable.
Manufacturer Name	Displays ATI Corporation as the manufacturer name. This value is not adjustable.
Model Name	Displays the model name of the switch. This value is not adjustable.
Asset ID	The asset ID value. This value is adjustable. It can be up to 32 alphanumeric characters.
LLDP Port State Settings	
State	Configures the port setting. Options in the pull-down menu are: – Disabled: Configures the port to block ingress and egress LLDPDUs. – RxTx: Configures the port to transmit and receive LLDPDUs. This is the default setting. – RxOnly: Configures the port to receive but not transmit LLDPDUs. – TxOnly: Configures the port to transmit but not receive LLDPDUs.

Basic TLVs Settings Table



To set basic TLV settings on the individual ports:

1. Select **Network** > **LLDP** > **Basic TLVs Settings** from the menu. The LLDP Neighbors Information window is shown in Figure 116.
2. Configure the TLV parameters on the individual ports. Refer to Table 89.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 89. Basic TLVs Settings Window

Column	Description
Port	Physical port number.
Port Description	Alpha numeric description of the port's function. Refer to Chapter 19, "Basic Port Settings" on page 191
System Name	The system's assigned name. Refer to Chapter 3, "System Name, Location, and Administrator" on page 69.
System Description	A description of the device in alpha-numeric format. The information includes the device's hardware and operating system.
System Capabilities	The device's bridge functions, and whether they are currently enabled.

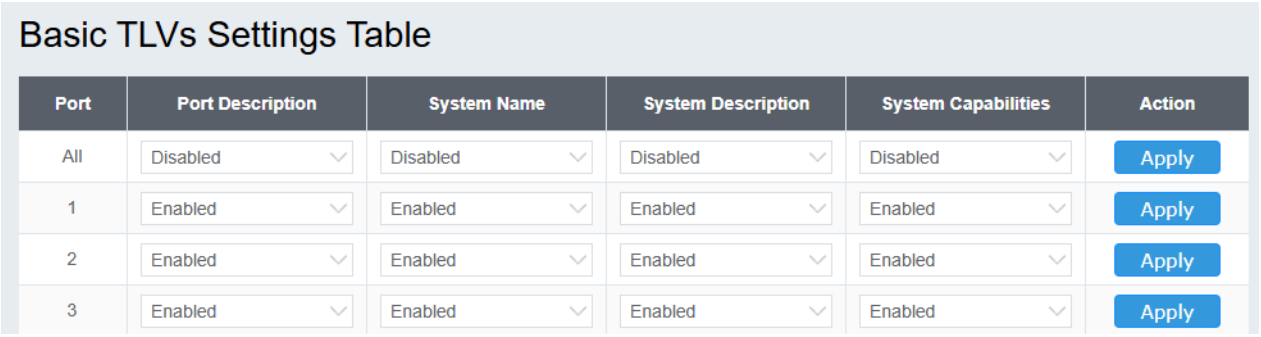
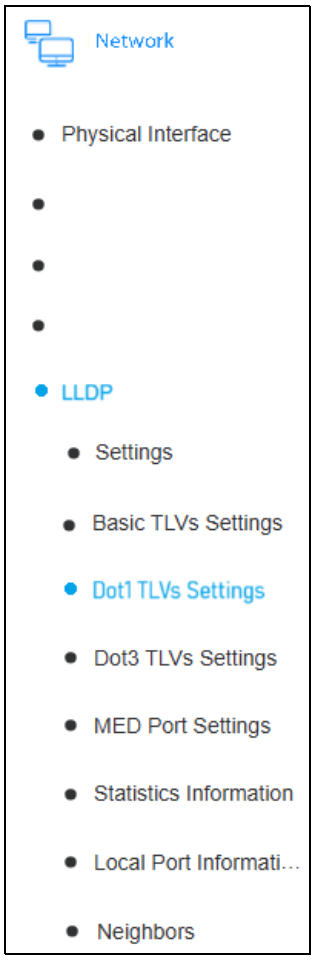


Figure 116. Basic TLVs Setting Table

Dot1 TLVs Settings Table



To set Dot1 TLV settings on the individual ports:

1. Select **Network** > **LLDP** > **Dot1 TLVs Settings** from the menu. The Dot1 TLVs Setting window is shown in Figure 117.
2. Configure the TLV parameters on the individual ports. Refer to Table 90.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 90. Dot1 TLVs Setting Window

Column	Description
Port	Physical port number.
Port VLAN ID	VLAN identifier that the local port associates with untagged or priority tagged frames.
VLAN ID List	VLAN identifiers of the port and protocol VLANs supported by the port.
Protocol Identity	Designates the protocols that are available from the switch port. Available protocols are: – EAPOL – LACP – GVRP – STP

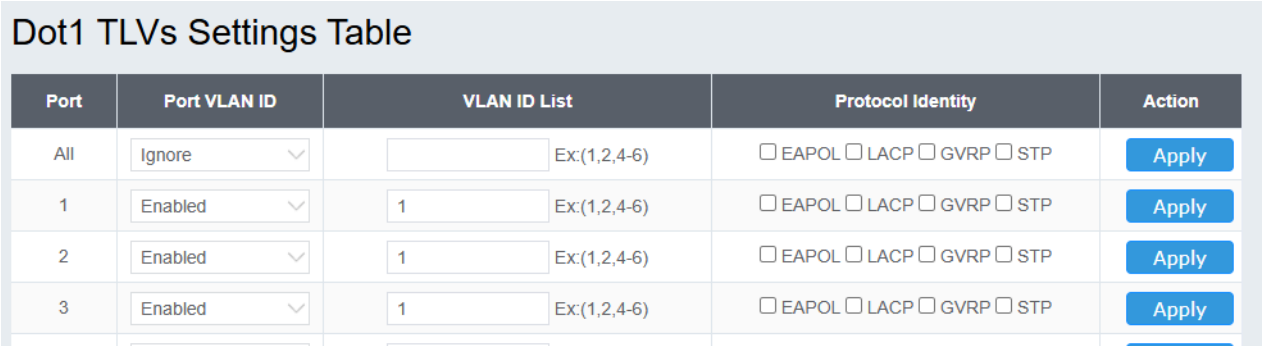
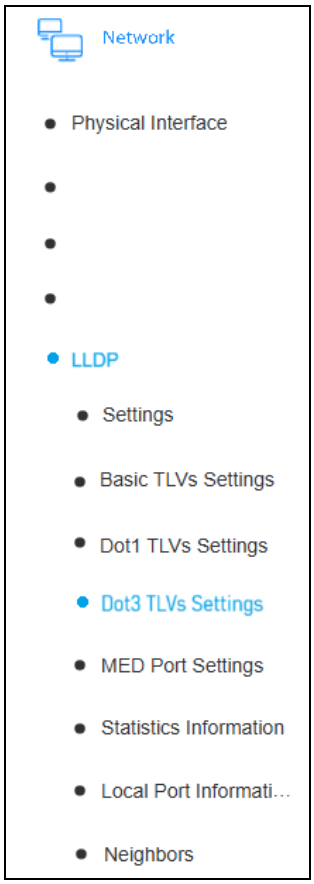


Figure 117. Dot1 TLVs Setting Table

Dot3 TLVs Settings Table



To set Dot3 TLV settings on the individual ports:

1. Select **Network** > **LLDP** > **Dot3 TLVs Settings** from the menu. The Dot3 TLVs Setting window is shown in Figure 118 on page 390.
2. Configure the TLV parameters on the individual ports. Refer to Table 91.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 91. Dot3 TLVs Settings Table Window

Column	Description
Port	Physical port number.
MAC/PHY Configuration/ Status	The current values of the following port operations: – Speed and duplex mode auto-negotiation support – Auto-negotiation status – PMD (physical media dependent) auto-negotiation advertised capability – Operational MAU type This TLV is always included in LLDP-MED advertisements.
Link Aggregation	Whether the link supports aggregation. whether it is currently in an aggregation, and if it is, the port of the aggregation.
Maximum Frame Size	The maximum supported 802.3 frame size that the sending device is capable of receiving. Larger frames are dropped.
Power Via MDI	Capabilities of power via MDI.

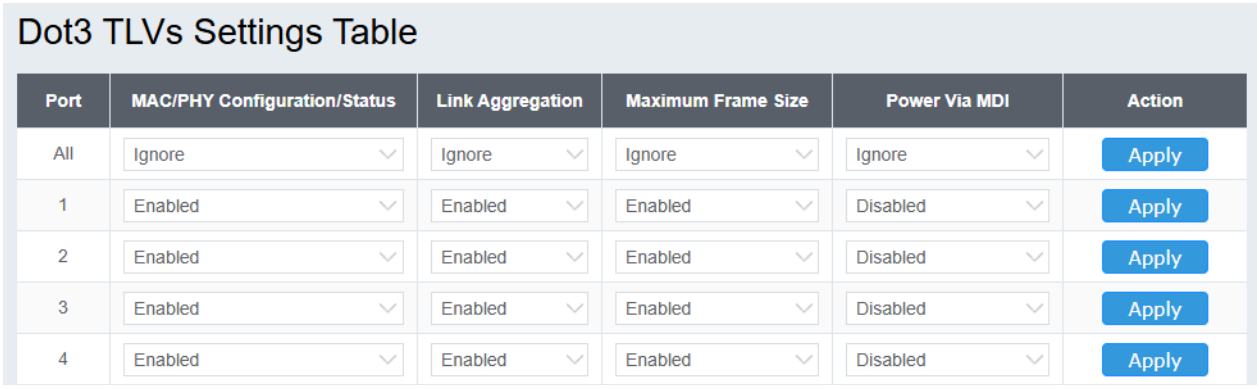
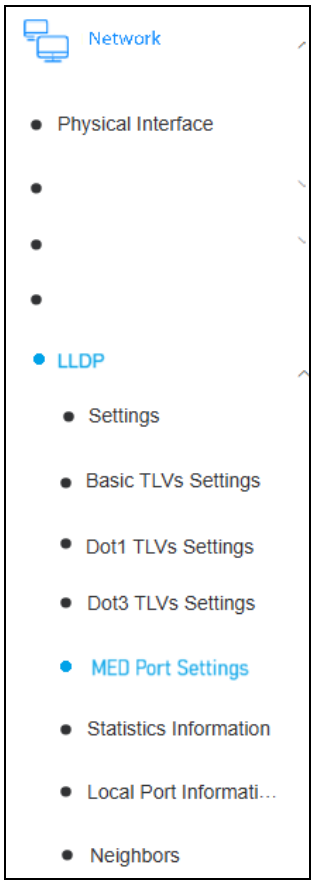


Figure 118. Dot3 TLVs Setting Table

MED Port TLV Settings



To set MED TLV settings on the individual ports:

1. Select **Network** > **LLDP** > **MED Port Settings** from the menu. The MED Port Settings window is shown in Figure 119.
2. Configure the MED parameters on the individual ports. Refer to Table 92.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 92. MED Port TLV Settings Window

Column	Description
Port	Physical port number.
Capabilities	LLDP-MED Capabilities TLV. When this is enabled, the MAC/PHY Configuration/Status TLV is also included in LLDP-MED advertisements.
Inventory	Inventory Management TLV Set. Includes the following TLVs: – Hardware Revision – Firmware Revision – Software Revision – Serial Number – Manufacturer Name – Model Name – Asset ID

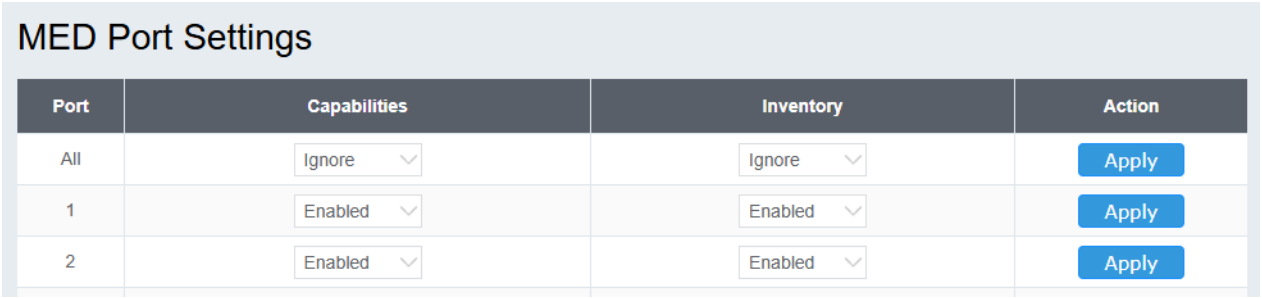
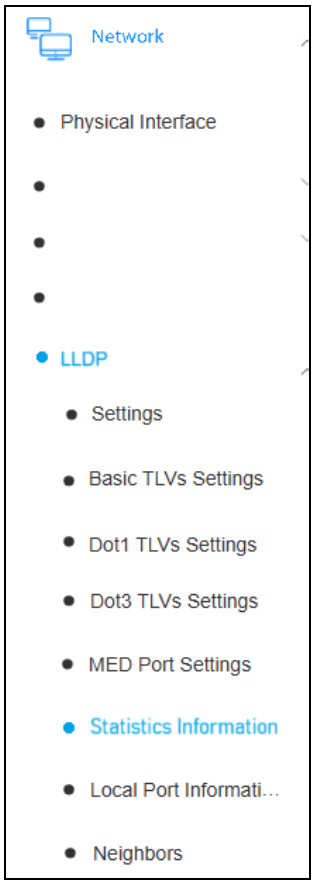


Figure 119. MED Port Settings

Statistics Information



To view LLDP statistics, select **Network** > **LLDP** > **Statistics Information** from the menu. The Statistics Information window is shown in Figure 120 on page 393. The statistics in the top LLDP Statistics Information section of the window are defined in Figure 93. The statistics in the bottom LLDP Statistics Port section are defined in Figure 94.

Table 93. LLDP Statistics Information Window

Row	Description
Last Change Time	The amount of time passed since the switch last implemented a change based on advertised information from a neighbor.
Total Inserts	Total number of times the switch received advertised information from neighbors.
Total Deletes	Total number of times the switch deleted advertised information from neighbors from the neighbor table, for any reason.
Total Drops	Total number of times insufficient resources prevented the switch from entering information advertised by neighbors into the neighbor table.
Total Ageouts	Total number of times the switch deleted information from the neighbor table because the TTL interval expired.

Table 94. LLDP Statistics Ports Window

Column	Description
Port	Physical port number.
Total Transmits	Total number LLDPDU frames the switch transmitted from a port.
Total Discards	Total number LLDPDU frames the switch deleted from a port before transmission.
Total Errors	Total number LLDPDU frames with errors the switch detected on a port before transmission.
Total Receives	Total number LLDPDU frames the switch received on a port.

Table 94. LLDP Statistics Ports Window (Continued)

Column	Description
Total TLV Discards	Total number of LLDP TLVs received and discarded on a port for any reason.
Total TLV Unknowns	Total number of LLDP TLVs received on a port that were not recognized.
Total Ageouts	Total number of times the switch deleted TLVs learned on a port from the neighbor table because the TTL interval expired.

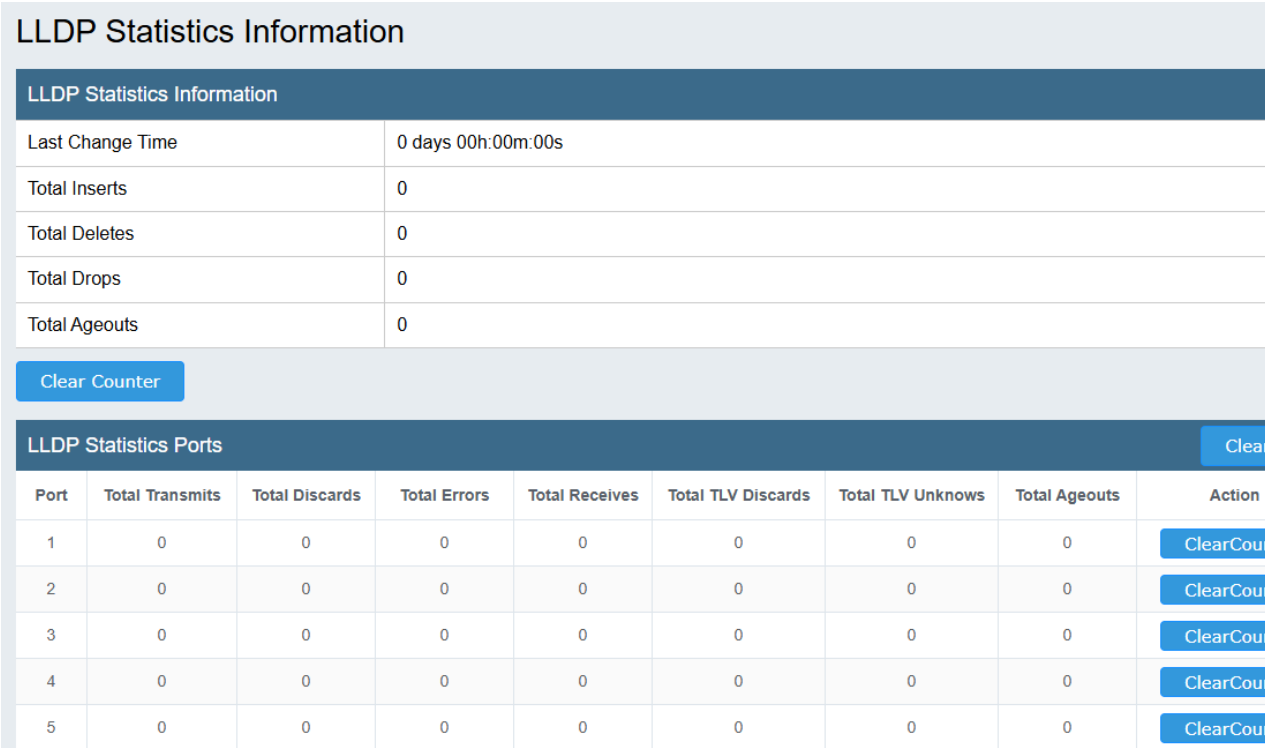
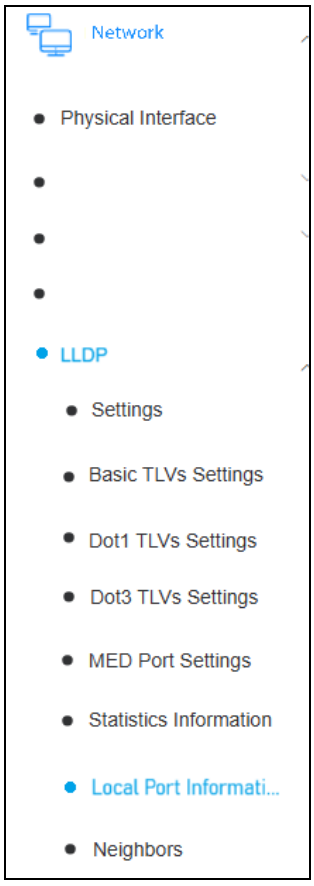


Figure 120. LLDP Statistics Information Table

LLDP Local Port Information



To view LLDP local port information, select **Network** > **LLDP** > **Local Port Information** from the menu. The LLDP Local Port Information window is shown in Figure 121. The columns are defined in Figure 95.

Table 95. LLDP Local Port Information Window

Row	Description
Port ID Subtype	Local.
Port ID	Physical port number.
Port Description	Default or assigned port description.

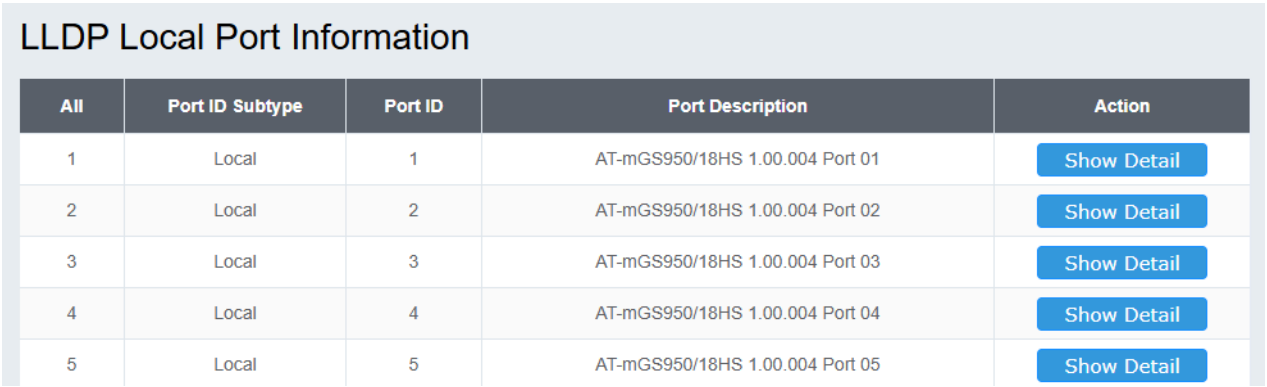
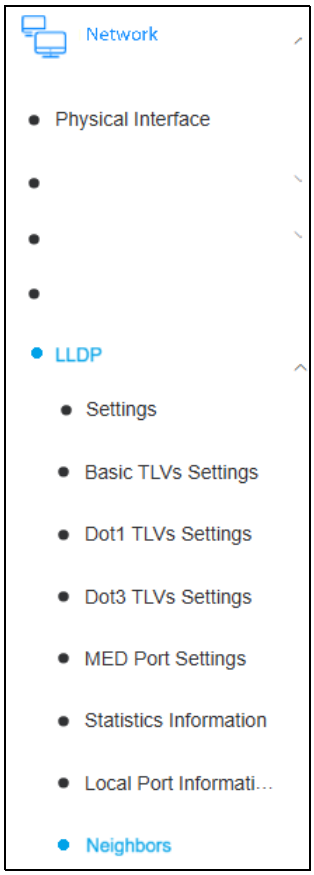


Figure 121. LLDP Local Port Information

Displaying Neighbor Information



To view information from neighboring LLDP devices, select **Network** > **LLDP** > **Neighbors** from the menu. The LLDP Neighbors Information window is shown in Figure 122. The table columns are described in Table 96.

Table 96. LLDP Neighbors Information Window

Column	Description
Entity	The number the switch assigned to the reporting neighbor in the order it received the LLDP information.
Port	The port number that received the LLDP information.
Chassis ID Subtype	The Chassis ID subtype of the neighboring network device.
Chassis ID	The Chassis ID of the neighboring network device. For Allied Telesis products, Chassis ID is the device's MAC address.
Port ID Subtype	The Port ID subtype of the port on the neighboring network device port.
Port ID	The port number on the neighboring network device port
Port Description	The description of the neighboring port.
Show Detail	Click the button to display a detailed report on the neighboring port.

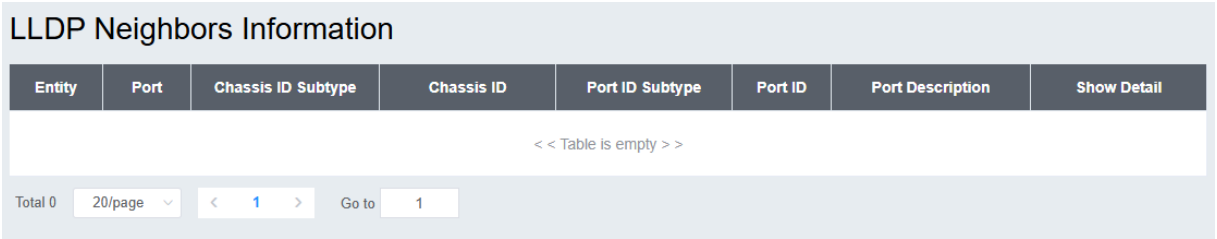


Figure 122. LLDP Neighbors Information Window

Chapter 40

MAC VLANs

Description and Procedure

Memberships of network devices in MAC VLANs are determined by the MAC addresses of the devices themselves. This is in contrast to other forms of VLANs, such as IEEE 802.3ac tagged VLANs, where VLAN memberships are determined by the VLAN identifiers (VIDs) in the packet headers.

When the switch receives packets from members of MAC VLANs, it examines the MAC addresses in the headers and automatically directs them to the preassigned VLANs, regardless of the physical port connections of the devices on the switch.

MAC VLANs can play an important role with ports that are used by different devices at different times. Rather than you having to reconfigure VLANs whenever ports are used by different devices, a switch with MAC VLANS can automatically direct the traffic from the devices to their appropriate VLANs based on their MAC addresses.

Creating a MAC VLAN has two basic steps:

1. Create a tagged VLAN. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.

2. Assign the MAC addresses of the devices to the VLAN, explained in “Managing MAC VLANs” on page 398.

Managing MAC VLANs

To manage MAC VLANs, select **Network** > **MAC VLAN** from the menu. The MAC VLAN window is displayed. Refer to Figure 123 on page 399.

- To add MAC addresses to a MAC VLAN, configure the window by referring to Table 97 and click the **Add** button.
- To modify MAC address entries, click the corresponding **Modify** button in the MAC VLAN Table, edit the values in Table 97, and click the **Apply** button.
- To delete MAC address entries, click the corresponding **Delete** button.
- To delete a MAC VLAN, refer to “Deleting 802.1Q Tagged VLANs” on page 351.

Note
Select **Save** from the menu to save your changes.

Table 97. MAC VLAN Window

Setting	Description
MAC Address	Enter the MAC address of a device. You can enter only one address at a time. You cannot enter a range or addresses. You can enter the addresses with or without dashes or colons: - nnnnnnnnnnnn - nn-nn-nn-nn-nn-nn - nn:nn:nn:nn:nn:nn
Description	Enter a description of the device or user. The description can contain up to eight alphanumeric characters. Spaces are permitted.
VLAN ID	Enter the ID number of the VLAN, You can enter only one VLAN ID. The VLAN must already exist on the switch. To view existing VLANs, refer to “Viewing All 802.1Q Tagged VLANs” on page 352.

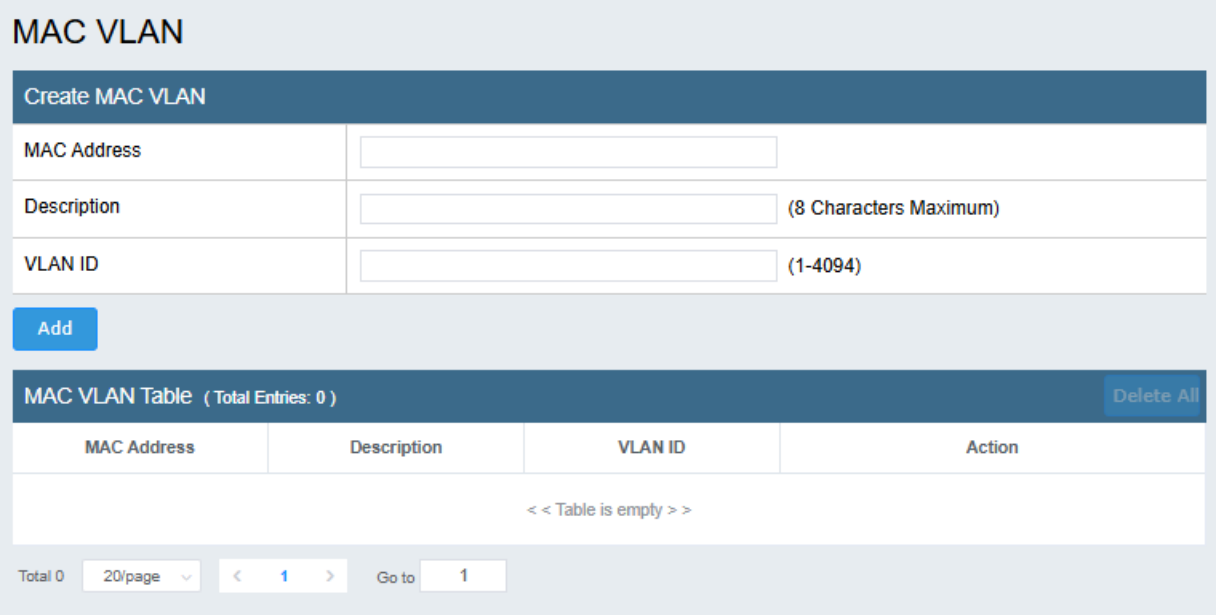


Figure 123. MAC VLAN Window

Chapter 41

Protocol VLANs

Introduction

As its name impllies, Protocol VLANs are VLANs dedicated to handling packets belonging to specified protocols. The switch examines and identifies the protocols of ingress packets and forwards them to defined VLANs according to pre-established profiles.

A protocol VLAN consist of these components:

- One or more tagged VLANs. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.
- Protocol VLAN Profile - Identifies a protocol, which can be Ethernet II, SNAP, or LLC, and an EtherType value, from 0000 to FFFF. The switch supports up to eight profiles. Each profile can identify one protocol and EtherType value. Refer to “Managing Protocol VLAN Profiles” on page 402
- Protocol VLAN Profile Interface - Identifies the ingress/egress port of the traffic, the protocol as specified by a Protocol VLAN Profile, and the tagged VLAN. Refer to “Managing VLAN Profile Interfaces” on page 404.

The components have to be generated in the order listed above.

Managing Protocol VLAN Profiles

Protocol VLAN Profiles identify the protocols of protocol VLANs. The protocol can be one of the following, plus an EtherType value:

- Ethernet II
- SNAP
- LLC

The switch supports a maximum of eight profiles.

To add a Protocol VLAN Profile to define the protocol of a protocol VLAN:

1. Select **Network** > **Protocol VLAN** > **Profile** from the menu to display the Protocol VLAN Profile window. Refer to Figure 124.

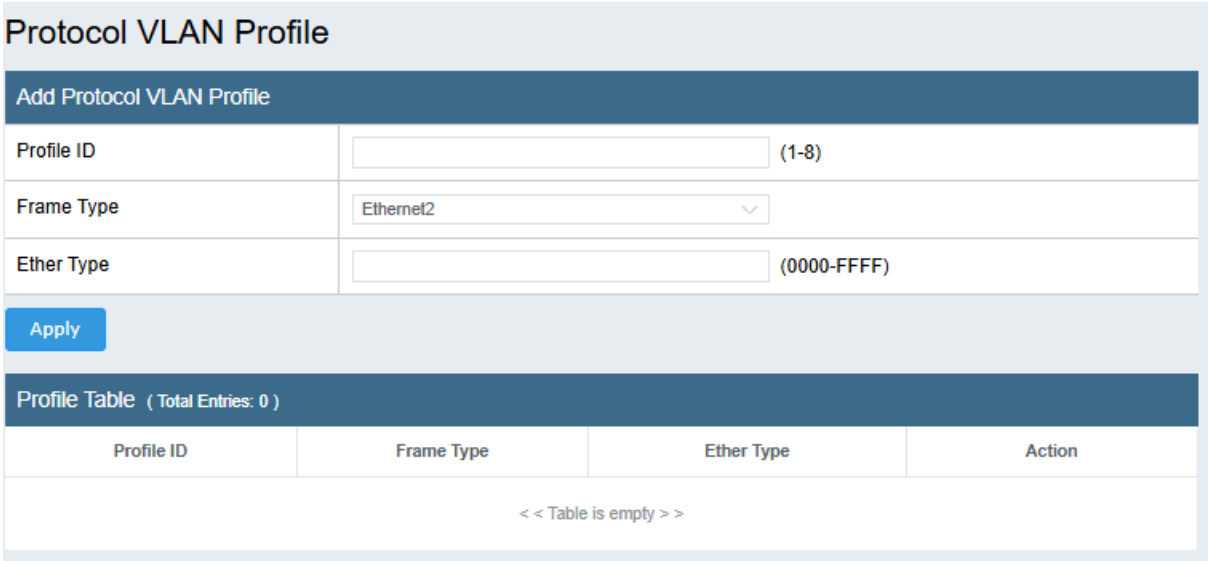


Figure 124. Protocol VLAN Profile

2. Configure the window options by referring to Table 98.

Note
You cannot modify a profile. To edit a profile, you must delete and recreate it.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 98. Protocol VLAN Profile Window

Setting	Description
Profile ID	Assign a unique ID number to the profile. The range is 1 to 8.
Frame Type	Select the frame type that corresponds to the protocol of the VLAN. Options are: ❒ Etherner2 (Ethernet II) ❒ SNAP ❒ LLC A profile can have only one frame type, but the same frame type can be applied to multiple profiles by assigning different EtherType values to the frame types.
Ether Type (EtherType)	Specifies the EtherType valve of a protocol. The range is 0000 to FFFF. A profile must include one EtherType value.

Managing VLAN Profile Interfaces

This procedure adds Protocol VLAN Profile Interfaces. An interface matches a Protocol VLAN Profile, which defines the designated protocol, with a tagged VLAN. The procedure requires the following;

- Tagged VLAN - refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337
- Protocol VLAN Profile - refer to “Managing Protocol VLAN Profiles” on page 402

Note
A protocol VLAN is activated when the Protocol VLAN Profile Interface is created.

To add a Protocol VLAN Profile Interface to match a Protocol VLAN Profile with a tagged VLAN:

1. Select **Network** > **Protocol VLAN** > **Profile Interface** from the menu to display the Protocol VLAN Profile window. Refer to Figure 124.

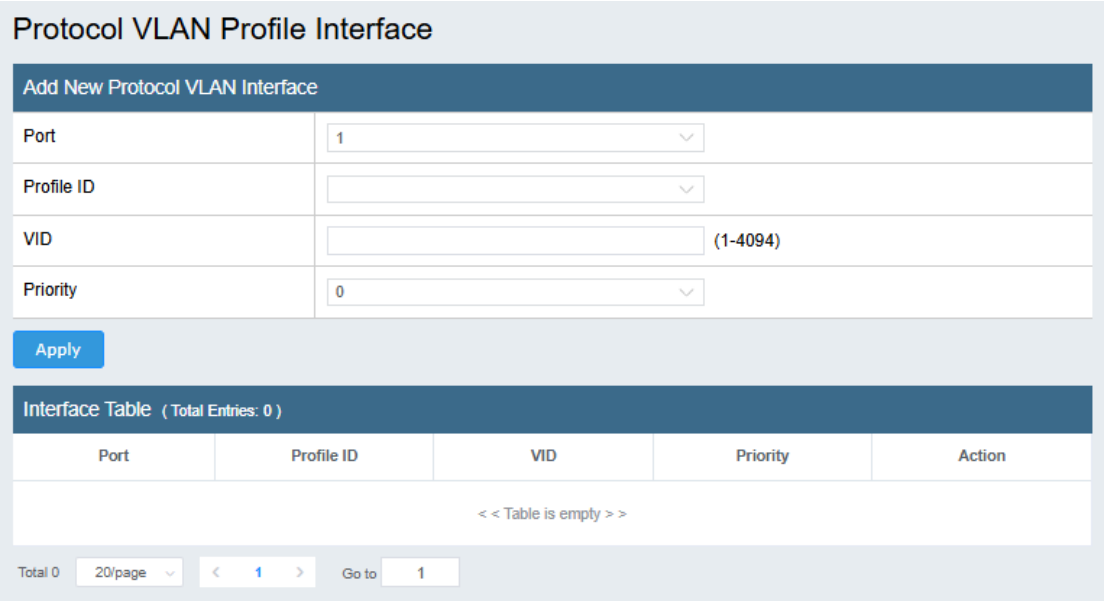


Figure 125. Protocol VLAN Profile Interface

2. Configure the window options by referring to Table 98 on page 403.

Note
You cannot modify Protocol VLAN Profile Interfaces. To correct or change an interface, you must delete and recreate it.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 99. Protocol VLAN Profile Interface Window

Setting	Description
Port	Select a port on the switch from the pull-down menu to attach the profile ID and protocol VLAN. You can select only one port per interface, but you can assign multiple profiles and VLANs to the same port by adding multiple interfaces.
Profile ID	Select the ID of a Protocol VLAN Profile from the pull-down menu. You can select only one Protocol VLAN Profile per Protocol VLAN Profile Interface, and the Protocol VLAN Profile must already exist. Refer to “Managing Protocol VLAN Profiles” on page 402.
VID	Displays the VID of the tagged VLAN for the protocol VLAN. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337
Priority	Displays which Protocol VLANs Profile Interface takes precedence if there are opposing protocol VLANs. The lower the value, the higher the priority.

Section IV

Quality of Service Menu

This section contains the following chapter:

- Chapter 42, “Quality of Service and Class of Service” on page 409

Chapter 42

Quality of Service and Class of Service

This chapter describes the Quality of Service (QoS) and Class of Service (CoS) features in the following sections:

- ❒ “QOS and COS Overview” on page 410
- ❒ “Mapping CoS Priorities to Egress Queues” on page 414
- ❒ “Mapping CoS Priorities to Ports” on page 416
- ❒ “Mapping DSCP Classes to Egress Queues” on page 417
- ❒ “Setting the Queue Scheduling Algorithm” on page 418
- ❒ “Mapping IPv6 Traffic Classes to Port Egress Queues” on page 419

QOS and COS Overview

Class of Service (CoS) is used to assign network packets to port egress queues in the switch based on their priority levels. The switch uses CoS to prioritize transmission of network packets, giving higher priority to designated packets, such as delay sensitive traffic, over other packets.

When a port on an Ethernet switch becomes oversubscribed, its egress queues contain more packets than the port can handle in a timely manner. When this happens, a port may be forced to delay the transmission of some packets, resulting in the delay of packets reaching their destinations. A port may be forced to delay transmission of packets while it handles other traffic, and, in some situations, some packets destined to be forwarded to an oversubscribed port from other switch ports may be discarded.

Minor delays are usually of no consequence to a network or its performance. But there are applications, referred to as delay or time-sensitive applications, that can be impacted by packet delays. Voice transmission and video conferences are two examples. The audio or video quality may suffer if packets carrying their data are delayed from reaching their destinations.

The topics of CoS are:

- ❒ “Packet Priority” next
- ❒ “Egress Queue vs Packet Priority Mapping” on page 411
- ❒ “Prioritizing Untagged Packets” on page 412
- ❒ “Scheduling Algorithm” on page 412

Packet Priority

CoS applies primarily to tagged packets. Tagged packets contain information that specifies the VLANs to which they belong. Tagged packets can also contain priority levels that are used by network switches and other networking devices to know how important (delay sensitive) packets are compared to other packets. Packets with high priorities are handled before packets with low priorities.

CoS, as defined in the IEEE 802.1p standard, has eight priority levels. The priority levels are 0 to 7, with 0 the lowest and 7 the highest priority.

When tagged packets are received on ports, the switch examines them for their priorities. It uses the priorities to determine which egress queues the packet should be directed to on the egress ports.

Egress Queue vs Packet Priority Mapping

Each port has four egress queues, labeled as follows:

- 0 = Low
- 1 = Medium
- 2 = High
- 3 = Highest

Low is the lowest priority queue and Highest is the highest. Packets in high-priority egress queues are usually transmitted before packets in low-priority queues. Table 100 lists the default mappings of the eight CoS priority levels and the four egress queues of the switch ports.

Table 100. Default Mappings Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0

You can change these mappings. For example, you might decide that packets with priority 4 or 5 should be handled in the High egress queues while packets with a priority of 6 or 7 should be handled in the Highest egress queues. The result is shown in Table 101.

Table 101. Example of Customized Mappings Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	0
1	0
2	0
3	0

Table 101. Example of Customized Mappings Priority Levels to Priority Queues (Continued)

IEEE 802.1p Priority Level	Port Priority Queue
4	2
5	2
6	3
7	3

The procedure for changing the default mappings is found in “Mapping CoS Priorities to Ports” on page 416. These mappings are applied at the switch level. All ports use the same priority-to-egress queue mappings.

You can also map an IPv6 packet header’s 8 bit priority field, used by the switch to differentiate between classes or priorities of IPv6 ports, to one of the switch’s priority queues. The procedure is found in “Mapping IPv6 Traffic Classes to Port Egress Queues” on page 419.

The switch does not change the priority levels in tagged packets. It transmits them from the egress ports with the same priority levels they had when they were received. This is true even if you change the default priority-to-egress queue mappings.

Prioritizing Untagged Packets

Unlike tagged packets, untagged packets do not contain priority values, but they can still be prioritized by the switch. Priority values are assigned to untagged packets by their ingress ports. Each port has a priority value for ingress untagged packets. As untagged packets arrive on a port, the switch assigns them the port’s priority value. The priority determines the queue untagged packets are placed in on the egress ports. The default priority value for ingress untagged packets is “0”, which places them in the Low priority queue. You can change the setting as described in “Mapping CoS Priorities to Ports” on page 416.

Scheduling Algorithm

The switch has a process for controlling the order in which it transmits packets from the four egress queues of ports. The process is called the scheduling algorithm. The switch uses scheduling to determine the order in which ports handle the packets in their egress queues. For example, if all the queues of a port contain packets, the switch uses the process to determine whether to transmit all the packets from the highest (the highest priority queue) before moving on to the other queues, or transmit a few packets from each queue in a sequential fashion.

The switch has two types of scheduling:

- Strict priority
- Weighted round robin priority

To specify the scheduling, refer to “Mapping CoS Priorities to Ports” on page 416.

Note
Scheduling is set at the switch level and applies to all ports.

Strict Priority Scheduling

With strict priority scheduling, ports transmits all packets out of higher priority queues before transmitting any from the lower priority queues. For instance, as long as there are packets in the Highest queues, they do not handle any packets in the High queues. The value of this type of scheduling is that high-priority packets are always handled before low-priority packets which is required for voice or video data.

The problem with this method is that some low-priority packets might never be transmitted from the switch. This can happen if higher priority queues always contain packets because of high traffic volume.

Weighted Round Robin Priority Scheduling

The weighted round robin (WRR) scheduling method functions as its name implies. The port transmits a set number of packets from each queue, in a round robin fashion, so that each has a chance to transmit traffic. Normally, the higher a queue’s priority, the more packets are transmitted from it as compared to lower priority queues. This method guarantees that every queue receives some attention from the port for transmitting packets.

Table 102 shows the WRR settings for the number of packets transmitted from each queue. You cannot change these settings.

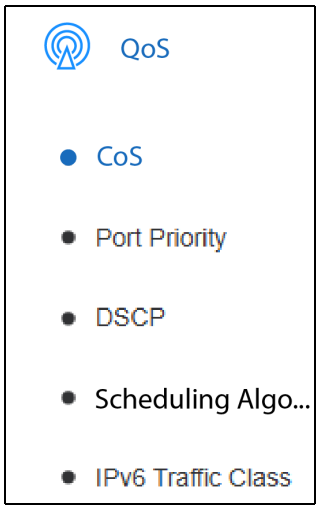
Table 102. Weighted Round Robin Priority

Port Egress Queue	Maximum Number of Packets
3 (Highest)	8
2 (High)	4
1 (Medium)	2
0 (Low)	1

Mapping CoS Priorities to Egress Queues

Note
CoS is not compatible with Jumbo frames. Before enabling CoS, disable Jumbo frames on all ports. Refer to Chapter 19, “Basic Port Settings” on page 191.

To change the mappings of CoS priorities to all port egress queues:



1. Select **QoS** > **CoS** from the menu. The CoS window is shown Figure 126 on page 415.
2. To enable or disable the mappings, select **Enabled** or **Disabled** from the CoS Status menu and click **Apply**. The feature has to be enabled for you to change the settings. The default is disabled.
3. To change the mapping of a traffic class priority to a port egress queue, select the new mapping from the corresponding egress Queue ID pull-down menu. The default for all traffic classes is the Low egress queue. The Queue IDs are:
   - ❒ 0 = Low
   - ❒ 1 = Medium
   - ❒ 2 = High
   - ❒ 3 = Highest
4. Click **Apply** to activate your changes.

Note
Select **Save** from the menu to save your changes.

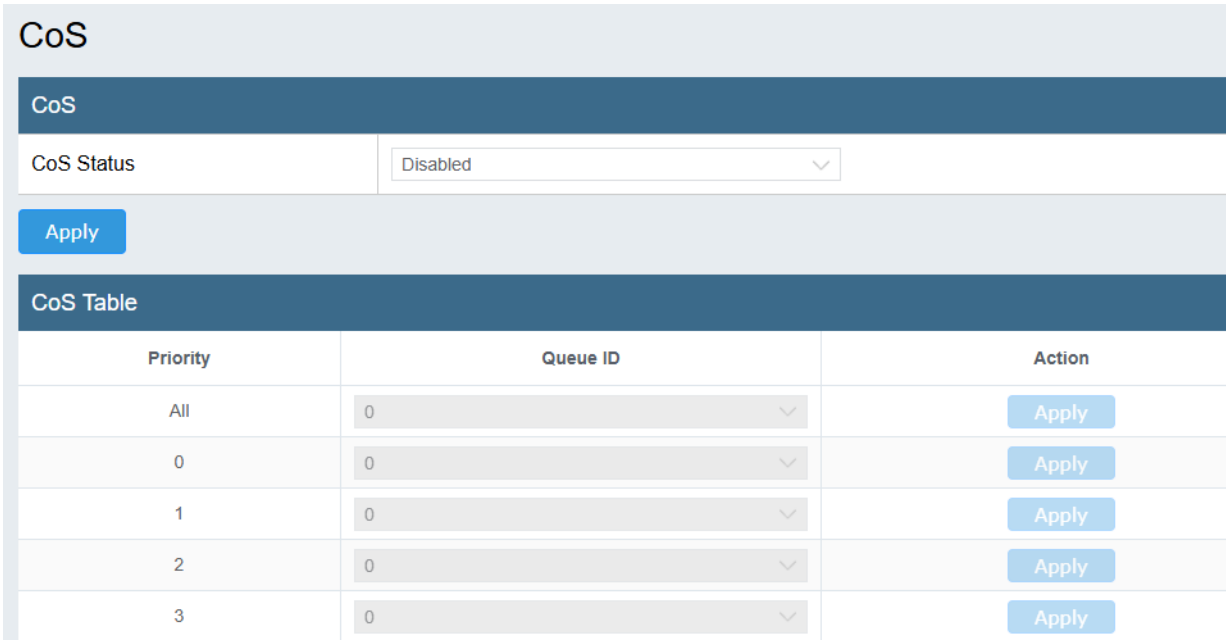
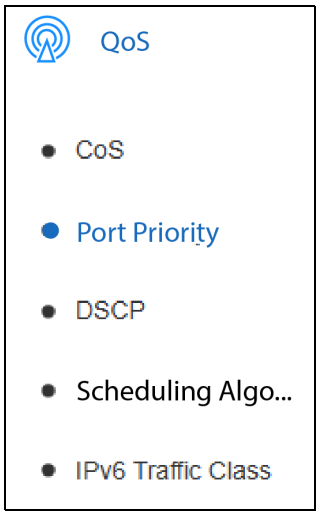


Figure 126. CoS Window

Mapping CoS Priorities to Ports

This procedure explains how to set the CoS port priority values on the individual ports on the switch. The switch assigns the priority values to ingress untagged packets. A port can have only one port priority value. The default setting is 0, which places untagged packets in the Low queue on egress ports. Refer to “Prioritizing Untagged Packets” on page 412.

To change the CoS port priority settings:



1. Select **QoS** > **Port Priority** from the menu. The Port Priority window is shown in Figure 127.
2. To change a port’s CoS priority, select the new value from the User Priority pull-down menu. The range is 0 (lowest) to 7 (highest). The default is 0.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

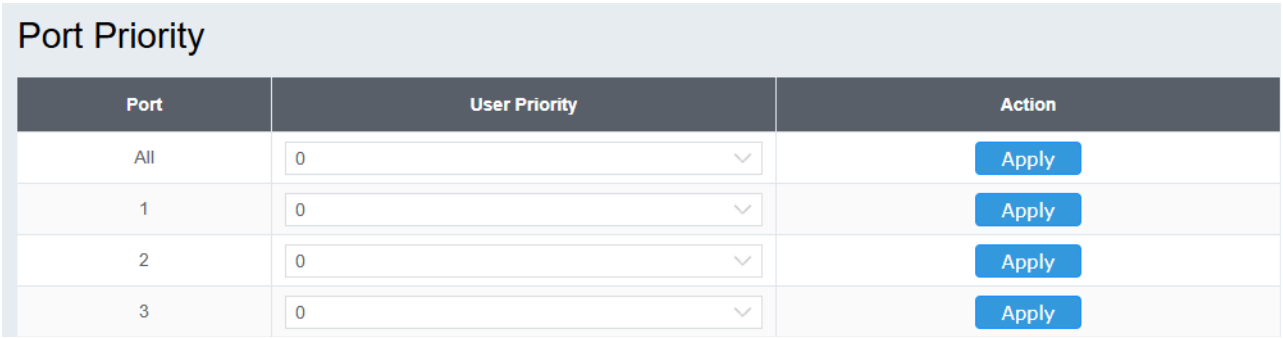


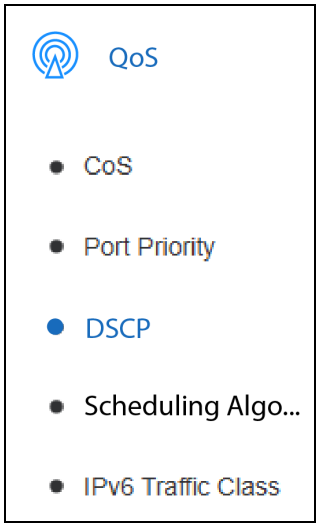
Figure 127. Port Priority Window

Mapping DSCP Classes to Egress Queues

This procedure explains how to map DSCP values (0-63) to port egress queues. The queue IDs are:

- 0 = Low
- 1 = Medium
- 2 = High
- 3 = Highest

The default queue for all DSCP values is Low. To map DSCP values to egress queues:



1. Select **QoS** > **DSCP** from the menu. The DSCP Class Mapping window is shown in Figure 128 on page 417.
2. Select **Enabled** or **Disabled** from the DSCP Mapping Status menu to enable or disable the mappings, and click **Apply**. The default is disabled. You must enable DSCP mappings to change the values.
3. To adjust the queue setting of a DSCP value, select the new queue ID from the pull-down menu and click **Apply** at the bottom of the window.

   To return the DSCP class mapping to the default values, click **Reset to Default**.

Note
Select **Save** from the menu to save your changes.

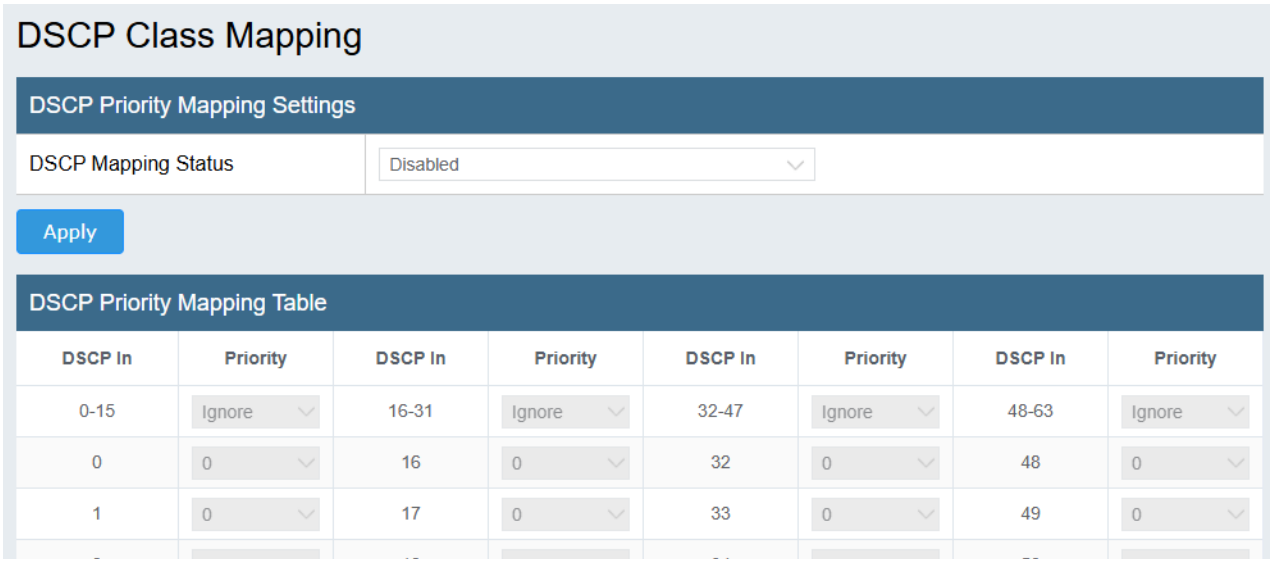
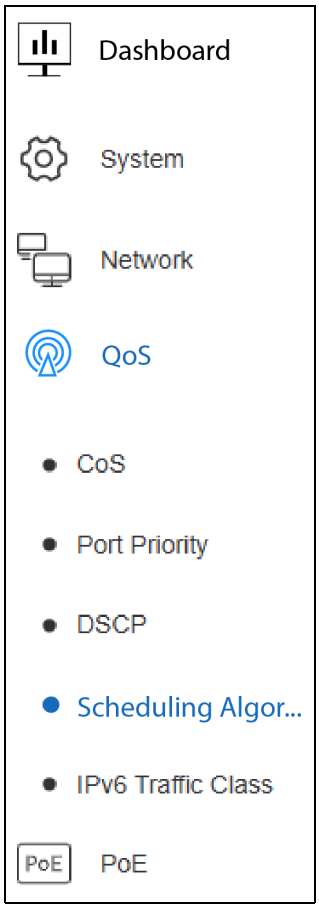


Figure 128. DSCP Class Mapping Window

Setting the Queue Scheduling Algorithm



This procedure explains how to set the scheduling algorithm. The switch uses the scheduling algorithm to control the order in which it transmits packets from a port's four egress queues. Refer to "Scheduling Algorithm" on page 412.

To change the scheduling algorithm for a port's egress queues:

1. Select **QoS** > **Scheduling Algorithm** from the menu. The Scheduling Algorithm window is shown in Figure 129.

2. From the Scheduling Algorithm pull-down menu, select one of the following algorithms and click **Apply**:

   - **Strict Priority** - The port transmits all packets out of higher priority queues before transmitting any from the lower priority queues. Refer to "Strict Priority Scheduling" on page 413. This is the default setting.
   - **Weighted Round Robin** - The port transmits a set number of packets from each queue, in a round robin, so that each has a chance to transmit traffic. Refer to "Weighted Round Robin Priority Scheduling" on page 413.

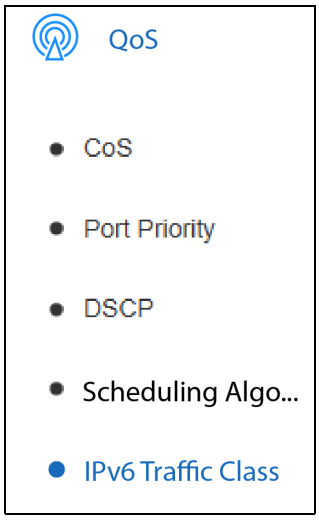
Note
Select **Save** from the menu to save your changes.

Figure 129. Scheduling Algorithm Window

Mapping IPv6 Traffic Classes to Port Egress Queues

Note
You cannot map IPv6 traffic class mapping to egress queues when Jumbo frames are enabled on ports. To disable Jumbo frames, refer to Chapter 19, “Basic Port Settings” on page 191.

To map IPv6 traffic classes to port egress queues:



1. Select **QoS** > **IPv6 Traffic Class** from the menu. The IPv6 Traffic Class Priority Settings window is shown in Figure 130 on page 420.
2. To enable or disable IPv6 traffic class priority mappings on the switch, select **Enabled** or **Disabled** from the State pull-down menu, and click **Apply**. You must enable the feature to change the values.
3. To add a new mapping, do the following:
   a. In the IPv6 Traffic Class field, enter a value for the IPv6 packet header’s 8 bit priority in the IPv6 Traffic Class field. The range is 0-255. You can enter only one value.
   b. With the Priority pull-down menu, select the priority level of the port egress queues for the packets. The values are:
      - ❒ 0 = Low
      - ❒ 1 = Medium
      - ❒ 2 = High
      - ❒ 3 = Highest
   c. Click **Apply**. The new mapping is added to the table.
   d. Repeat this step to add more mappings.
4. To delete IPv6 traffic class priority mappings, click **Delete** In the Action column to delete individual mappings or click **Delete All** to delete all entries.

Note
Select **Save** from the menu to save your changes.

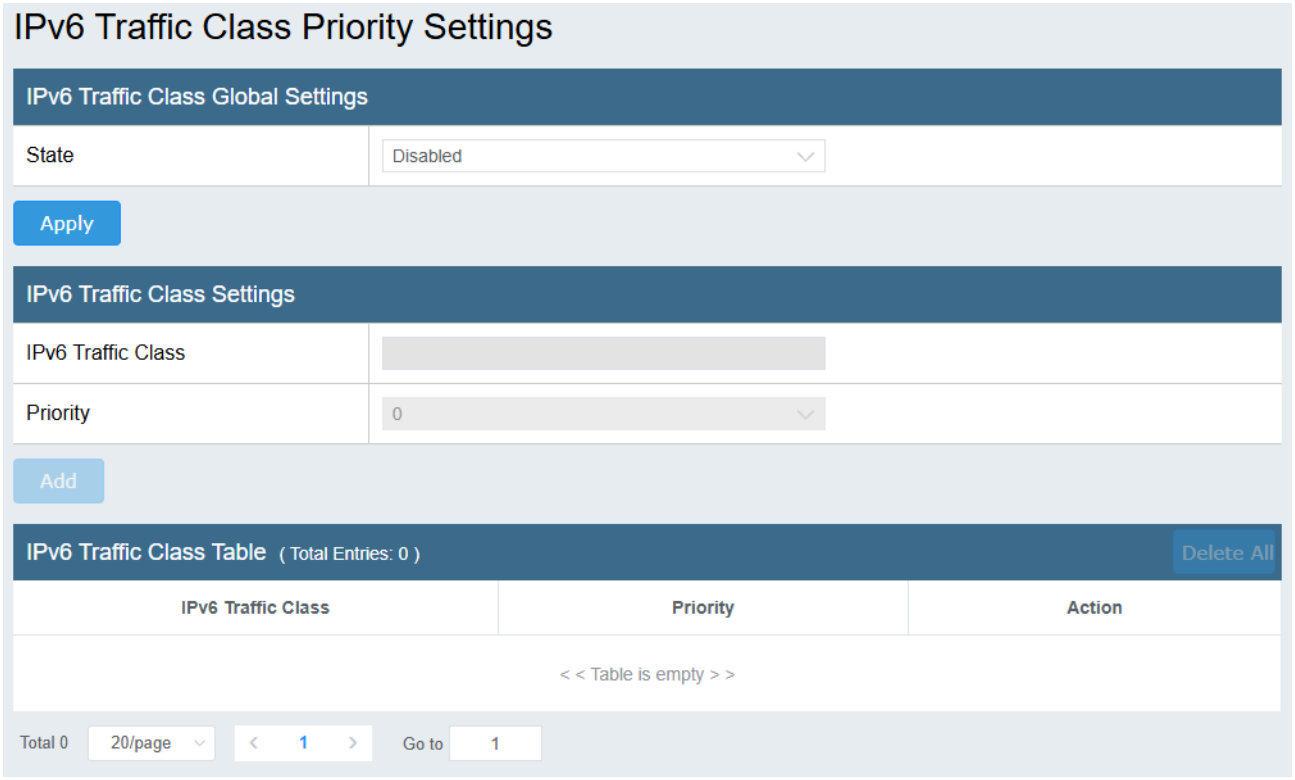


Figure 130. IPv6 Traffic Class Priority Settings Window

Section V

PoE Menu

This section contains the following chapter:

- Chapter 43, “Power over Ethernet” on page 423

Chapter 43

Power over Ethernet

This chapter describes PoE on the iGS950 Series in the following sections:

- “Overview” on page 424
- “Managing PoE” on page 428
- “Managing Time Range Power Schedules” on page 430

Overview

The iGS950 Series of Layer 2 Gigabit Ethernet Switches features PoE+ on the copper ports. This feature enables the switches to supply power to network devices over the same cables that carry the network traffic. The value of PoE+ is that it can make it easier to install networks. Selecting locations for network devices are often limited by whether there are power sources nearby. This often limits equipment placement or requires the added time and cost of having additional electrical sources installed. But with PoE+, you can install PoE-compatible devices wherever they are needed without having to worry about whether there are adjacent power sources.

A device that provides PoE+ to other network devices is referred to as *power sourcing equipment* (PSE). The switches in the iGS950 Series act as PSE units by adding DC power on the network cables connected to its ports, thus functioning as a power source for other network devices.

Devices that receive their power from a PSE are called *powered devices* (PD). Examples include wireless access points, IP telephones, webcams, and even other Ethernet switches.

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

PoE+ Ports

Table 103 lists the ports that support PoE+ on the switches.

Table 103. PoE+ Ports

Switch	PoE+ Ports
AT-iGS950/10PS	1 to 8
AT-iGS950/20PS	1 to 16
AT-iGS950/28PS	1 to 24
AT-iGS950/52PS	1 to 48

Note
PoE+ is not supported on the combo copper ports on the AT-iGS950/20PS, AT-iGS950/28PS, and AT-iGS950/52PS Switches. Refer to Table 7 on page 40 for the combo port numbers.

Maximum PoE+ Power Budget

The maximum PoE+ power budget is the maximum amount of power the switches have for powered devices on their ports. Table 104 lists the maximum PoE+ power budgets for the switches.

Table 104. PoE+ Maximum Power Budgets

Switch	PoE+ Maximum Power Budget
AT-iGS950/10PS	130W
AT-iGS950/20PS	370W
AT-iGS950/28PS	370W
AT-iGS950/52PS	740W

PoE+ Standards

The iGS950 Series supports the PoE standards listed in Table 105.

Table 105. PoE Standards

PoE Standard	IEEE Standard	Definition
PoE	IEEE 802.3af, IEEE 802.3at Type 1	Supplies up to 15.4 watts at switch ports for powered devices requiring up to 12.95 watts.
PoE+	IEEE 802.3at Type 2	Supplies up to 30.0 watts at switch ports for powered devices requiring up to 25.5 watts.

Powered Device Classes

Powered devices are grouped into classes, based on their power requirements. The iGS950 Series supports the five classes in Table 106.

Table 106. IEEE Powered Device Classes Supported by the iGS950 Series

Class	Maximum Power Output at the Switch Port	Powered Device Power Range
0	15.4W	0.44W to 12.95W
1	4.0W	0.44W to 3.84W
2	7.0W	3.84W to 6.49W
3	15.4W	6.49W to 12.95W
4	30.0W	12.95W to 25.5W

Note
The iGS950 Series can support any combination of powered devices, up to the maximum PoE power budgets. Refer to Table 104 on page 425.

Mode A Power Delivery

The PoE IEEE 802.3at standard defines two modes for delivering power over copper cables from a PSE, such as the iGS950 Series, to PDs. The two modes define the pins on the RJ-45 copper ports of the PSE that supply power to the PDs.

The modes are called Mode A and Mode B, In Mode A, the PSE use pins 1, 2, 3, and 6 on its copper ports to supply power over the copper cables to the PDs. In Mode B, the PSE uses pins 4, 5, 7, and 8 on its copper ports as the power output.

The iGS950 Series supports Mode A of the IEEE 802.3at standard. The switches use pins 1, 2, 3, and 6 on copper ports to deliver power to PDs.

Most PDs are designed to support both modes. However, older PDs might support only one mode. You should review the documentation included with your PDs before connecting them to the switches to confirm that they support both modes. If they are older units that support only one mode, they must support Mode A to be compatible with the iGS950 Series

Note
Older PDs that only support Mode B are not compatible with the iGS950 Series.

PoE Port Priorities

If the power requirements of the powered devices exceed the switch's power budget, the switch will deny power to some ports based on a system called PoE+ port priorities. You can use this feature to ensure that powered devices critical to the operations of your network or business are given preferential treatment by the switch in the allocation of power should the demands of the devices exceed the available power.

There are three priority levels:

- Critical
- High
- Low

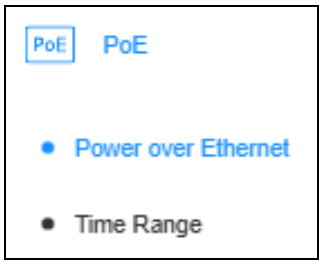
Ports set to the Critical level, the highest priority level, are guaranteed power before any of the ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all the Critical ports are receiving power. Ports that are connected to your most critical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

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

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

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

Managing PoE



This section has the procedure for configuring PoE on the individual ports on the switch. To manage PoE:

1. Select **PoE** > **Power over Ethernet** from the menu. The Power over Ethernet window is shown in Figure 131 on page 429. The window has two parts:
   - ❒ Power over Ethernet Settings: This section displays the power budget of the switch and the power consumption of the active powered devices. Refer to Table 107.
   - ❒ Power over Ethernet Table: This section is used to configure the PoE settings on the individual switch ports and to view current settings.

Table 107. Power over Ethernet Settings

Row	Description
Power Budget	Displays the switch's maximum PoE power budget in watts. This value is not adjustable.
Power Consumption	Displays the current power in watts supplied by the switch to active powered devices on its ports.

2. To configure PoE on the individual ports, refer to Table 108.

Table 108. Power over Ethernet Table

Column	Description
Port	Lists the port numbers.
Admin	Enables or disables PoE on a port. The default is enabled.
Status	Displays the current status of PoE on a port: - POWER ON: The switch is supplying power to a powered device on the port. - POWER OFF: The switch is not supplying power to a powered device.
Class	Displays the class (0 to 4) of the powered device. Refer to "Powered Device Classes" on page 425.
Priority	Displays the Critical, High, Low priority of a port. Refer to "PoE Port Priorities" on page 426.

Table 108. Power over Ethernet Table (Continued)

Column	Description
Power Limit	Displays the power limit of a port by class or by user defined value.
User Def	Defines the power limit, in watts. To set this value, set Power Limit to UserDef.
Time Range	To apply a power schedule to the port to define the days and times when the switch supplies power on the port, select the schedule from the pull-down menu. Refer to “Managing Time Range Power Schedules” on page 430. The default is N/A, meaning PoE is always available on a port.

3. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

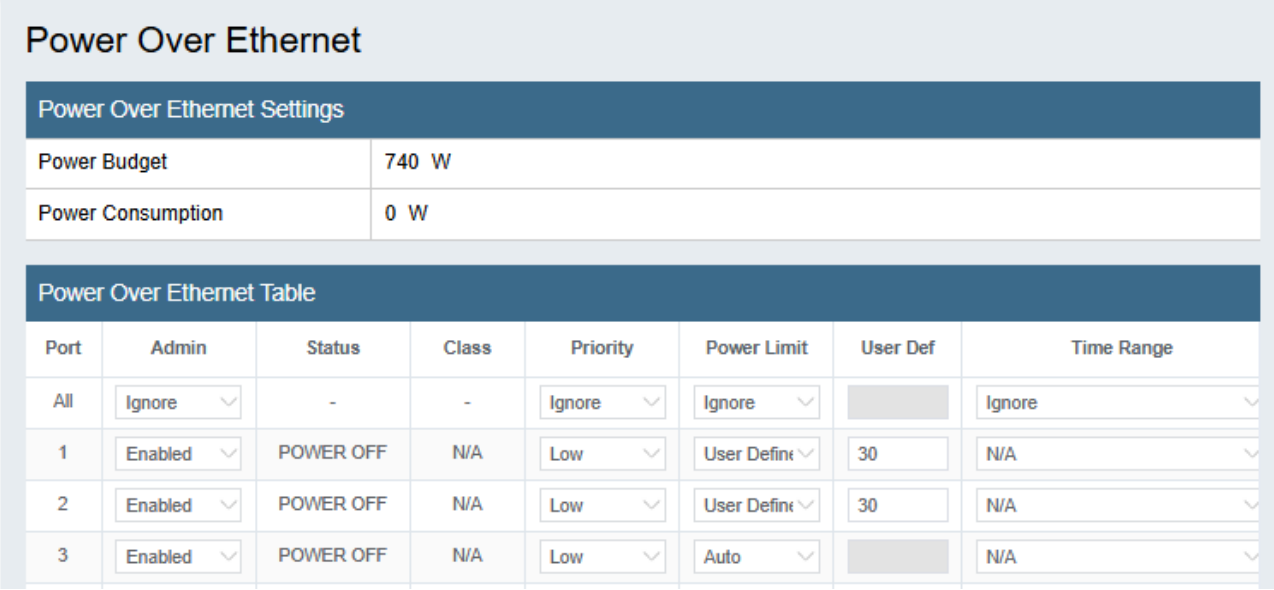


Figure 131. Power Over Ethernet Window

Managing Time Range Power Schedules

You can control the days and times when the switch supplies power to the powered devices on its ports by adding time range power schedules. Power schedules define the days and times when the switch BLOCKS power on a port. Schedules are optional. Schedules can span entire weeks or specific days, and can include starting and ending times. Schedules are applied to individual ports so that different ports can have different schedules, allowing you to restrict power delivery to ports by the switch depending on the various work requirements of the end users.

Please review the following guidelines:

- Time range power schedules define the days and times when the switch BLOCKS power to a port. At all other times, the switch supplies power to a port.
- Ports without schedules always receive power from the switch, depending, orf course, on the power requirements of the powered devices and available power reserves.
- Power schedules do not affect the network functionally and availability of ports. To disable network functionality on a port, disable the port. Refer to Chapter 19, “Basic Port Settings” on page 191.

Adding a Power Schedule

To add a time range power schedule:

1. Select **PoE** > **Time Range** from the menu. The Time Range window is shown in Figure 132 on page 432. The window has two parts:
   - Time Range: This section is used to add new schedules.
   - Time Range Table: This section lists the existing schedules.
2. To add a new schedule, enter the values in Table 109.

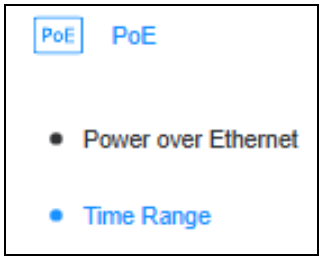


Table 109. Time Range Window

Field	Description
Range Name	Assign a unique name of up to 32 alphanumeric characters to the schedule.
Daily box	Check this box if the schedule is to apply to all seven days of the week. Checking this box disables the From Week and To Week selections.
From Week	Select the starting weekday of the schedule from the pull-down menu. The default is Sunday.

Table 109. Time Range Window (Continued)

Field	Description
To Week	Select the ending weekday of the schedule from the pull-down menu. The default is Sunday.
End Weekday box	Check this box to apply the schedule to only one day of the week, specified in From Week. For example, if From Week specifies Thursday, checking this box restricts the schedule to Thursdays only.
From Time (HH:MM)	Specify the start time of the schedule. This time specifies when the switch is to start blocking power on a port. The time is entered in 24-hour format with the pull-down menus. For example, if the switch is to start blocking power at 5:45 PM, enter 17 (HH) and 45 (MM).
To Time (HH:MM)	Specify the ending time of the schedule. This time controls when the switch is to resume supplying power on a port. The time is entered in 24-hour format with the pull-down menus. For example, to resume power at 8:30 AM, enter 08 (HH) and 30 (MM).

3. Click **Apply**.

Note
Click **Save** in the menu to save your changes.

4. To add the power schedule to switch ports, perform “Managing PoE” on page 428.

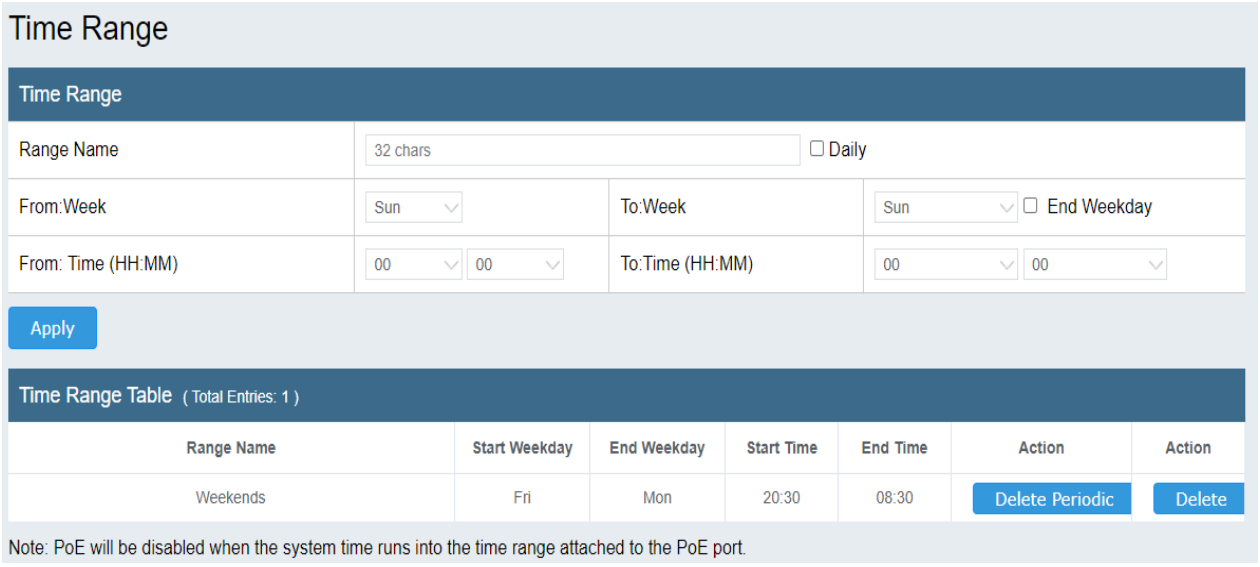


Figure 132. Time Range Window

Editing a Power Schedule

You cannot edit a power schedule. To change a schedule, you mist delete it and reenter it.

Deleting a Power Schedule

To delete a power schedule, click the **Delete** button.

Note
You cannot delete a schedule that is applied to a port. You must remove it from all its port assignments first. Refer to “Managing PoE” on page 428.

Section VI

Security

This section contains the following chapters:

- Chapter 44, “Port Security” on page 435
- Chapter 45, “Port Authentication” on page 443
- Chapter 46, “Local Dial-in User Accounts” on page 465
- Chapter 47, “RADIUS Client” on page 471
- Chapter 48, “TACACS+ Client” on page 477
- Chapter 49, “Destination MAC Address Filters” on page 483
- Chapter 50, “Denial of Service” on page 487
- Chapter 51, “DHCP Snooping” on page 491
- Chapter 52, “Traffic Rules and Policies” on page 507

Chapter 44
Port Security

This chapter describes the local dial-in user accounts feature in the following sections:

- “Port Security Overview” on page 436
- “Configuring the Global Setting for the Maximum Number of MAC Addresses” on page 437
- “Configuring Port Security” on page 438
- “Configuring Port and VLAN Security” on page 441

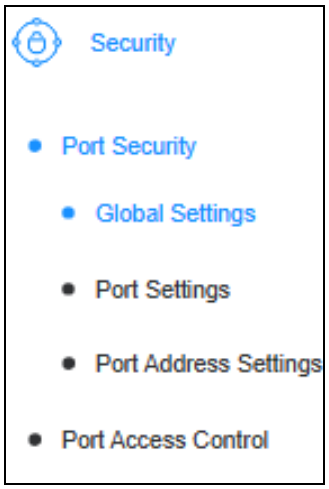
Port Security Overview

The iGS950 Series has the following port security features:

- You can set a maximum number for static and dynamic MAC addresses the switch can learn, and so limit the number of devices that can use the switch to access your network. Refer to “Configuring the Global Setting for the Maximum Number of MAC Addresses” on page 437.
- You can enable and disable individual ports and set limits on the number of supported dynamic and static MAC addresses on a per port basis. Refer to “Configuring Port Security” on page 438.
- You can configure ports to only support specific devices and specify the VLANs they can access. Refer to “Configuring Port and VLAN Security” on page 441

Configuring the Global Setting for the Maximum Number of MAC Addresses

This feature allows you to set the maximum number of static and dynamic MAC addresses the switch supports. After reaching the maximum number, the switch blocks systems with new MAC addresses from forwarding traffic through its ports.



To set the maximum number of permitted static and dynamic MAC addresses the switch supports:

1. Select **Security** > **Port Security** > **Global Settings** from the menu. The Port Security Global Settings window is shown in Figure 133.
2. In the System Maximum Address (1 - 6656) field, do one of the following options:
   - ❒ Option 1: Click the No Limit dialog box if there is to be no limit of MAC addresses. This is the default setting.
   - ❒ Option 2: Enter a value from 1 to 6656 MAC addresses in the System Maximum Address field.

Note
The number entered for option Option 2 must be greater than the sum of the settings of maximum MAC address set on the individual ports in “Configuring Port Security” on page 438. For example, if the individual ports on a ten port switch are configured to learn no more than five addresses, than the value for the global setting must be greater than 50 MAC addresses.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

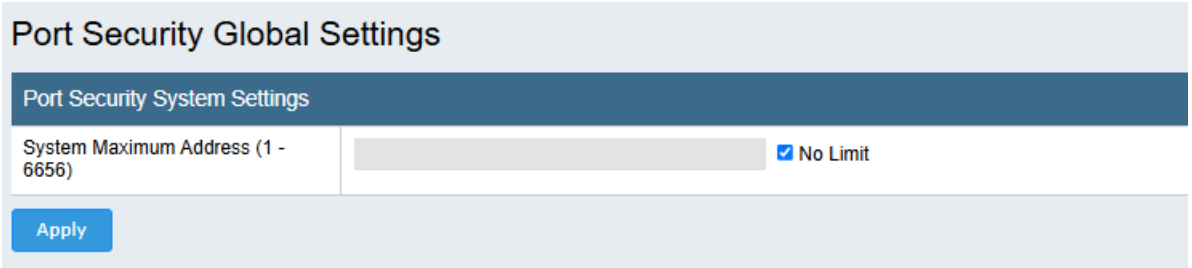


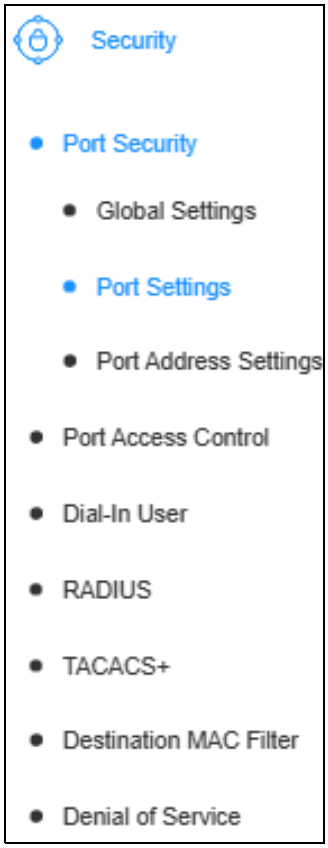
Figure 133. Port Security Global Settings Window

Configuring Port Security

This section describes the following security functions that can be set on the individual ports:

- Port state: enabled or disabled
- Maximum number of static and dynamic MAC addresses
- Violation action if a port exceeds its maximum MAC addresses
- Time duration of violation action

To configure port security:



1. Select **Security** > **Port Security** > **Port Settings** from the menu. The Port Security Port Settings window is shown in Figure 134 on page 440.
2. Configure the settings in Table 110.

Table 110. Port Security Port Settings Window

Field	Description
Port	Select the port you want to configure from the pull-down menu. You can configure only one port at a time or all ports with the All option.
State	Set the optional state of the port: ❒ Enabled - The port forwards ingress and egress traffic. ❒ Disabled - The port blocks all ingress and egress traffic.
Maximum (1 - 64)	Specify the maximum number of static and dynamic MAC addresses a port will support.
Violation Action	Set the violation action if a port exceeds its maximum number of MAC addresses. Violation actions are: ❒ Protect: The port stops accepting new static and dynamic MAC addresses while continuing to forward traffic from devices with MAC addresses it has already learned. This is the default value. ❒ Shutdown: The port's state is changed to disabled, blocking all ingress and egress traffic.

Table 110. Port Security Port Settings Window (Continued)

Field	Description
Security Mode	Specifies the duration of the action ❒ Delete-on-Timeout: The violation action times out in accordance with the Aging Time and Aging Type parameters. This is the default value. ❒ Permanent: The violation action remains permanent, until intervention by the network administrator.
Aging Time (0-1440)	Specifies the time duration for the violation action when the Security Mode is set to Delete-on-Timeout. The range is 0 to 1440 minutes. The value 0 disables the timer, in which case there is no timeout.
Aging Type	Specify the type of timer: ❒ Absolute: The aging timer is active whether the port is active or inactive. This is the default value. ❒ Inactivity: The aging timer is active only when the port is inactive.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

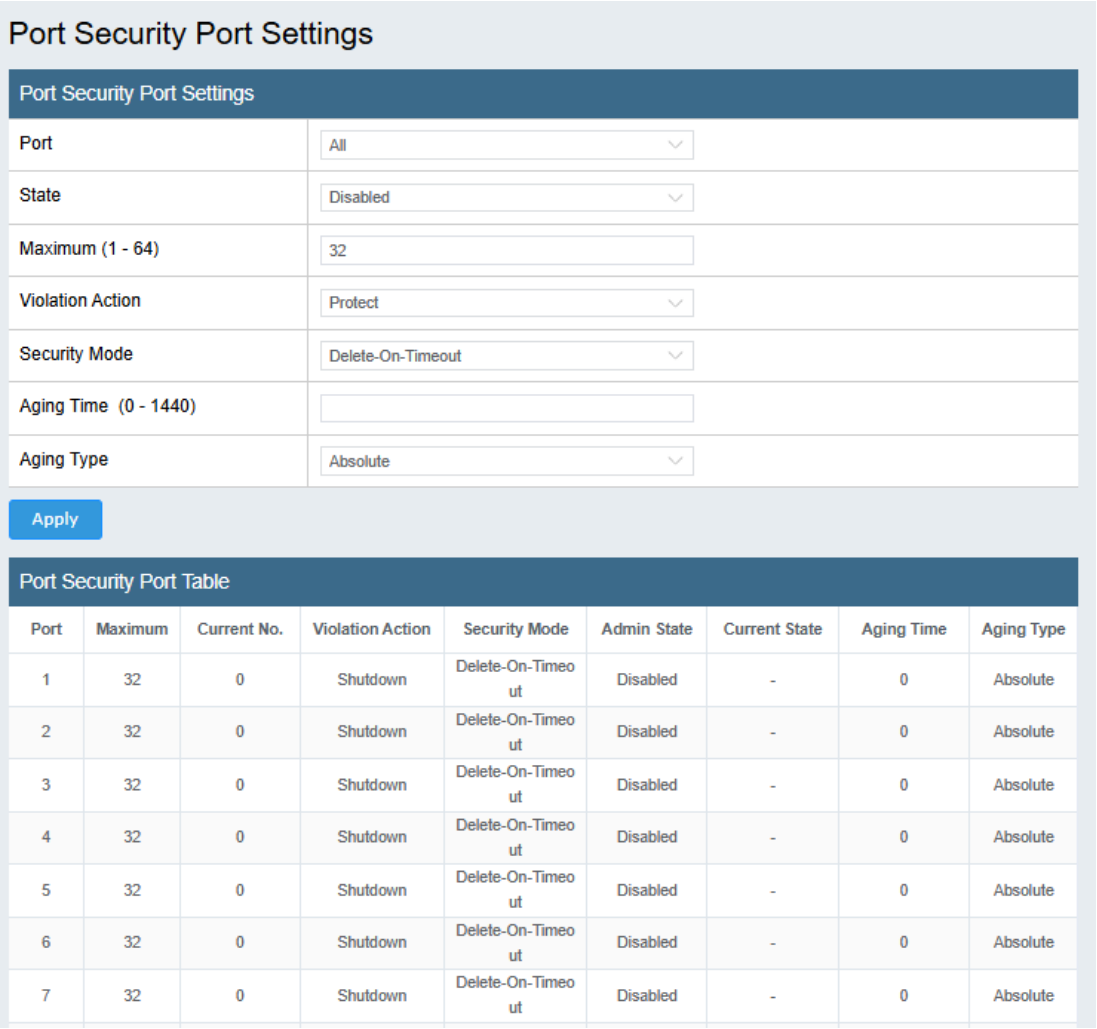


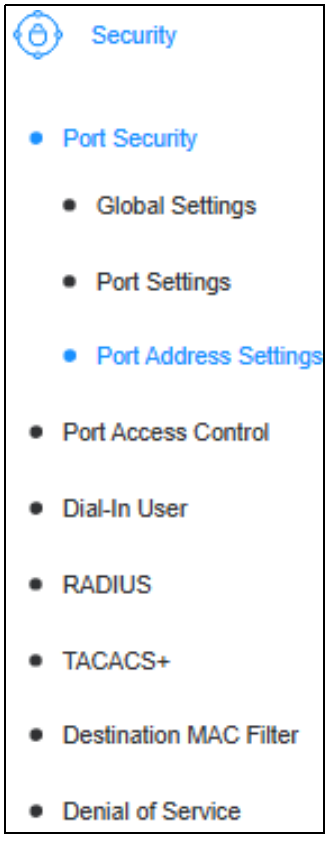
Figure 134. Port Security Port Settings Window

Configuring Port and VLAN Security

This section describes the following port security features on the switch:

- Configure ports to support only specified network devices, identified by their MAC addresses.
- Specify the VLANs that network devices can access through the ports.

Note
This feature can be used together with “Configuring Port Security” on page 438 to specify a violation action in the event an unauthorized device attempts to access a switch port.



To set port and VLAN security:

1. Select **Security** > **Port Security** > **Port Address Settings** from the menu. The Port Security Address Settings window is shown in Figure 133 on page 437.
2. Configure the settings in Table 111:

Table 111. Port Security Address Settings Window

Field	Description
Port	Select the port that the device is authorized to use on the switch.
MAC Address	Enter the MAC address of the authorized device.
VID (1 - 4094)	Enter the VID of the VLAN the device is authorized to access. You can enter only one VID. The VLAN must already exist on the switch.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

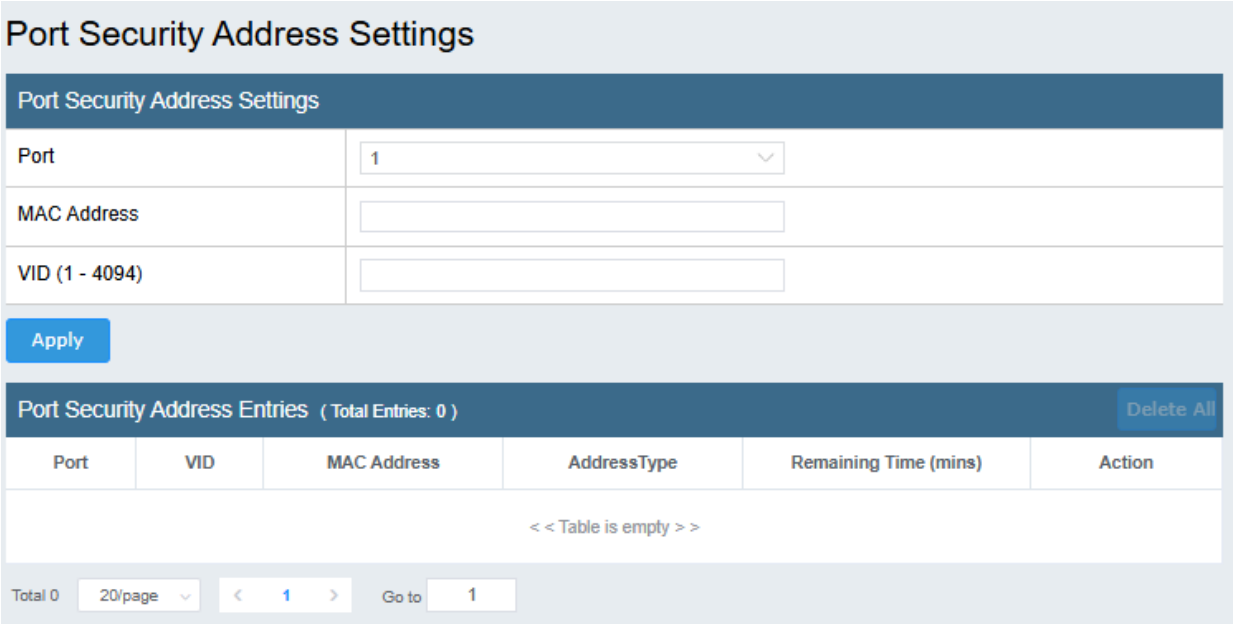


Figure 135. Port Security Address Settings Window

Chapter 45

Port Authentication

This chapter contains background information on the port authentication feature of the switch. The chapter contains the following sections:

- “Overview” on page 444
- “Authentication Methods” on page 446
- “Authenticator Port Operational Settings” on page 447
- “Authenticator Port Operating Modes” on page 448
- “Supplicant and VLAN Associations” on page 451
- “Guest VLAN” on page 453
- “RADIUS Accounting” on page 454
- “General Steps” on page 455
- “Guidelines” on page 456
- “Configuring Port Access Control” on page 458

Overview

Port authentication is a network security feature. Network users have to log with log-on credentials before the switch forwards their traffic. Depending on the authentication method, network users may be required to manually provide user names and passwords when they log on or their workstations may automatically transmit their MAC addresses as their log-on user names and passwords.

Here are several feature terms:

- Supplicant - A supplicant is an end user or node that wants to access the network through a switch port. Supplicants are also referred to as clients.
- Authenticator - The authenticator is a port on the switch that prohibits network access until a supplicant has logged on and been validated by an authentication device.
- Authentication device - The device that authenticates the user names and passwords from the supplicants on the switch ports. This can be RADIUS or TACACS+ servers on your network, or the switch’s local dial-in user accounts.

Authentication Devices

Port-based network access control is a security feature for network clients. It requires that clients log on by providing user names and passwords when they initially send traffic through the switch ports. The feature is used to prevent unauthorized individuals from connecting computers to switch ports or accessing unattended workstations. The switch permits only those users who have been assigned log on credentials to forward traffic through its ports.

The device that performs the verification of user credentials is referred to as the authentication device. The iGS950 Series supports the following three authentication devices:

- RADIUS server with Extensible Authentication Protocol (EAP) extensions: The switch has a RADIUS client so that it can communicate with RADIUS servers on your network. The client on the switch acts as an intermediary between the network users and the RADIUS servers. When network users provide their credentials to log on the network, the client on the switch forwards the information to the RADIUS server, which validates the credentials and notifies the switch as to whether the credentials are valid. Refer to Chapter 47, “RADIUS Client” on page 471.
- TACACS+ server: The switch also has a TACACS+ client for validating log on credentials with TACACS+ servers. Refer to Chapter 48, “TACACS+ Client” on page 477.
- Local dial-in user accounts: If your network does not have RADIUS or TACACS+ servers, you can instead use the switch’s own internal authentication system. When network users log on, the switch checks their log on credentials itself, using its internal database. The switch can store up to 64 local dial-in user accounts. Refer to Chapter 46, “Local Dial-in User Accounts” on page 465.

Authentication Methods

The switch supports two authentication methods:

- 802.1x port-based network access control
- MAC address-based authentication

802.1x Port-based Network Access Control

Supplicants of this type of port authentication use usernames and passwords as their logon credentials. They have to provide their unique credentials when they initially begin to forward traffic through the ports on the switch. Supplicants may provide their usernames and passwords manually when prompted by their workstations or their network devices can provide the information automatically. The switch forwards the user credentials for verification to an authentication device, which can be a RADIUS or TACACS+ server on your network, or internally to its local dial-in user accounts.

Supplicants that manually enter their logon credentials are not tied to any specific computer or node. They can log on from any system and still be verified as valid users of the switch and network.

The supplicants must have 802.1x client software to support this port authentication method.

MAC Address-based Authentication

The log-on credentials for supplicants of this type of port authentication consist of the MAC addresses of the network nodes. The MAC addresses of the devices are used as the usernames and passwords of the supplicants. Supplicants are not prompted for this information. Rather, the switch transmits the initial frames with the source MAC address of the node to the authentication device for authentication.

The advantage to this approach is that supplicants do not need 802.1x client software. The disadvantage is that because clients are not prompted for usernames and passwords, unauthorized individuals can access your network through unattended network nodes or by counterfeiting valid network MAC addresses.

Authenticator Port Operational Settings

An authenticator port on the switch can have one of three possible operational settings:

- Auto - Activates port authentication on a port. Supplicants must provide logon credentials for verification before a port begins to forward their network traffic. This is the default setting for an authenticator port.
- Force-authorized - Disables port authentication and automatically places the port in the authorized state without any authentication exchange required. The port transmits and receives normal traffic without authenticating the client.

Note
A supplicant connected to an authenticator port set to force-authorized must have 802.1x client software if the port's authenticator mode is 802.1x. Though the force-authorized setting prevents an authentication exchange, the supplicant must still have the client software to forward traffic through the port.

- Force-unauthorized - Causes the port to remain in the unauthorized state, ignoring all attempts by the supplicant to authenticate. This setting is analogous to disabling a port.

Authenticator Port Operating Modes

Authenticator ports support three modes:

- Single host mode
- Single host mode with piggy-backing
- Multiple Host mode

Single Host Mode

An authenticator port set to the single host mode permits only one supplicant to log on and forwards only the traffic of that supplicant. After one supplicant has logged on, the port discards packets from any other supplicant that might try to log on.

In Figure 136, port 8 is an authenticator port set to the single host mode. It permits only one supplicant to log on and forwards the traffic from only that supplicant.

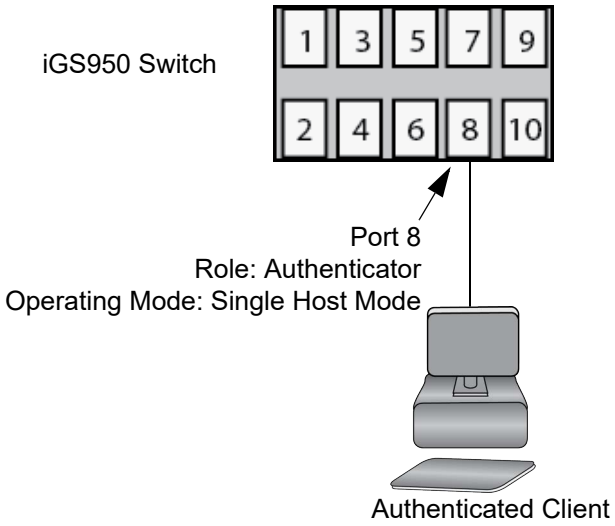


Figure 136. Single Host Mode

Single Host Mode with Piggy Backing

This mode permits multiple clients on an authenticator port, but only one of the clients is authenticated. An authenticator mode forwards packets from all the clients after one client has successfully logged on. This mode is typically used in situations where you want to add authentication to a switch port that is supporting multiple clients, but do not want to create individual accounts for all the clients on the authentication device.

This is referred to as “piggy-backing.” After one client has successfully logged, the port permits the other clients to piggy-back onto the initial client’s log on, so that they can forward packets through the port without being authentication.

Note, however, that should the client who performed the initial log on fail to periodically reauthenticate or log out, the authenticator port reverts to the unauthenticated state. It bars all further traffic to and from all of the clients until the initial client or another client logs on.

Figure 137 is an example of this mode. Port 8 is connected to an Ethernet hub or non-authentication compliant switch, which in turn is connected to several supplicants. The switch blocks all client traffic until one client logs on. Afterwards, it forwards traffic from all the clients.

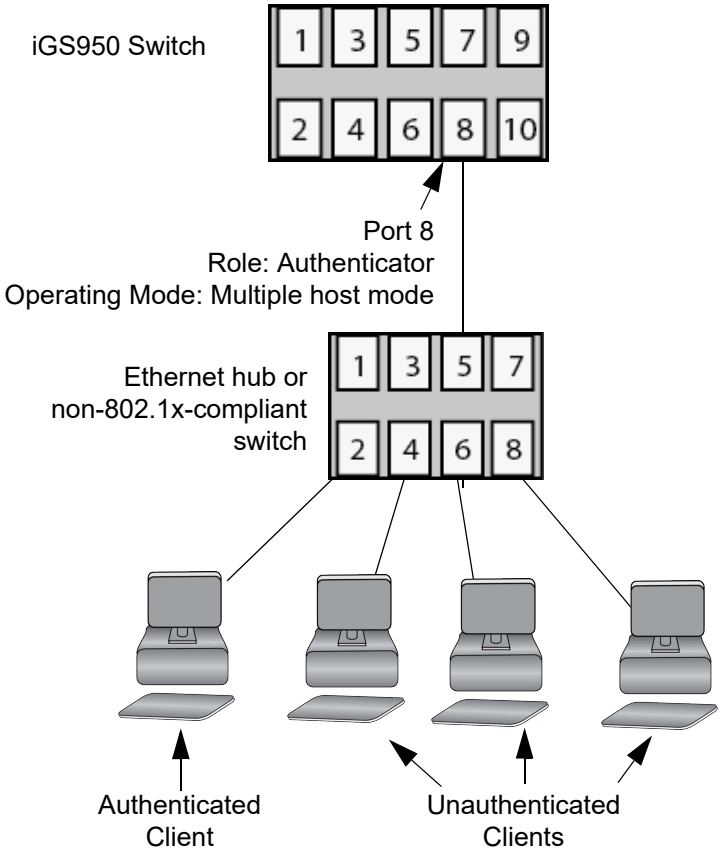


Figure 137. Multiple Host Operating Mode

If the port is set to the 802.1x authentication method, one client has to have 802.1x client firmware and provide a username and password during authentication. (The other clients do not need 802.1x client firmware to forward traffic through the port after one client is authenticated.)

If the port is using MAC address-based authentication, 802.1 client firmware is not required. The first client to forward traffic through the port is used for authentication. When that client is authenticated, all supplicants have access to the port.

As mentioned earlier, should the client who performed the initial log on fail to reauthenticate when necessary or log out, the port reverts to the unauthenticated state, blocking all traffic to and from all clients. Another client has to be authenticated in order for the remaining clients to continue to forward traffic through the port.

Multiple Host Mode

This mode requires the authentication of all the clients on an authenticator port. This mode is appropriate in situations when you want all the clients to be authenticated on authenticator ports that are supporting more than one client.

If you are using 802.1x authentication, you have to provide each client with a separate username and password combination and the clients have to provide their credentials to forward traffic through a switch port.

An example of this authenticator operating mode is illustrated in Figure 138. The clients are connected to a hub or non-authentication switch which is connected to an authenticator port on the iGS950 Switch. If the authenticator port is set to 802.1x authentication, the clients have to provide their username and password credentials before they can forward traffic through the switch.

If the authentication method is MAC address-based, the authenticator port uses the MAC addresses of the clients as the username and password combinations. The port accepts and forwards traffic only from those clients whose MAC addresses have been entered on the authentication devices and denies access to all other users.

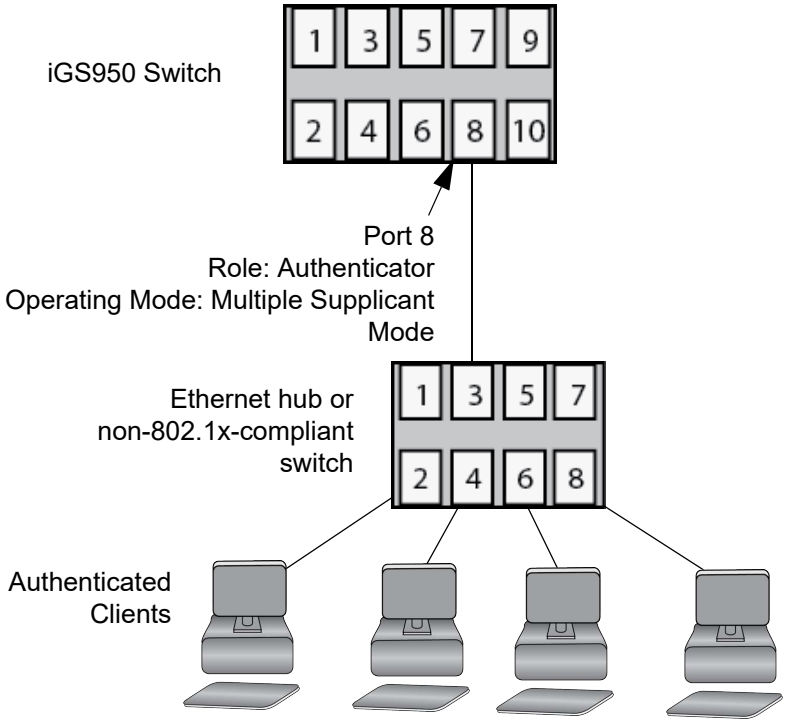


Figure 138. Multiple Supplicant Mode

Supplicant and VLAN Associations

One of the challenges to managing a network is accommodating end users who roam. These are individuals whose work requires that they access the network resources from different points at different times. The difficulty arises in providing them with access to the same network resources and, conversely, restricting them from unauthorized areas, regardless of the workstation from where they access the network. A closely related issue is where a workstation is employed at various times by different individuals with unique requirements in terms of network resources and security levels.

Providing network users with access to their network resources while also maintaining network security is often achieved with VLANs. As explained in Chapter 34, “802.1Q Tagged Virtual LANs” on page 337, VLANs are independent traffic domains where the traffic generated by the nodes within a VLAN are restricted to nodes of the same VLAN, unless there is a router or Layer 3 device. Typically, network users are assigned to different VLANs depending on their resource requirements and security levels.

The problem with a port-based VLAN is that VLAN membership is determined by the port on the switch to which the device is connected. If a different device that needs to belong to a different VLAN is connected to the port, the port must be manually moved to the new VLAN using the management software.

With port authentication, you can link username and password credentials or MAC addresses to specific VLANs so that the switch automatically moves ports to the appropriate VLANs when clients log on. This frees you from having to reconfigure VLANs as end users access the network from different points or where the same workstation is used by different individuals at different times.

To use this feature, you have to enter a VLAN identifier, along with other information, when you add supplicant accounts on the authentication device. The server passes the identifier to the switch when a user logs on with a valid username and password credential or MAC address, depending on the authentication method.

How the switch responses when it receives VLAN information during the authentication process can differ depending on the operating mode of an authenticator port.

Single Host Mode

Here are the operating characteristics for the switch when an authenticator port is set to the single host mode:

- If the switch receives a valid VLAN ID or VLAN name from the RADIUS server, it moves the authenticator port to the designated guest VLAN and changes the port to the authorized state. Only the authenticated supplicant is allowed to use the port. All other supplicants are denied entry.
- If the switch receives an invalid VLAN ID or VLAN name from the authentication device (e.g., the VID of a nonexistent VLAN), it leaves the port in the unauthorized state to deny access to the port.

Multiple Host Mode

Here are the operating characteristics for the switch when an authenticator port is set to the multiple host mode:

- If the switch receives a valid VLAN ID or VLAN name from the authentication device, it moves the authenticator port to the designated VLAN and changes the port to the authorized state. All clients are allowed access to the port and the same VLAN after the initial authentication.
- If the switch receives an invalid VLAN ID or VLAN name from the authentication device (e.g., the VID of a nonexistent VLAN), it leaves the port in the unauthorized state to deny access to the port.

Multiple Supplicant Mode

The initial authentication on an authenticator port running in the multiple supplicant mode is handled in the same fashion as with the Single operating mode. If the switch receives a valid VLAN ID or name from the authentication device, it moves the authenticator port to the designated VLAN and changes the port to the authorized state. All subsequent supplicants who log on to the same port are also authenticated. However, the port remains in the VLAN specified in the initial authentication.

Supplicant VLAN Attributes on RADIUS Servers

If you are using RADIUS servers as the authentication devices, you have to include the following information as part of supplicant accounts when associating supplicants to VLANs.

- Tunnel-Type: This is the protocol to be used by the tunnel specified by Tunnel-Private-Group-Id. The only supported value is VLAN (13).
- Tunnel-Medium-Type: This is the transport medium to be used for the tunnel specified by Tunnel-Private-Group-Id. The only supported value is 802 (6).
- Tunnel-Private-Group-ID This is the ID of the tunnel the authenticated user should use. This must be the name of VID of the VLAN of the switch.

Guest VLAN

An authenticator port in the unauthorized state typically accepts and transmits only 802.1x packets while waiting to authenticate a supplicant. However, you can configure authenticator ports to be members of a Guest VLAN when no supplicants are logged on. Client using the ports are not required to log on and have full access to the resources of the Guest VLAN.

If the switch receives 802.1x packets on the port, signaling that a supplicant is logging on, it moves the port to its predefined VLAN and places it in the unauthorized state. The port remains in the unauthorized state until the log on process between the supplicant and the authentication device is completed. When the supplicant logs off, the port automatically returns to the Guest VLAN.

Note
The Guest VLAN feature is only supported on authenticator ports in the Single operating mode.

RADIUS Accounting

The switch supports RADIUS accounting for switch ports in the authenticator role. This feature sends information to the RADIUS server about the status of the supplicants so that you can monitor network activity and use.

The switch sends accounting information to the RADIUS server when the following events occur:

- Supplicants log on
- Supplicants logs off
- Authenticator ports change states during active supplicant sessions (for example, a port is reset or is changed from the Authenticator role to None role while a supplicant is logged on)

The event information sent to the RADIUS server includes:

- The port number where an event occurred.
- The date and time when an event occurred.
- The number of packets transmitted and received by a switch port during a supplicant's session. (This information is sent only when a client logs off.)

You can also configure the accounting feature to send interim updates so that you can monitor which clients are still active.

Here are the guidelines to using the accounting feature:

- The management software supports the Network level of accounting, but not the System or Exec.
- This feature is only available on Authenticator ports.
- You have to configure 802.1x Port-based Network Access Control as explained in this chapter and designate the Authenticator ports.
- You have to configure the RADIUS client.

General Steps

Here are the general steps to implementing port-based authentication on the switch:

1. To use RADIUS or TACACS+ servers as the authentication devices, install server software on one or more of your network devices.

2. Add supplicant accounts to the authentication device:

   - For 802.1x authentication, the accounts should have user names and passwords. The maximum length for user names and passwords is 23 alphanumeric characters. Spaces and special characters are not supported.
   - For MAC address-based authentication, the accounts use the MAC addresses of the supplicant devices as the user names and passwords.

3. Verify that clients connected to authenticator ports set to 802.1x authentication have 802.1x client software. (MAC address authentication does not require 802.1x client software.)

4. If the authentication devices are RADIUS or TACACS+ servers, configure the RADIUS or TACACS+ client on the switch. This involves entering the IP addresses and encryption keys of the servers on your network. Refer to Chapter 47, “RADIUS Client” on page 471 or Chapter 48, “TACACS+ Client” on page 477.

5. Configure the port access control settings on the switch. Refer to “Configuring Port Access Control” on page 458.

Guidelines

Here are the general feature guidelines:

- Ports configured for authentication do not support dynamic MAC address learning.
- A port connected to a RADIUS or TACACS+ authentication server cannot be set to the authenticator role because an authentication server cannot authenticate itself.
- The authentication method can be 802.1x or MAC address authentication.
- Supplicants connected to authenticator ports set to 802.1x authentication need to have 802.1x client software.
- Supplicants do not need 802.1x client software for MAC address authentication.
- The log-on credentials for 802.1x supplicants are not tied to the MAC addresses of an end node. This allows end users to use the same log- on credentials when working from different workstations.
- The MAC addresses of authenticated clients are added to the MAC address table as authenticated addresses. They remains in the table until clients log off the network or fail to reauthenticate, at which point they are removed. The addresses are not timed out, even if the nodes are inactive.

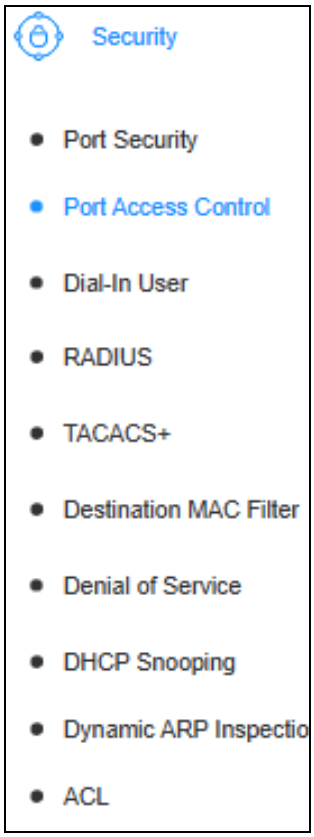
Note
End users of port authentication should be instructed to always log off at the conclusion of every work session. This can prevent unauthorized individuals from accessing the network through unattended network workstations.

- Authenticator and supplicant ports need to be untagged ports. They cannot be tagged ports.
- Authenticator ports cannot use destination MAC address filters. Refer to Chapter 49, “Destination MAC Address Filters” on page 483.
- Authenticator ports cannot be members of LACP or static port trunks or the port mirror.
- The Guest VLAN feature requires that the designated VLAN already exist on the switch.
- The Guest VLAN can be a port-based or tagged VLAN.
- The switch must have a IP address to communicate with RADIUS or TACACS+ servers. Refer to Chapter 4, “Management IPv4 Addresses” on page 71 or Chapter 5, “Management IPv6 Addresses” on page 81.

Here are the guidelines to adding VLAN assignments to supplicant accounts:

- The VLAN can be either a port-based or tagged VLAN.
- The VLAN has to already exist on the switch.
- A supplicant account can have only one VLAN.
- When a supplicant logs on, the switch moves the port to the designated VLAN as an untagged port.

Configuring Port Access Control



To configure port-based access control:

1. Select **Security** > **Port Access Control** from the menu. The Port Access Control Settings window is shown in Figure 139 on page 459.
2. Configure the parameters in Table 112.

Table 112. Port Access Control Settings Window

Parameter	Description
NAS ID	Enter an 802.1x identifier that the switch applies to all ports. The NAS ID can be up to 16 characters. Valid characters are 0 to 9, a to z, and A to Z. Spaces are allowed. The default is NAS1. Specifying an NAS ID is optional.
Port Access Control Status	Select the status of port access control from the pull-down menu: - **Enabled**: Enables Port Access Control. - **Disabled**: Disables the feature. This is the default setting.
Authentication Method	Select the authentication method from the menu: - **RADIUS**: Selects remote authentication with RADIUS servers. Refer to the Chapter 47, “RADIUS Client” on page 471 to define the servers. - **TACACS+**: Selects remote authentication with TACACS+ servers. Refer to Chapter 48, “TACACS+ Client” on page 477 to define the servers. - **Local**: Selects local authentication. Refer to Chapter 46, “Local Dial-in User Accounts” on page 465 to define the supplicants. This is the default setting.

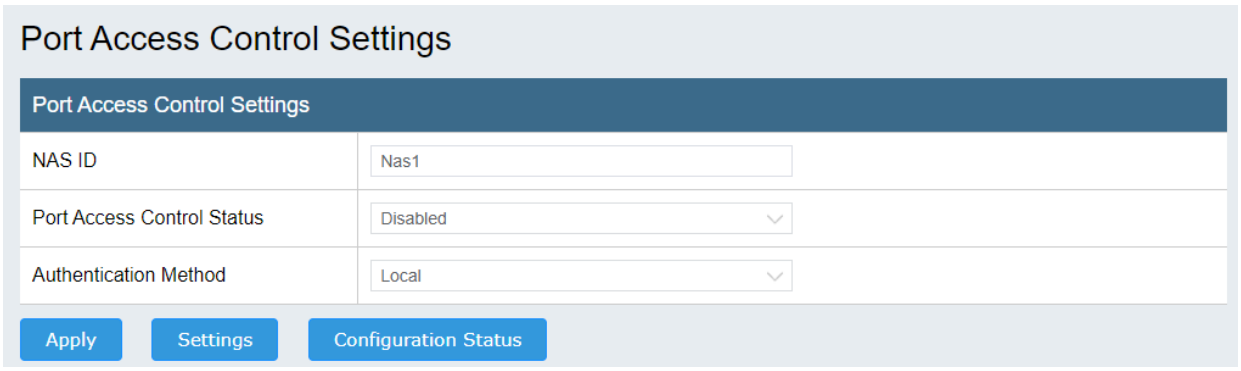


Figure 139. Port Access Control Settings Window

3. Click **Apply**.

4. To configure the port settings, click **Settings**. The window can display the settings of only one port at a time. Refer to Figure 140.

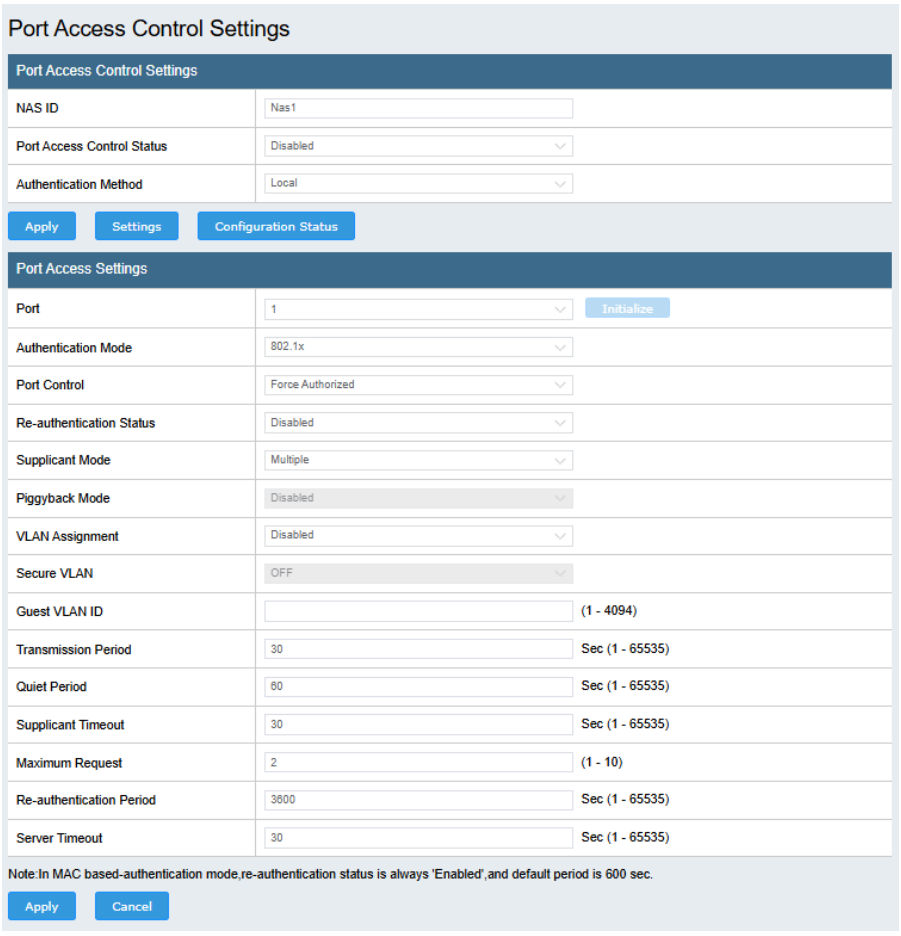


Figure 140. Port Access Control Settings Window - Port Settings

5. Configure the fields in Table 113 and click **Apply**.

Note
Select **Save** from the menu to save your changes.

Table 113. Port Access Control Settings Window - Advanced Settings

Field	Description
Port	Select a port to configure from the pull-down menu. You can configure only one port at a time.
Authentication Mode	Select an authentication mode for the port from the pull-down menu: - **802.1x**: Designates 802.1x as the authentication mode for the port. Clients on ports in this mode have to provide user names and passwords to log in to access the network. - **MAC Based**: Designates MAC address-based authentication on the port. Clients on ports in this mode are logged on using the MAC addresses of their network devices. The switch sends the initial frames from the clients to the authentication server. The server uses the source MAC addresses in the frames as the user names and passwords for the clients. Supplicant nodes do not need 802.1x client software for this authentication method.

Table 113. Port Access Control Settings Window - Advanced Settings

Field	Description
Port Control	Select a control method for the port from the pull-down menu: - **Forced Authorized**: Sets the port to Forced-Authorized port control. Ports transition to the authorized state without any authentication exchanges required. The port transmits and receives traffic normally without 802.1x based authentication of a client. This is the default setting. - **Forced Unauthorized**: Sets the port to the 802.1x authenticator role, in the unauthorized state. The port blocks all authentications, preventing any client from logging on and forwarding packets. - **Auto**: Sets the port to the 802.1x port-based authenticator role. The port begins in the unauthorized state, forwarding only EAPOL frames, until a client successfully logs on. Refer to “Authenticator Port Operational Settings” on page 447.
Re-authentication Status	Select a re-authentication state from the menu: - **Enabled**: Activates re-authentication on the port. The client has to periodically reauthenticate according to the time interval set with the Re-authentication Period. - **Disabled**: Deactivates re-authentication. The client does not have to reauthenticate after the initial authentication. Reauthentication is still required if there is a change to the status of the link between a client and the switch, or the switch is reset or power cycled. This is the default setting.

Table 113. Port Access Control Settings Window - Advanced Settings

Field	Description
Supplicant Mode	Select a supplicant mode from the menu: - **Single**: Enables the single supplicant mode. Ports in this mode support only one supplicant at a time. They blocks all other clients once one client has successfully logged in. This is the default setting. Refer to “Single Host Mode” on page 448. - **Multiple**: Enables the multiple supplicant mode. Ports in this mode permit more than one supplicant at a time to access them. Use the piggyback mode to control whether only one client or all clients have to log in to use ports in this mode. Refer to “Multiple Host Mode” on page 450.
Piggyback Mode	Select a piggyback mode for the port from the menu: - **Enabled**: Activates the piggyback mode. This mode is used with the multiple supplicant mode. It is commonly used when you want to add 802.1x port-based network access control to a port that is supporting multiple clients, but do not want to add individual accounts for all the clients on the authentication server. After one client has successfully logged on, the port permits other clients to piggy-back onto the initial client’s logon, so that they can use the port without being authenticated. Refer to “Single Host Mode with Piggy Backing” on page 448. - **Disabled**: Deactivates the piggyback mode. This is the default mode. All clients on ports set to the multiple supplicant mode have to have authentication credentials and log in.
VLAN Assignment	Select the VLAN assignment mode from the pull-down menu: - **Enabled**: The switch moves the port to the VLAN specified in the clients login credentials on the authentication device when the clients log on. - **Disabled**: The port remains in its current VLAN when the client logins on.
Secure VLAN	Reserved for future use.

Table 113. Port Access Control Settings Window - Advanced Settings

Field	Description
Guest VLAN ID	Enter the VID for a Guest VLAN. Clients do not have to log in to access the Guest VLAN. The default is no Guest VLAN. The range is 1 to 4094. Refer to “Guest VLAN” on page 453.
Transmission Period	Enter the switch-to-client retransmission time for EAP request frames. The range is 1 to 65535 seconds. The default is 30 seconds.
Quiet Period	Enter the number of seconds that authenticator ports wait after a failed authentication before accepting authentication requests again. The range is 1 to 65535 seconds.
Supplicant Timeout	Enter the switch-to-client retransmission time interval for EAP request frames. The range is 1 to 65535 seconds. The default is 30 seconds.
Maximum Request	Enter the maximum number of times authenticator ports transmit EAP Request packets to clients before timing out authentication sessions. The range is 1 to 10. The default is 2.
Re-authentication Period	Enter the time interval in seconds when an authenticator port requires a client to reauthenticate. The range is 1 to 65,535 seconds. The default is 3600 seconds.
Server Timeout	Enter the amount of time in seconds the switch waits for a response from an authentication server. The range is 1 to 65535 seconds. The default is 30 seconds.

Chapter 46

Local Dial-in User Accounts

This chapter describes the local dial-in user accounts feature in the following sections:

- ❒ “Local Dial-in User Authentication Overview” on page 466
- ❒ “Adding Local Dial-in User Accounts” on page 467
- ❒ “Modifying or Deleting Local Dial-in User Accounts” on page 469

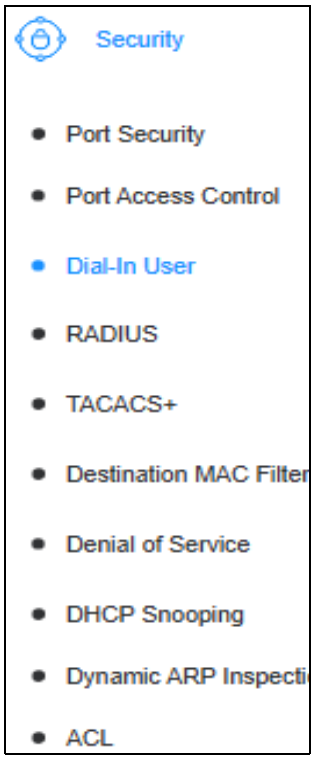
Local Dial-in User Authentication Overview

Local dial-in user authentication is part of the 802.1x port-based network access control feature. You can use it instead of RADIUS or TACACS+ servers to authenticate clients on authenticator ports on the switch. The feature consists of an internal database that the switch maintains of client credentials of user names, passwords, and VLAN assignments. As clients log on, the switch refers to its internal database to validate the log on credentials.

Here are the guidelines:

- The switch supports up to 64 user accounts.
- You have to configure port-based network access control before activating the local dial-in user authentication. Refer to Chapter 45, “Port Authentication” on page 443.
- The switch uses standard EAP over LAN (EAPOL) transactions to authenticate clients.

Adding Local Dial-in User Accounts



To add local user accounts:

1. Select **Security** > **Dial-in User** from the menu. The Dial-in User window is shown in Figure 141 on page 468.
2. Configure the fields in Table 114.

Table 114. Dial-In User Window

Field	Description
User Name	Enter a unique user name for the account. The maximum length is 20 alphanumeric characters. The user name is not case-sensitive. Spaces are allowed. Special characters are not allowed. This field is required.
Password	Enter a password for the account. The maximum length is 20 alphanumeric characters. The password is not case-sensitive. Spaces are allowed. Special characters not allowed. This field is required.
Dynamic VLAN	Enter a VID of the 802.1Q tagged VLAN where the switch moves the port when a client logs on. Here are the guidelines: - The VID range is 1 to 4094. - An account can have only one VID. - The 802.1Q tagged VLAN must already exist on the switch. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337. - You cannot specify a Port-based or private VLAN. - Leave this field empty if you want ports to remain in their pre-defined VLANs when clients log on. - If you enter a VID, you have to enable the VLAN Assignment parameter on the switch ports where clients will log on. Refer to “Configuring Port Access Control” on page 458. - The default is no VID.

3. Click **Add**.

Note
Select **Save** from the menu to save your changes.

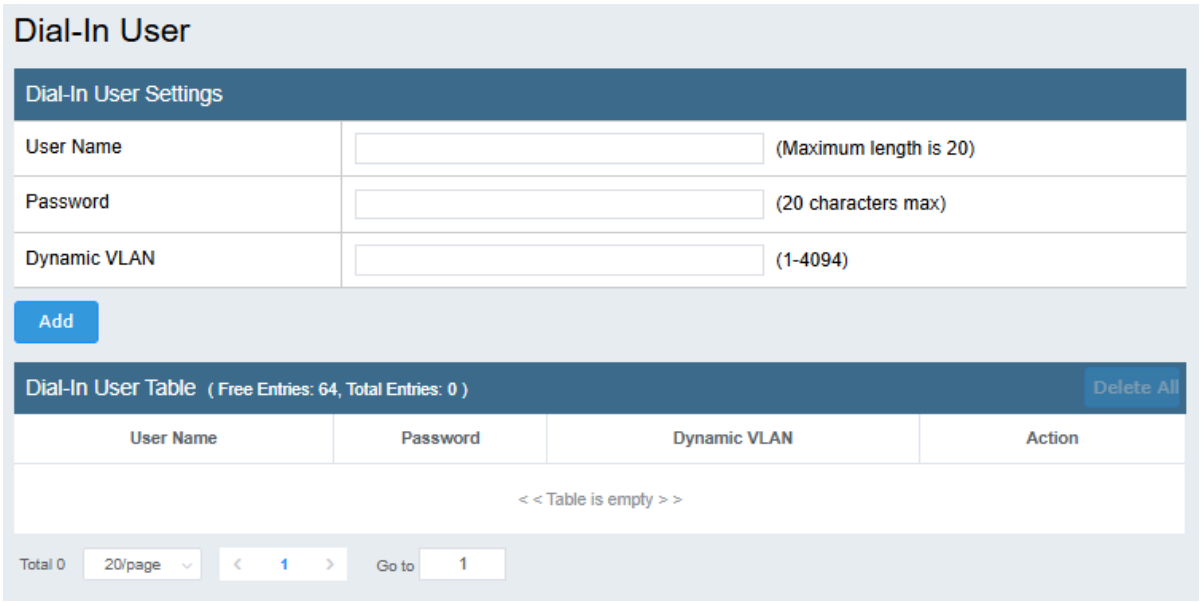


Figure 141. Dial-In User Window

Modifying or Deleting Local Dial-in User Accounts

To modify or delete local dial-in user accounts:

1. Select **Security** > **Dial-in User** from the menu. The Dial-in User window is shown in Figure 141 on page 468.
2. To modify an account, do the following:
   a. Click **Modify** in the Action column of the table. You can modify only one account at a time. The account's details are displayed in the window.
   b. Modify the account by referring to Table 114 on page 467.
3. To delete accounts, do one of the following:
   - ❒ To delete a single account, click **Delete** in the Action column in the table.
   - ❒ To delete all the accounts on the switch, click **Delete All**.
4. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

Chapter 47

RADIUS Client

This chapter describes the RADIUS client in the following sections:

- “RADIUS Client Overview” on page 472
- “Managing Server IP Addresses in the RADIUS Client” on page 473

RADIUS Client Overview

Remote Authentication Dial In User Services (RADIUS) is one of the ways that the switch can authenticate network clients of 802.1x port-based access control. The switch has a RADIUS client that allows it to communicate with RADIUS servers on your network. When a network user logs in to the switch, the switch uses its RADIUS client to forward the client's credentials to the RADIUS server for authentication.

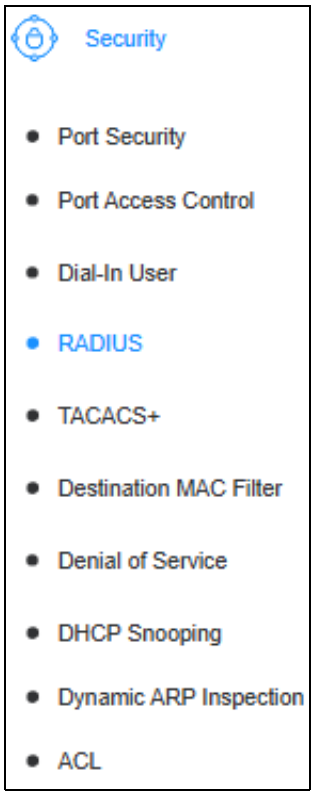
The following guidelines apply to the RADIUS client.

- ❒ You have to designate RADIUS as the authentication method for 802.1x port-based access control on the switch. Refer to Chapter 45, "Port Authentication" on page 443.
- ❒ You have to install RADIUS server software on a network server or management station.
- ❒ You can designate up to five RADIUS servers on the switch.
- ❒ You can specify RADIUS servers by their IPv4 or IPv6 addresses.
- ❒ The RADIUS server has to communicate with the switch through a port that is an untagged member of the Default VLAN and is configured for Forced-Authorized (802.1x) port control. Refer to "Configuring Port Access Control" on page 458.
- ❒ If the RADIUS server is on a different subnet from the switch, be sure to specify a System Default Gateway in the IP Setup page, so that the switch and server can communicate with each other via the gateway. Refer to Chapter 4, "Management IPv4 Addresses" on page 71 or Chapter 5, "Management IPv6 Addresses" on page 81.
- ❒ You have to specify the user name and password credentials when configuring the RADIUS server software on the authentication server.
- ❒ RADIUS servers have to support Extensible Authentication Protocol (EAP) extensions.

Note
This guide does not explain how to configure RADIUS server software. Refer to the documentation that comes with the server software for instructions.

For more information on the RADIUS authentication protocol, refer to the RFC 2865 standard.

Managing Server IP Addresses in the RADIUS Client



To manage up to five IPv4 or IPv6 addresses of RADIUS servers in the client on the switch:

1. Select **Security** > **RADIUS** from the menu. The RADIUS window is shown in Figure 142 on page 475.
2. Do one of the following:
   a. To add an IP address, configure the fields in Table 115.
   b. To modify an IP address, click **Modify** in the **Action** column of the IP address to be modified. You can modify only one address at a time. Modify the fields in Table 115.
   c. To delete an IP address, click **Delete** of the IP address to be deleted from the table.
3. Click the **Apply** button.

Note
Select **Save** from the menu to save your changes.

Table 115. RADIUS Window

Field	Description
Server Priority	Enter a priority number for the server address. The range is 1 to 5. The switch queries the servers in ascending order, starting with 1. A RADIUS IP address can have only one priority number.

Table 115. RADIUS Window (Continued)

Field	Description
Server IP Address	Enter the IPv4 or IPv6 address of the RADIUS server. The format for an IPv4 address is shown here: nnn nnn nnn nnn Each N is a decimal number from 0 to 255. The format for an IPv6 address is shown here: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx Each x is a hexadecimal digit representing four bits. The eight groups of digits have to be separated by colons. Groups where all four digits are ‘0’ can be omitted. Leading ‘0’s in groups can also be omitted. As an example, the following IPv6 addresses are equivalent: 3710:421e:09a8:0000:0000:0000:00a4:1c50 3710:421e:9a8::a4:1c50
Server Port	Enter the UDP destination port for RADIUS authentication requests. The range is 1 to 65535. The default port is 1812.
Accounting Port	Enter the UDP destination port for RADIUS accounting requests. The range is 1 to 65535. The default port is 1813.
Shared Secret	Enter the encryption key used by the RADIUS server. The maximum length is 32 characters.

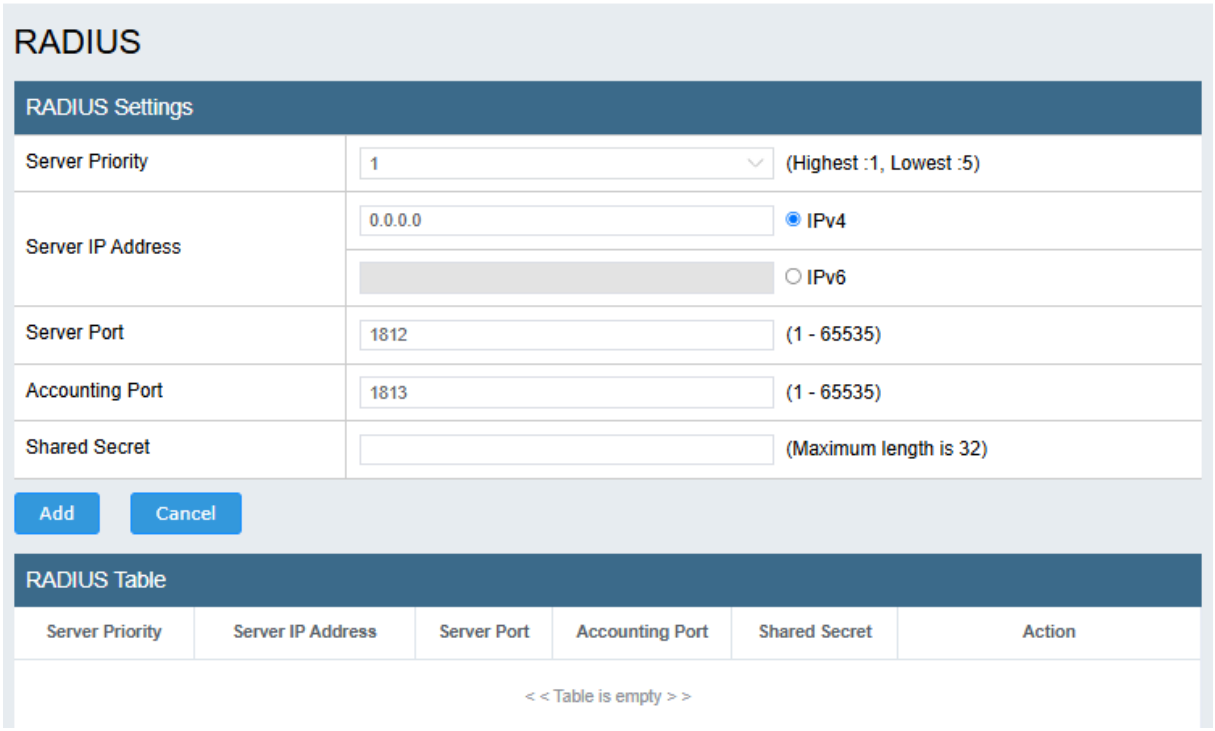


Figure 142. RADIUS Window

Chapter 48

TACACS+ Client

The TACACS+ client is described in the following sections:

- ❒ “TACACS+ Client Overview” on page 478
- ❒ “Managing Server IP Addresses in the TACACS+ Client” on page 479

TACACS+ Client Overview

The iGS950 Switch has a Terminal Access Controller Access-Control System Plus (TACACS+) client. The client is one of several ways that the switch can authenticate supplicants of 802.1x port-based access control. When supplicants log in to authenticator ports, the switch can use the client to transmit the user names and passwords to TACACS+ servers on a network for verification.

Here are the TACACS+ client guidelines.

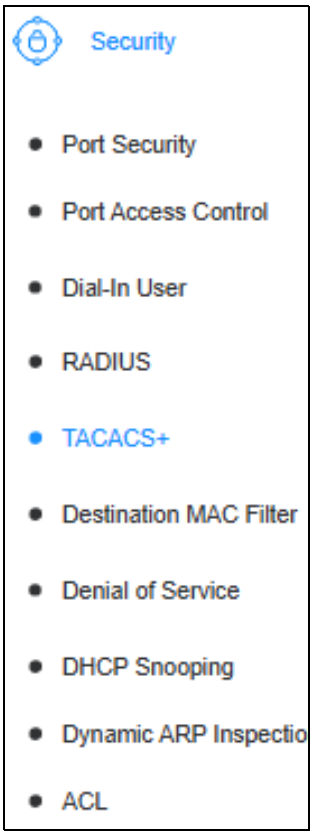
- ❒ You have to designate TACACS+ as the authentication method for 802.1x port-based access control on the switch. Refer to Chapter 45, “Port Authentication” on page 443.
- ❒ You have to install TACACS+ server software on a network server or management station.
- ❒ You can specify the IP addresses of up to five TACACS+ servers.
- ❒ You can identify the servers by IPv4 or IPv6 addresses.
- ❒ The TACACS+ server has to communicate with the switch through a port that is an untagged member of the Default VLAN and is configured for Forced-Authorized (802.1x) port control.
- ❒ If the TACACS+ server is on a different subnet from switch, be sure to specify a System Default Gateway in the IP Setup window, so that the switch and server can communicate with each other via the gateway. Refer to Chapter 4, “Management IPv4 Addresses” on page 71 or Chapter 5, “Management IPv6 Addresses” on page 81.
- ❒ You have to configure the TACACS+ servers with the user name and password credentials of the network clients.

Note
This guide does not explain how to configure TACACS+ server software. Refer to the software documentation for instructions.

You can also authenticate supplicants of 802.1x port-based access control with RADIUS. The differences between TACACS+ and RADIUS are as follows:

- ❒ TACACS+ separates authentication and authorization in a user profile, whereas, RADIUS combines authentication and authorization.
- ❒ TACACS uses TCP instead of UDP.

Managing Server IP Addresses in the TACACS+ Client



To manage the IP addresses of up to five TACACS+ servers in the TACACS+ client on the switch:

1. Select **Security** > **TACACS+** from the menu. The TACACS+ window is shown in Figure 143 on page 481.

   The table in the bottom portion of the window lists the current TACACS+ server IP addresses. The columns are defined in Table 116.

2. Do one of the following:

   a. To add an IP address of a TACACS+ server, configure the fields in Table 116.

   b. To modify an IP address in the table, click **Modify** in the **Action** column. You can modify only one address at a time. Modify the fields in Table 116.

   c. To delete an IP address from the table, click **Delete** in the **Action** column.

3. Click **Apply**.

Note
Select **Save** in the menu to save your changes.

Table 116. TACACS+ Window

Field	Description
Server Priority	Select a unique priority number for the server address from the menu. The range is 1 to 5. The switch queries the server addresses in ascending order, starting with 1. An IP address can have only one priority number.

Table 116. TACACS+ Window (Continued)

Field	Description
Server IP Address	Enter the IPv4 or IPv6 address of the TACACS+ server. The format for an IPv4 address is shown here: nnn nnn nnn nnn Each N is a decimal number from 0 to 255. The format for an IPv6 address is shown here: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx Each x is a hexadecimal digit representing four bits. The eight groups of digits have to be separated by colons. Groups where all four digits are ‘0’ can be omitted. Leading ‘0’s in groups can also be omitted. As an example, the following IPv6 addresses are equivalent: 3710:421e:09a8:0000:0000:0000:00a4:1c50 3710:421e:9a8::a4:1c50
Server Port	Enter the TCP destination port for TACACS+ authentication requests. The range is 1 to 65535. The default port is 49.
Timeout	Enter the length in time (seconds) the switch waits for a response from a TACACS+ server to an authentication request before querying the next server in the list.
Shared Secret	Enter the encryption key used by the TACACS+ server. The maximum length is 32 characters.

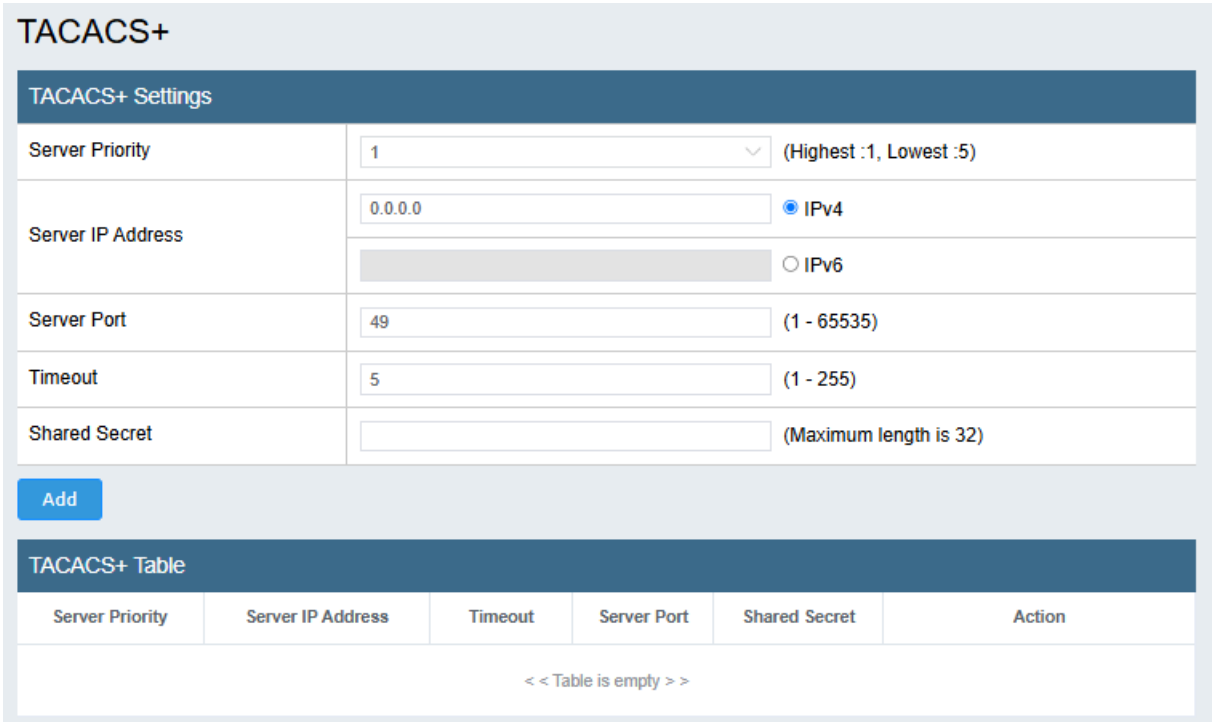


Figure 143. TACACS+ Window

Chapter 49
Destination MAC Address Filters

This chapter describes the destination MAC address filters in the following sections:

- “Destination MAC Address Filters Overview” on page 484
- “Managing Destination MAC Address Filters” on page 485

Destination MAC Address Filters Overview

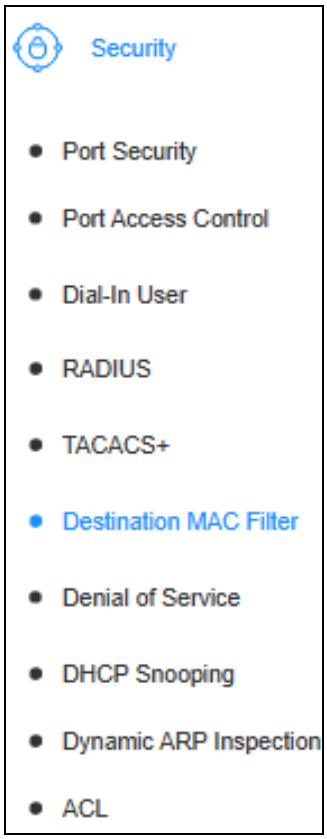
Destination MAC address filters are a network security feature that block network users from accessing designated devices on your network. The restricted devices are identified by their MAC addresses. The switch discards ingress packets whose destination MAC addresses match the filters.

You can use the feature to block switch clients from gaining unauthorized access to secured devices on your network. For instance, if the users connected to the switch are part of the Sales department, you could add filters to block them from accessing the accounting and engineering servers.

Here are the guidelines to destination MAC address filters:

- The switch supports up to 188 filters.
- Each filter can have one destination MAC address.
- Filters have to contain the MAC addresses of specific devices. Filters cannot contain MAC address ranges.
- The filters are set at the switch level and apply to all switch ports.

Managing Destination MAC Address Filters



To add or delete destination MAC address filters:

1. Select **Security** > **Destination MAC Filter** from the menu. The Destination MAC Filter window is shown in Figure 144.

   The table in the bottom portion of the window lists the current destination MAC address filters.

2. To add a new destination MAC address filter to block network clients from accessing the designated device, do the following:

   a. Enter the MAC address of the destination device in the MAC Address field.

   b. Click **Add**. The switch immediately activates the new filter. Client devices connected to the ports on the switch are now blocked from accessing the specified destination device.

3. To delete destination MAC address filters from the switch, do one of the following:

   - To delete a single filter, click **Delete** in the Action column.
   - To delete all the filters, click **Delete All** above the table.

Note
Select **Save** from the menu to save your changes.

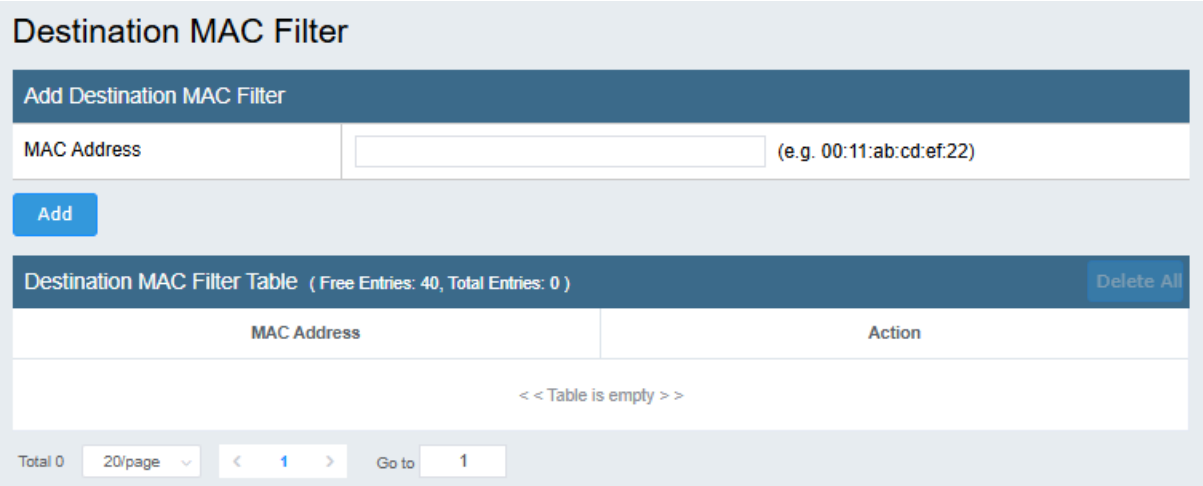


Figure 144. Destination MAC Filter Window

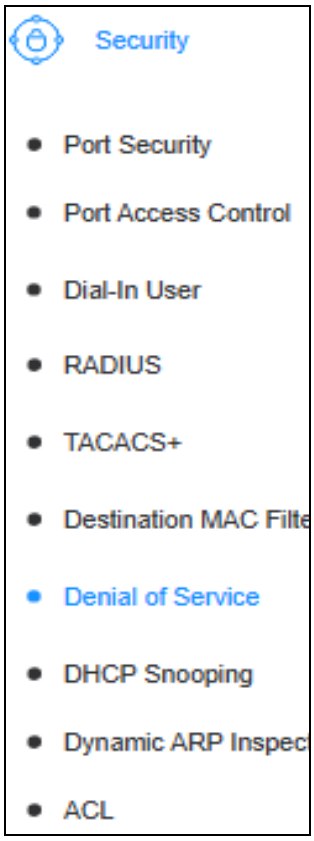
Chapter 50

Denial of Service

This chapter contains the following sections:

- “Configuring Denial of Service Protection” on page 488

Configuring Denial of Service Protection



The switch has filters for blocking selected types of TCP/IP packets that might pose network security risks. The filters are set at the switch level and apply to all ports. To configure the Denial or Service protection filters:

1. Select **Security** > **Denial or Service** from the menu. The Denial of Service window is shown in Figure 145 on page 489.

2. Adjust the filters, as listed here:

   - **Allow**: The switch forwards the packets. This is the default.
   - **Deny**: The switch discards the packets.

   The filters are described in Table 117.

Table 117. Denial of Service Filters

Filters	Description
Land Attack	Blocks TCP packets in which the values for the source and destination IP addresses and source and destination port numbers are the same.
Blat Attack	Blocks TCP packets in which the values for the source and destination port numbers are the same.
TCP Null Scan	Blocks TCP packets with no TCP flags set.
TCP Xmascan	Blocks TCP packets with the FIN-URG-PSH flag set to 1.
TCP SYN/FIN	Deletes TCP packets with the SYN and FIN flags set to 1.
TCP SYN SrcPort less 1024	Blocks TCP packets in which the SYN source port is less than 1024.
TCP Tiny Flag Attack	Blocks TCP packets in which IP datagrams are less that 400 bytes.

3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

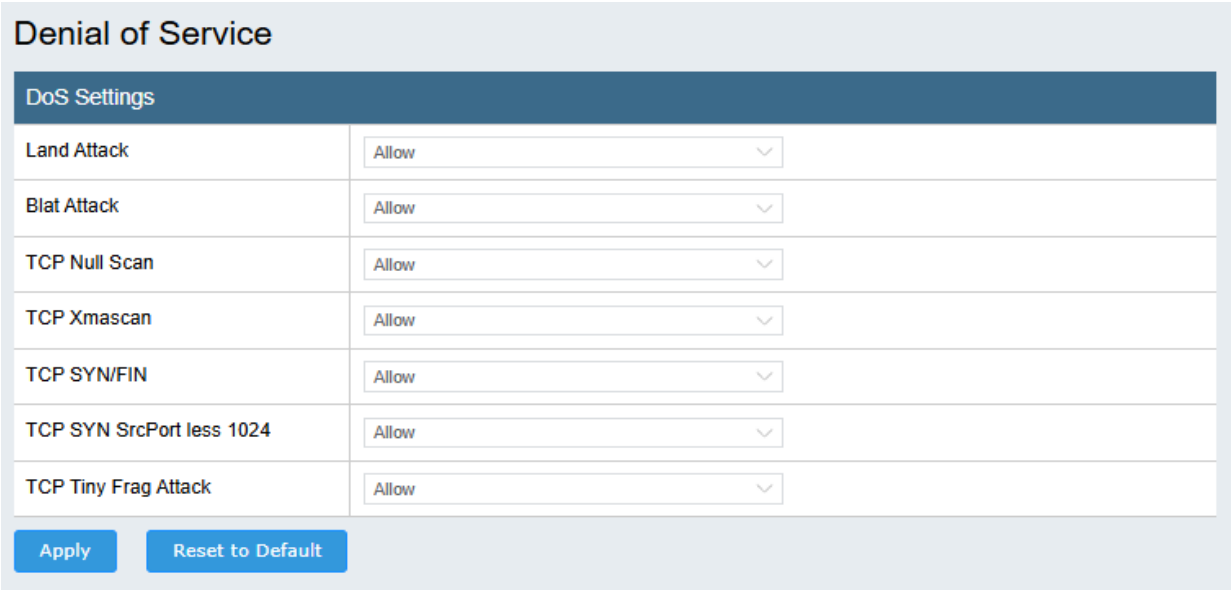


Figure 145. Denial of Service Window

Chapter 51

DHCP Snooping

This chapter describes DHCP snooping in the following sections:

- ❒ “DHCP Snooping Overview” on page 492
- ❒ “General Guidelines” on page 497
- ❒ “Configuring DHCP Snooping” on page 498
- ❒ “Adding DHCP Snooping to VLANs” on page 501
- ❒ “Designating Trusted and Untrusted Ports” on page 503
- ❒ “Managing the Binding Database” on page 504

DHCP Snooping Overview

DHCP snooping is a network security feature that enables the switch to monitor and block packets from unauthorized DHCP servers.

The switch monitors DHCP packets from nodes and discards invalid packets that contain fake or counterfeit IP addresses. The switch maintains a table called the binding database that contains the MAC and IP addresses of the nodes on its ports. When it receives an ARP packet it compares the packet's source MAC and IP addresses against the addresses in the database. If there is no match, it discards the packet.

DHCP snooping increases security by inspecting ingress packets for the correct IP and MAC address information. The DHCP snooping feature defines the ports on the iGS950 Switch as either trusted or untrusted. With DHCP snooping enabled, two network security issues are addressed:

- ❒ All ingress DHCP packets are examined on untrusted ports, and only authorized packets are passed through the switch. Unwanted ingress DHCP packets are discarded. Refer to "Unauthorized DHCP Servers," next below.
- ❒ DHCP ingress packets on an untrusted port are inspected to ensure that the source IP address and MAC address combination in each packet is valid when compared to the DHCP snooping binding table. If a match is not found, the packet is discarded.

Trusted Ports

By definition, trusted ports inherently trust all ingress Ethernet traffic. There is no checking or testing on ingress packets for this type of port. A trusted port connects to a DHCP server in one of the following ways:

- ❒ Directly to the legitimate trusted DHCP server
- ❒ A network device relaying DHCP messages to and from a trusted server
- ❒ Another trusted source such as a switch with DHCP snooping enabled

Untrusted Ports

Ethernet traffic on untrusted ports are inherently not trusted. The switch tests ingress packets against specified criteria to determine if they should be forwarded or discarded. Untrusted ports should be connected to DHCP clients and to traffic that originates outside of the LAN.

Unauthorized DHCP Servers

A local area network typically has a single DHCP server that supplies the network configurations, including as IP addresses, to the network devices. A switch port connected to a trusted DHCP server should be designated as a trusted port.

It is possible that an unauthorized DHCP server could be connected to the network. This situation might occur if a network client activates a DHCP server application or if someone outside the network sends DHCP packets to your network. These situations pose a security risk.

A network device initially sends out a DHCPDISCOVER packet so that a DHCP server will respond. It waits for, and then accepts, the first DHCPOFFER packet from the server that it receives. This packet contains the DHCP server's IP address and mask. If the unauthorized DHCP server responds first, then the network device will use the information from the unauthorized DHCP server for the default gateway or DNS server.

Untrusted ports are connected to the DHCP clients and to traffic that originated outside the LAN. By definition, untrusted ports do not accept DHCP packets originating from a DHCP server and immediately drop them when they are detected. The DHCP packets types that are not accepted are DHCPOFFER and DHCPACK.

However, untrusted ports do accept both DHCP DISCOVER and DHCPREQUEST packets sent from DHCP clients. This behavior allows DHCP clients to respond to a trusted DHCP server and not respond to a DHCP server that is untrusted.

DHCP with Option 82

When the switch receives DHCP request packets from end nodes, it can add information before forwarding them on to the DHCP server. Referred to as Option 82, the information can be used to identify the physical locations of the nodes. Here is the Option 82 information that the switch can add to the packets.

- Remote ID: This is the MAC address of the switch.
- Circuit ID: This is the port number on the switch where the node is connected and the VLAN ID where the port is a member.
- Subscriber ID: This is not applicable to the iGS950 switch.

The process is transparent to the end nodes because they never see the Option 82 information. The switch adds the information to the ingress DHCP request packets from end nodes before forwarding the packets to the DHCP server, and removes the information from the ingress reply packets from the DHCP server. The process is illustrated in Figure 146.

Option 82 can be enabled or disabled on the switch. The default setting is disabled. If the switch is at the network edge and there are end nodes directly connected to untrusted ports, enabling the option adds the information to the DHCP request packets from the nodes.

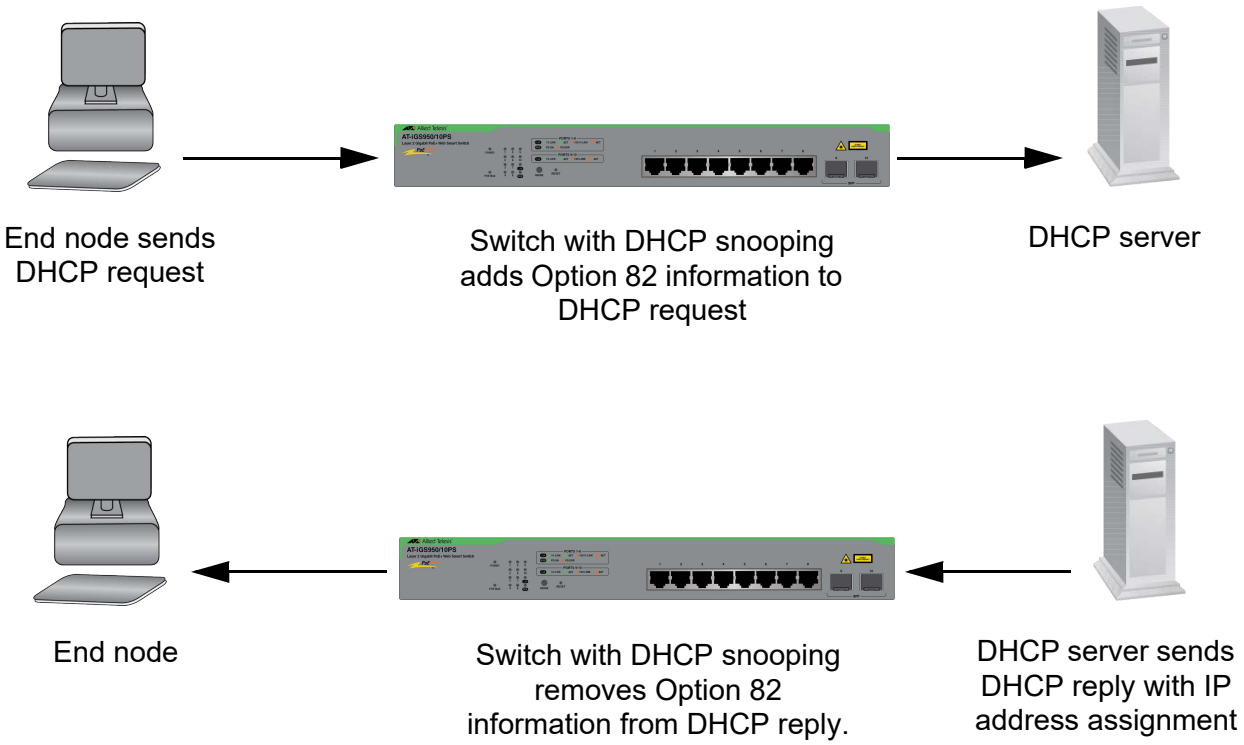


Figure 146. DHCP with Option 82

Option 82 Pass Through

As explained in the previous section, Option 82 is information the switch adds to DHCP request packets from end nodes to identify the node locations. At its default settings, the switch discards ingress DHCP request packets that already contain Option 82 information. This can occur when a switch port is connected to another switch that is adding Option 82 information to DHCP requests.

You can control this with the Option 82 pass through feature. When you enable the feature, the switch forwards ingress DHCP request packets that already contain Option 82 information. Figure 147 on page 495 illustrates what happens when Option 82 pass through is disabled and Figure 148 on page 496 when the option is enabled.

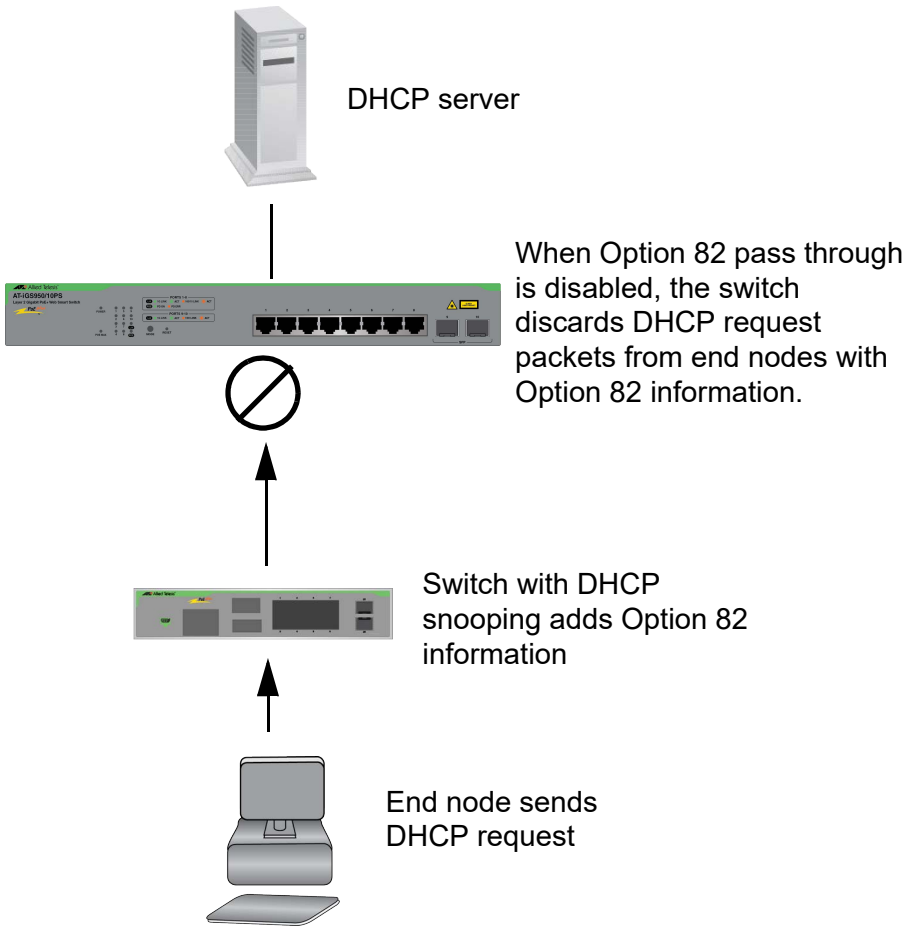


Figure 147. DHCP with Option 82 Pass Through Disabled

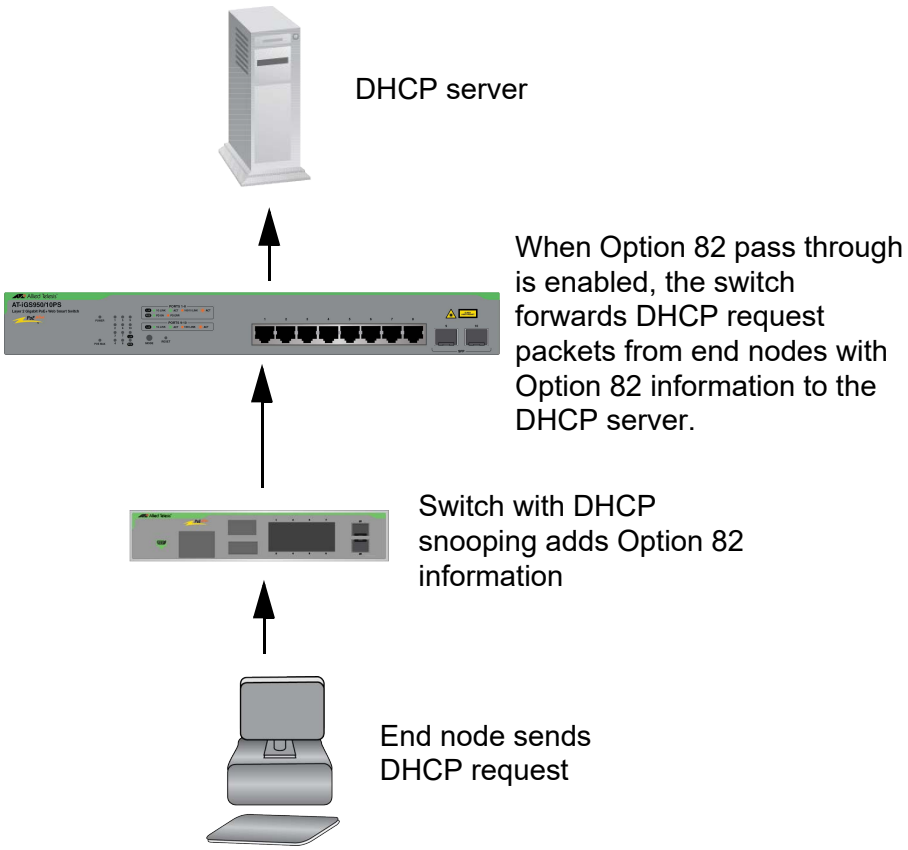


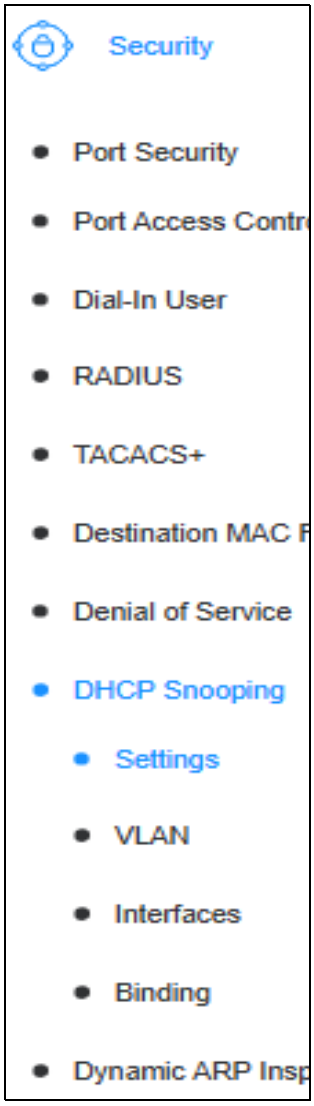
Figure 148. DHCP with Option 82 Pass Through Enabled

General Guidelines

Here is a summary of the rules to observe when configuring DHCP snooping:

- A trusted port is connected to one of the following:
  - Directly to a trusted DHCP Server.
  - A network device relaying DHCP messages to and from a trusted server.
  - Another trusted source, such as a switch with DHCP snooping enabled.
- Untrusted ports are connected to DHCP clients and to traffic that originates outside of the local area network.
- The VLANs to which the DHCP snooping feature applies must be specified in the DHCP snooping VLAN Setting configuration.
- Static IP addresses on the network have to be manually added to the Binding Database.

Configuring DHCP Snooping



Perform the following procedure to enable or disable DHCP snooping and configure its general settings:

1. Select **Security** > **DHCP Snooping** > **Settings** from the menu. The General Settings window is shown in Figure 149 on page 500.
2. Configure the fields in Table 118.
3. Click **Apply**.

Note
Select **Save** from the menu to save your changes.

4. Go to “Designating Trusted and Untrusted Ports” on page 503.
5. Go to “Adding DHCP Snooping to VLANs” on page 501.

Table 118. DHCP Snooping General Settings Window

Field	Description
DHCP Snooping	Select one of the following from the menu: - **Enabled**: Enables DHCP snooping on the designated VLANs on the switch. Refer to “Adding DHCP Snooping to VLANs” on page 501. You have to enable DHCP snooping before you can configure the settings. - **Disabled**: Disables DHCP snooping. This is the default setting.
Pass Through Option 82	Select one of the following choices from the menu: - **Enabled** - Configures the switch to forward DHCP packets with Option 82 information from nodes on untrusted ports to DHCP servers. Refer to “Option 82 Pass Through” on page 494. - **Disabled** - Configures the switch to discard DHCP packets with Option 82 information from nodes on untrusted ports. This is the default setting.

Table 118. DHCP Snooping General Settings Window (Continued)

Field	Description
Verify MAC Address	Select one of the following choices from the menu: - **Enabled** - Configures the switch to examine the MAC and IP addresses of ingress ARP packets on untrusted ports and to forward only those packets that have a match in the binding database. Invalid ARP packets are discarded. This is the default setting. - **Disabled** - Configures the switch to not verify the MAC and IP addresses of ingress ARP packet against the binding table. The switch forwards all ARP packets without regard to their IP and MAC addresses.
Backup Database	Select one of the following choices from the menu: - **Enabled** - Configures the switch to save a backup copy of the binding database to flash memory at the specified time interval. - **Disabled** - Prevents the switch from saving a backup copy of the binding database to flash memory. This is the default setting.
Database Update Interval	Enter the time interval for backing up the binding database. The range is 600 to 86400 seconds. The default is every 1200 seconds (20 minutes).
DHCP Option 82 Insertion	Select one of the following options: - **Enabled** - Inserts DHCP Option 82 information into DHCP request packets from hosts on untrusted ports and removes them from reply packets from DHCP servers. Refer to “DHCP with Option 82” on page 493. - **Disabled** - Disables the addition of DHCP Option 82 information into DHCP packets. This is the default setting.

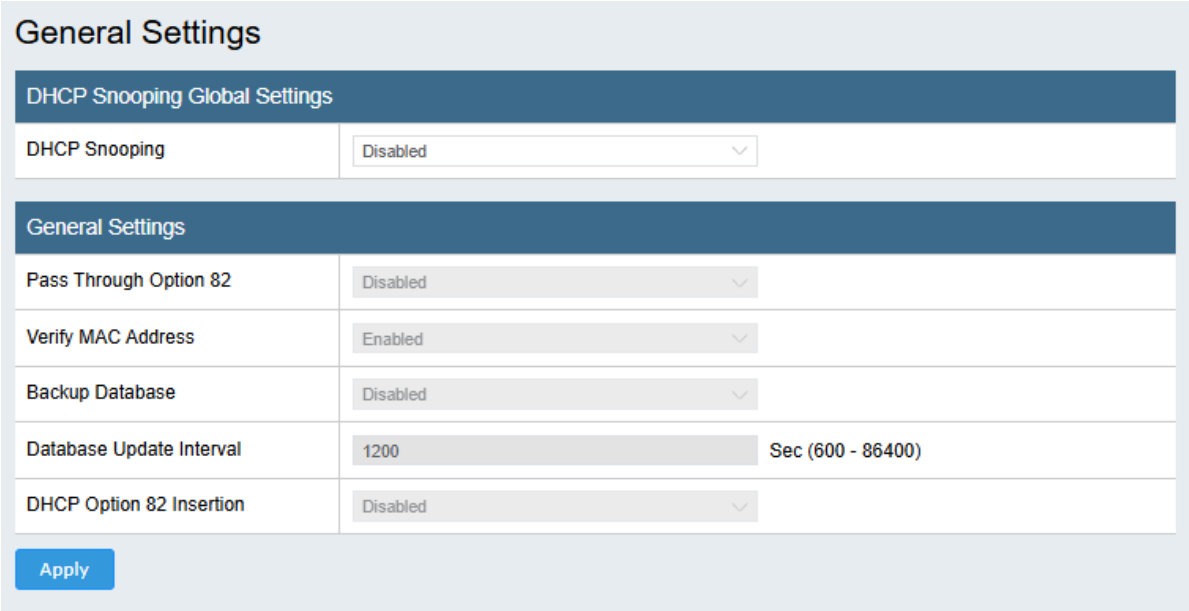
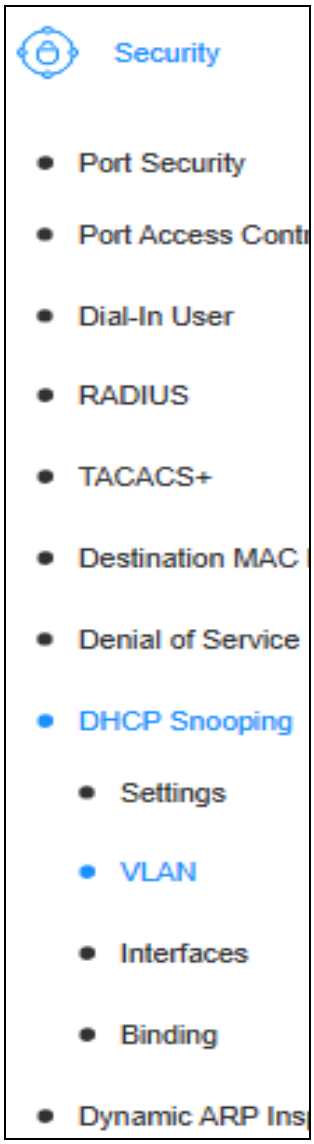


Figure 149. DHCP Snooping General Settings Window

Adding DHCP Snooping to VLANs



This section contains the procedure for adding DHCP snooping to 802.1Q tagged VLANs. Here are the guidelines:

- ❒ DHCP snooping is supported on 802.1Q tagged VLANs. Refer to Chapter 34, “802.1Q Tagged Virtual LANs” on page 337.
- ❒ DHCP snooping is not supported on port-based or private VLANs

To add DHCP snooping to 802.1Q tagged VLANs:

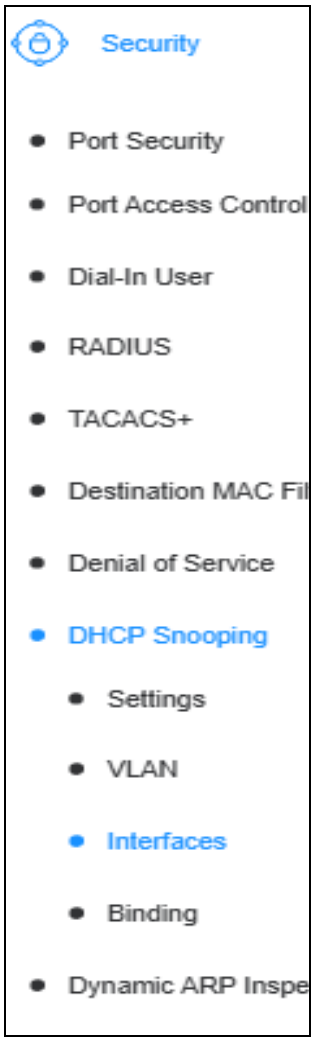
1. Select **Security** > **DHCP Snooping** > **VLAN** from the menu. The DHCP snooping VLAN Settings window is shown in Figure 150 on page 502.
2. To add DHCP snooping to an 802.1Q tagged VLAN, do the following:
   a. Enter the VID of VLAN in the **VLAN ID** field. You can add only one VLAN at a time.
   b. Click **Add**. The VLAN is added to the table. (The switch displays an error message if you enter the VID of a nonexistent 802.1Q tagged VLAN or the VLAN index number of a port-based VLAN.)
   c. Repeat this step to add DHCP snooping to more 802.1Q tagged VLANs.
3. To remove DHCP snooping from VLANs, do one of the following:
   - ❒ To remove DHCP snooping from a single VLAN, click **Delete** in the Action column of the entry.
   - ❒ To remove DHCP snooping from all the VLANs, click **Delete All**.

   Note
   Select **Save** from the menu to save your changes.

4. Go to “Designating Trusted and Untrusted Ports” on page 503 to designate ports in the VLAN as trusted or untrusted. Trusted ports are connected to authorized DHCP servers and untrusted ports to clients of the DHCP servers.

Figure 150. DHCP Snooping VLAN Settings Window

Designating Trusted and Untrusted Ports



For background information, refer to “Trusted Ports” on page 492 and “Untrusted Ports” on page 492. DHCP snooping has to be enabled for you to configure ports. Refer to “Configuring DHCP Snooping” on page 498.

To designate ports as trusted or untrusted for DHCP snooping:

1. Select **Security** > **DHCP Snooping** > **Interfaces** from the menu. The DHCP Snooping Trusted Interfaces window is shown in Figure 151.
2. In the Trust column for a port, select one of the following options from the menu:
   - **Disabled** - Defines ports as untrusted. This is the correct setting for ports connected to hosts or to devices outside the network. The switch will forward DHCP packets to and from hosts on the port, but will discard ingress packets from DHCP servers. This protects against unauthorized DHCP servers connecting to the network.
   - **Enabled** - Defines ports as trusted. This is the correct setting for posts connected to authorized DHCP servers. The switch will forward packets to and from the DHCP server on the port. This is the default setting.
3. Click **Apply** in the Action column for the port.
4. Repeat steps 2 and 3 to designate other ports as trusted or untrusted.

Note
Select **Save** from the menu to save your changes.

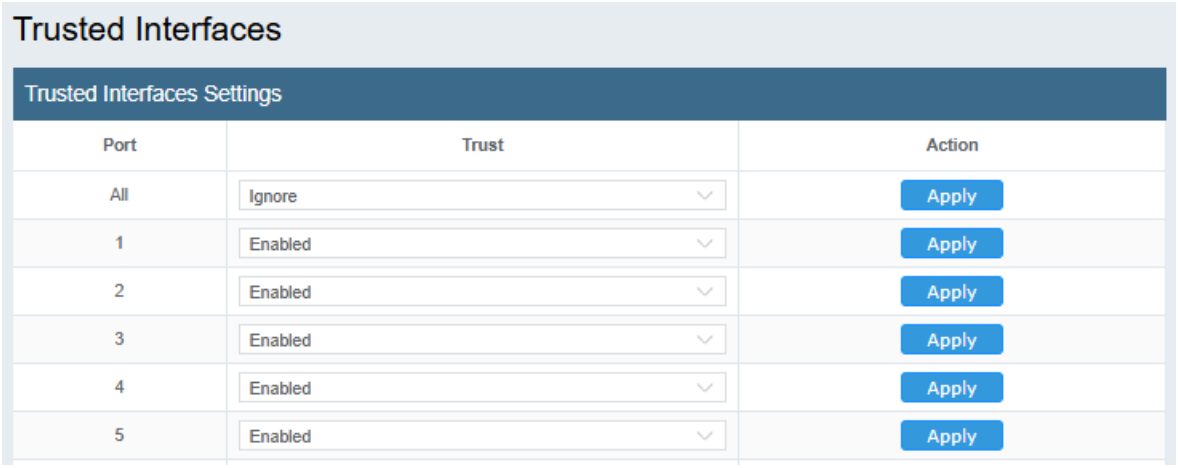
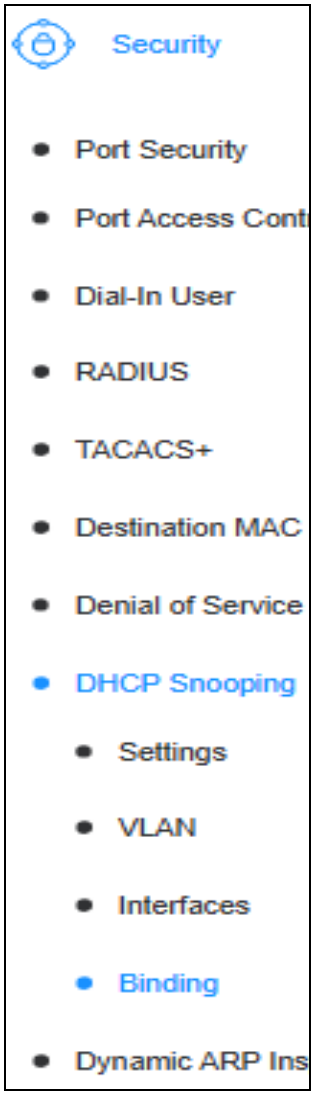


Figure 151. DHCP Snooping Trusted Interfaces Window

Managing the Binding Database

The DHCP snooping binding database contains the MAC addresses and IP addresses of the hosts on untrusted switch ports. (As explained earlier, untrusted ports are typically connected to end nodes or to devices outside the network.) The IP addresses can either be those assigned by DHCP servers or those you assigned manually. Along with the addresses the table lists the switch ports to which the hosts are connected and their VLAN assignments.

The switch builds the database by examining DHCP packets from DHCP servers on trusted ports and hosts on untrusted ports. You can also add to the database by entering static entries.



The switch uses the binding database to prevent unauthorized individuals from accessing the network on untrusted ports by transmitting fake ARP messages containing valid IP addresses. As ARP packets arrive on the ports, the switch compares their source MAC and IP addresses against the host entries in the table and discards packets that do not match the table entries.

To view or edit the entries in the binding database:

1. Select **Security** > **DHCP Snooping** > **Binding** from the menu. The Binding Database window is shown in Figure 152 on page 506.

   The table in the window displays the current dynamic and static entries of the IP address assignments to hosts. Refer to Table 119.

Table 119. DHCP Snooping Binding Database Window

Column	Description
MAC Address	Displays the host's MAC address.
VLAN	Displays the VLAN ID of the port.
IP Address	Displays the host's static IPv4 or IPv6 address.
Port	Displays the port number where the host is connected.
Type	Displays one of the following: - Static: The entry was entered manually into the database. - Learned: The switch and DHCP snooping learned the entry from a DHCP sever.

Table 119. DHCP Snooping Binding Database Window (Continued)

Column	Description
Lease Time	Displays the amount of time the IP address from the DHCP server is valid, before it has to be reauthorized. Does not apply to static entries.

2. To add a static entry, do the following:

   a. Enter the fields in Table 120.

Table 120. DHCP Snooping Binding Database Window

Field	Description
MAC Address	Enter the host's MAC address.
IP Address	Enter the host's static IPv4 or IPv6 address.
VLAN	Enter the VLAN ID.
Port	Select the port number where the host is connected, from the pull-down menu.
Type	Select **Static** from the pull-down menu.
Lease Time	Not applicable to static IP addresses.

   b. Click **Add**.

3. To delete entries, do one of the following:

   - ❒ To delete a single entry, click **Delete** in the Action column.
   - ❒ To delete all the entries, click **Delete All** above the table.

Note
Select **Save** from the menu to save your changes.

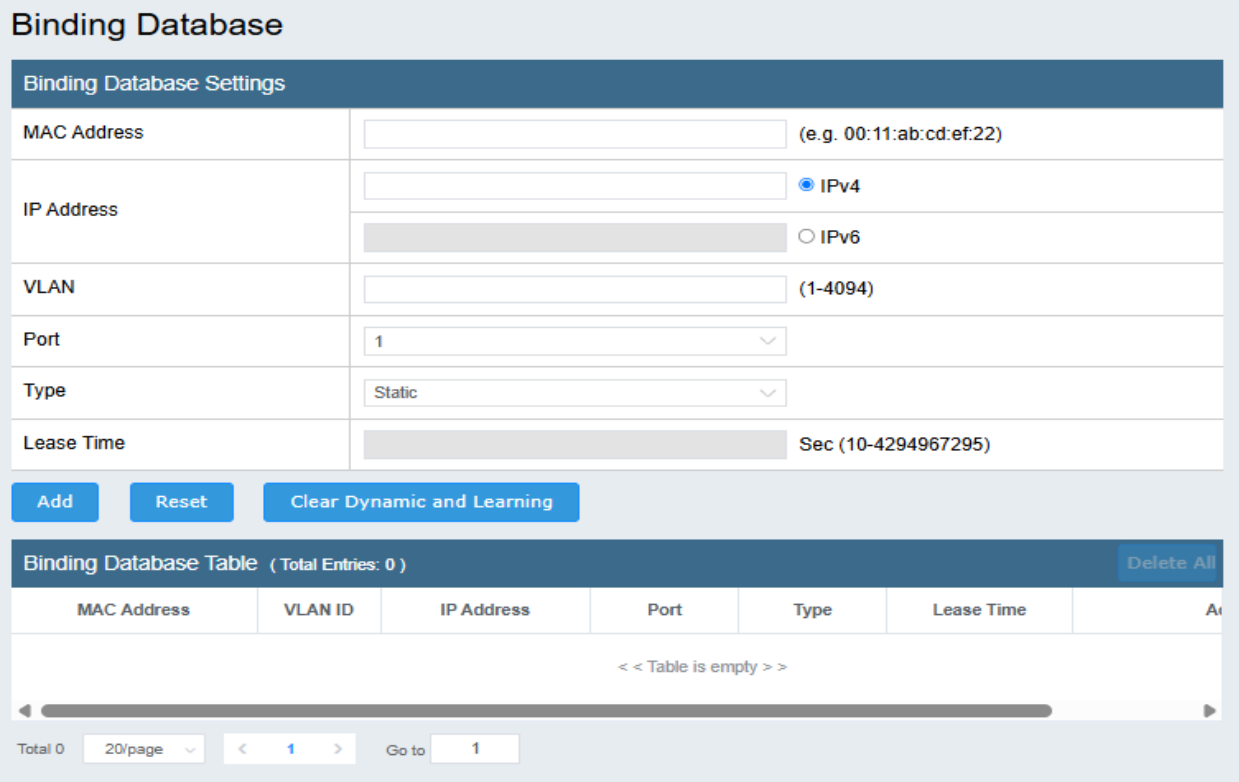


Figure 152. DHCP Snooping Binding Database Window

Chapter 52

Traffic Rules and Policies

This chapter describes traffic rules and policies in the following sections.

- “Traffic Rules and Policies Overview” on page 508
- “Adding IP Rules” on page 511
- “Adding L2 Rules” on page 514
- “Editing, Modifying or Deleting Policies” on page 516
- “Finding Policies” on page 517

Traffic Rules and Policies Overview

Traffic rules and policies function as packet filters on switch ports. You can use them to control the flow of ingress packets on ports by designating the types of packets the switch accepts or discards on ports. You might use the rules and policies to increase port security or to add physical links that are dedicated to carrying specific types of traffic. For instance, you might add policies to ports so that they accept only those ingress packets that have a specific source or destination IP or MAC address, and to reject all other packets.

Note
Before adding rules, be sure to configure the QoS parameters. QoS entries may have a direct effect on a policy's behavior. For more information, refer to Chapter 42, "Quality of Service and Class of Service" on page 409.

Policy Filters

You can add IPv4 or IPv6 port policies. The two types of policies support different sets of filters. Here are the available filters for IPv4 ingress packets:

- Source or destination MAC address
- Source or destination IPv4 address
- VLAN ID
- Ether type
- Ethernet protocol
- DSCP
- Source Transport Layer 4 Port

Here are the filters for IPv6 ingress packets:

- Source or destination IPv6 address
- VLAN ID
- 802.1p priority
- IPv6 traffic class
- Source Transport Layer 4 Port

Actions

The policy action defines a port's response to packets that match the filtering criterion of a policy. There are two actions:

- Permit - Instructs ports to accept ingress packets that match the policy.
- Deny - Instructs ports to discard ingress packets that match the policy.

Ports, by default, forward all ingress packets. Thus, a policy with a permit action is only required when you want a port to forward a subset of packets of a larger traffic flow that are otherwise to be blocked.

How Ingress Packets are Compared Against Policies

Ports that do not have any policies forward all ingress packets. Ports with one or more deny ACLs discard ingress packets that match the ACLs and forward all other traffic. A port that has one deny ACL that specifies a particular source IP address, for example, discards all ingress packets with that source address and forwards all other traffic. In situations where a port has more than one deny ACL, packets are discarded at the first match.

Since ports forward all ingress packets unless they have deny ACLs, permit ACLs are only necessary in situations where you want a port to forward packets that are a subset of a larger traffic flow that is to be blocked. An example is a port that is to forward only packets having a specified destination IP address. A permit ACL would specify the packets with the permitted destination IP address and a deny ACL would specify all traffic.

ACLs are assigned policy sequence numbers that control the order in which the switch uses them to filter packets when there are multiple ACLs on ports. The lower the number the higher the priority. The range is 1 to 65535. It is important to assign permit policies lower sequence numbers than deny policies so that packets are compared against them first when ports have both permit and deny ACLs. For example, you might reserve sequence numbers 1 to 500 for permit ACLs and numbers 501 to 1000 for deny ACLs.

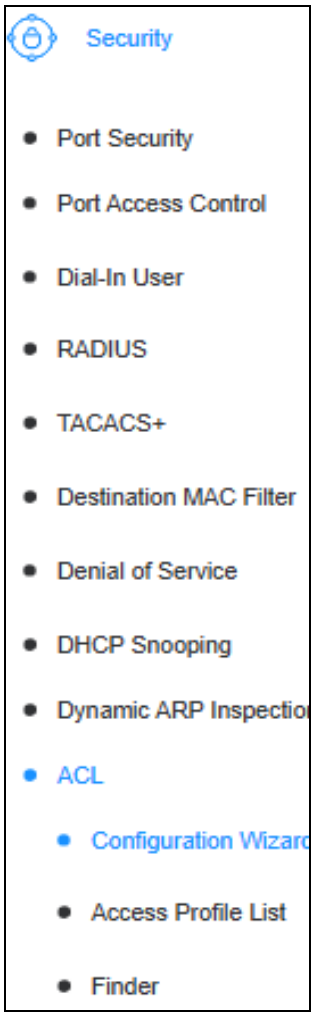
Guidelines

Here are the policy guidelines:

- The policy action can be permit or deny. Permit actions allow ports to accept ingress packets of the designated traffic flows while deny actions cause ports to discard packets.
- A port can have more than one policy.
- A policy can be assigned to more than one port.
- You cannot assign a policy more than once to the same port.
- Policies filter ingress packets on ports, but not egress packets. Therefore, policies have to be applied to the ingress ports of traffic flows.
- Policies for static port or LACP trunks have to be assigned to all the member ports of the trunks.
- Policies are assigned sequence numbers that determine the order in which they are performed on ports that have more than one policy. The range is 1 to 65535.

- On ports that have more than one policy, packets are compared against the policies in the order of the policy sequence numbers, from lowest to highest. Packets are forwarded or discarded at the first match.
- Ports can have policies with different filtering criteria. A port, for example, could have policies that filter on a source IP address and a VLAN ID.
- Because ports, by default, forward all ingress packets, permit policies are only required when ports are to forward packets that are subsets of larger packet flows that are blocked by deny policies.

Adding IP Rules



To add IP rules that filter on source and/or destination MAC addresses on switch ports:

1. Select **Security** > **ACL** > **Configuration Wizard** from the menu. The ACL Configuration Wizard window is shown in Figure 153 on page 513.
2. Select the **Add IP Rule** button at the top of the window. This is the default setting. Refer to Figure 153 on page 513.
3. Configure the IP Rule policy fields in Table 121.
4. Click **Apply** to activate the policy on the switch, or **Cancel** to cancel the procedure. To view the policy, refer to “Finding Policies” on page 517.

Table 121. IP Rule Policy Window for IP Rules and MAC Addresses

Field	Description
Source	To filter ingress packets based on a source MAC address, select one of the following from the pull-down menu: ❒ Any - Select this option to have the policy match all source MAC addresses. ❒ MAC Address - Select this option to enter one MAC address in the adjoining field. Masks are not supported.
Destination	To filter ingress packets based on a destination MAC address, select one of the following from the pull-down menu: ❒ Any - Select this option to have the policy match all source MAC addresses. ❒ MAC Address - Select this option to enter one MAC address in the adjoining field. Masks are not supported.

Table 121. IP Rule Policy Window for IP Rules and MAC Addresses

Field	Description
Service Type	To filter ingress packets based on an Ethernet frame protocol number, select one of the following from the pull-down menu: ❒ Any - Select this option to have the policy match all service types. ❒ EtherType - Select one of the following: – IP (0x800) – ARP (0x806) – User Define
Action	Select the action the switch performs on ingress packets that match the policy. The choices are listed here: - Permit: Forward packets. - Deny: Discard packets. - Rate Limit - The range is 16 to 1000000 (the entered value is multiplied by 16) - Replace 1p Priority - The range is 0 to 7. - Replace DSCP The range is 0 to 63
Port	Enter the switch ports to which the policy is to be assigned. The port list can be specified as a consecutive list, a non-consecutive list, or a combination of the two. For example, you can specify ports 1-3,5,8. A policy has to have at least one port. You cannot mix individual ports and ports of a port trunk in a port list. For example, if ports 3 and 4 are members of a trunk, you may not assign ports 1-4 in the port list, but you may assign ports 3 and 4.

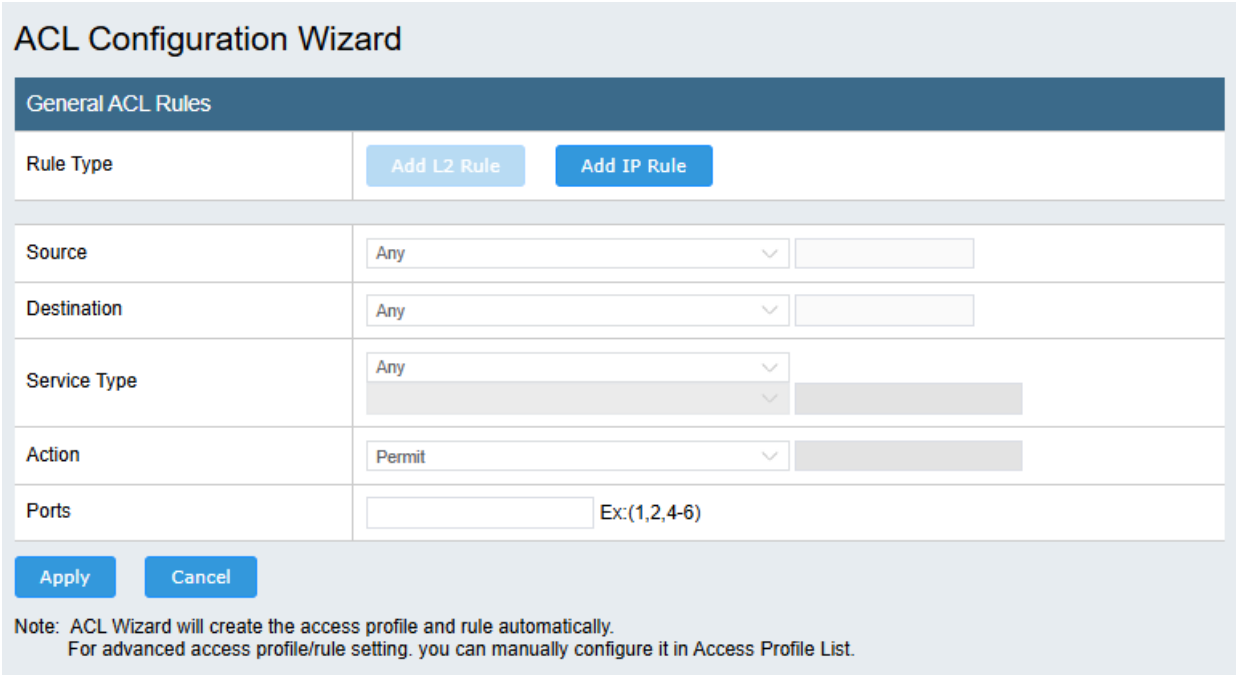
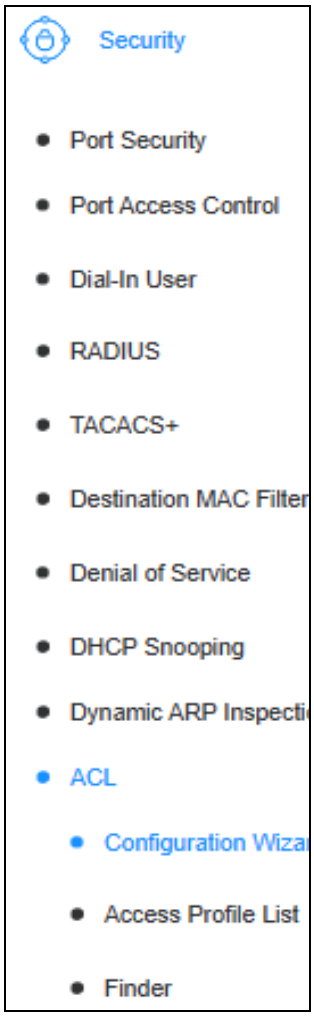


Figure 153. ACL Configuration Wizard Window

Adding L2 Rules



To add L2 rules that filter on source and/or destination IPv4 or IPv6 addresses on switch ports:

1. Select **Security** > **ACL** > **Configuration Wizard** from the menu. The Policy Settings window is shown in Figure 153 on page 513.
2. Click the **Add IP Rule** button to activate the **Add L2 Rule** button at the top of the window. The rule window is shown in Figure 153 on page 513.
3. Configure the L2 Rule policy fields in Table 122.
4. Click **Apply** to activate the policy on the switch, or **Cancel** to cancel the procedure. To view the policy, refer to “Finding Policies” on page 517.

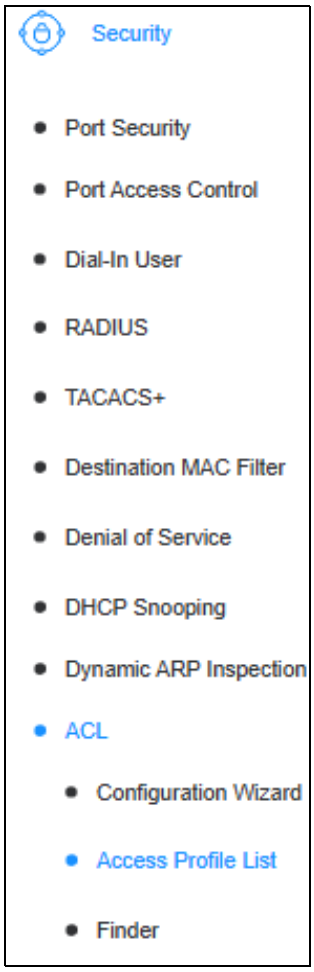
Table 122. IP Rule Policy Window for L2 Rules and IP Addresses

Field	Description
Source	To filter ingress packets based on a source IPv4 or IPv6 address, select one of the following from the pull-down menu: ❒ Any - Select this option to have the rule match all IPv4 and IPv6 addresses. ❒ IPv4 - Select this option to enter an IPv4 address in the adjoining field. Masks are supported. ❒ IPv6 - Select this option to enter an IPv6 address in the adjoining field. Masks are supported.
Destination	To filter ingress packets based on a destination IPv4 or IPv6 address, select one of the following from the pull-down menu: ❒ Any - Select this option to have the rule match all IPv4 and IPv6 addresses. ❒ IPv4 - Select this option to enter an IPv4 address in the adjoining field. Masks are supported. ❒ IPv6 - Select this option to enter an IPv6 address in the adjoining field. Masks are supported.

Table 122. IP Rule Policy Window for L2 Rules and IP Addresses

Field	Description
Service Type	To filter ingress packets based on service type, select one of the following from the pull-down menu: ❒ Any - Select this option to have the rule match all service types. ❒ ICMP All ❒ IGMP ❒ TCP All ❒ TCP Source Port ❒ TCP Destination Port ❒ UDP All ❒ UDP Source Port ❒ UDP Destination Port
Action	Select the action the switch performs on ingress packets that match the policy. The choices are listed here: - Permit: Forward packets. - Deny: Discard packets. - Rate Limit - The range is 16 to 1000000 (the entered value is multiplied by 16) - Replace 1p Priority - The range is 0 to 7. - Replace DSCP The range is 0 to 63
Port	Enter the switch ports to which the policy is to be assigned. The port list can be specified as a consecutive list, a non-consecutive list, or a combination of the two. For example, you can specify ports 1-3,5,8. A policy has to have at least one port. You cannot mix individual ports and ports of a port trunk in a port list. For example, if ports 3 and 4 are members of a trunk, you may not assign ports 1-4 in the port list, but you may assign ports 3 and 4.

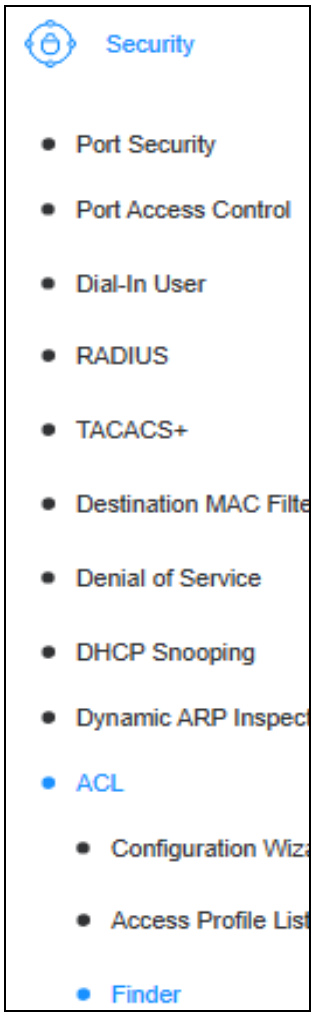
Editing, Modifying or Deleting Policies



To edit, modify or delete policies:

1. Select **Security** > **ACL** > **Access Pofile List** from the menu.
2. Do one of the following:
   - ❒ To view the details of a policy, click **Show Details.**
   - ❒ To edit a policy, click **Edit/New Rules**. Refer to Table 121 on page 511 or Table 122 on page 514.
   - ❒ To delete a policy, click **Delete.**
3. Select **Save** in the menu to save your changes.

Finding Policies



To find a policy on the switch:

1. Select **Security** > **ACL** > **Finder** from the menu. The ACL Finder window is shown in Figure 154.
2. Set one or more of the following policy filters:
   - ❒ Profile Type
   - ❒ Profile ID number
   - ❒ Ports
3. Click **Find**. The results are displayed at the bottom of the window.

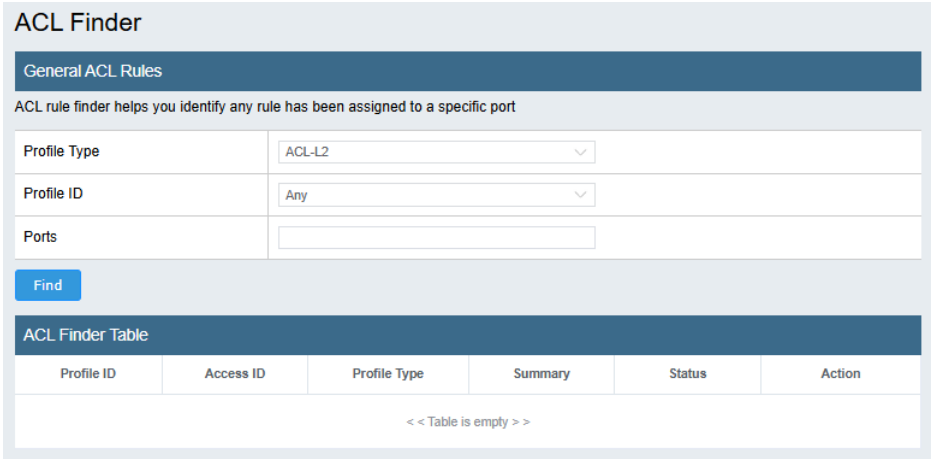


Figure 154. ACL Finder Window

Section VII

Tools Menu

This section contains the following chapter:

- Chapter 53, “Switch Firmware” on page 521
- Chapter 54, “Configuration Files” on page 531
- Chapter 55, “Troubleshooting Tools” on page 539

Chapter 53
Switch Firmware

This chapter contains instructions on upgrading the management software on the switch and selecting the active software management image:

- ❒ “Management Software Overview” on page 522
- ❒ “Upgrading the Management Software with HTTP” on page 523
- ❒ “Backing Up the Management Software with HTTP” on page 525
- ❒ “Upgrading the Management Software with TFTP” on page 526
- ❒ “Backing Up the Management Software with TFTP” on page 528
- ❒ “Designating the Boot Management Software” on page 529

Management Software Overview

Allied Telesis may periodically release new versions of the management software for this product and post them on its web site for customers to download. Refer to the Allied Telesis web site for details.

The switch maintains two copies of the management software in flash memory. The versions are called Image1 and Image2. One of the images will be the active image and the other a backup. The switch uses the active image when it is booted or powered on.

When you download a new firmware image, the switch stores it as the inactive image. It then makes that image active and the other inactive. Here is an example. Assume that Image1 is active and Image2 is inactive. When the switch receives a new firmware image, it stores it as Image2 because that is the inactive image. After completing the download process, it makes Image2 the active image and Image 1 the inactive image.

If the switch is unable to initialize the active image or you believe there is a problem with it, you can manually instruct the switch to use the inactive image instead the next time the device is booted. Refer to “Designating the Boot Management Software” on page 529.

There are two ways to download new management software to the switch. One way is with your web browser on your management workstation, explained in “Upgrading the Management Software with HTTP” on page 523. The other is with a TFTP server, explained in “Upgrading the Management Software with TFTP” on page 526.

Upgrading the Management Software with HTTP

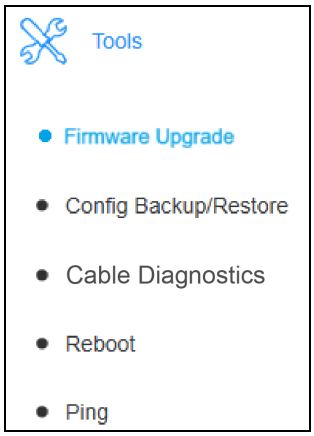
This section contains the procedure for upgrading the management software on the switch using HTTP on a web browser. Review the following guidelines:

- The switch This procedure assumes you have already obtained the new management software from the Allied Telesis web site and stored it on your computer.
- The switch retains its current configuration when new management software is installed.
- The switch stores the new firmware as the inactive image. After downloading the new firmware, you have to designate it as the active image and reboot the switch before it will use the new firmware. Refer to “Management Software Overview” on page 522.

Caution
Do not power off the switch during the software upgrade. Interrupting the transfer may corrupt the firmware on the switch.

Note
The switch does not forward network traffic while it uploads the management software from your computer and writes it to flash memory. To minimize the disruption of the upgrade procedure to network operations, you should perform this procedure during periods of low traffic activity, such as during non-business hours.

Note
Do not close the web browser window or change to a different window until the entire procedure is finished. Interrupting the transfer may corrupt the file on the switch.



Perform the following procedure to upgrade the management software on the switch with your web browser and HTTP:

1. Select **Tools** > **Firmware Upgrade** from the menu.

   The Next Boot Image ID and Running Image ID in the window are explained in “Designating the Boot Management Software” on page 529.

The Image1 Version and Image2 Version fields display the version numbers of the active and backup management software, respectively, on the switch. For background information, refer to “Management Software Overview” on page 522.

The Firmware Upgrade via HTTP window is shown in Figure 155.

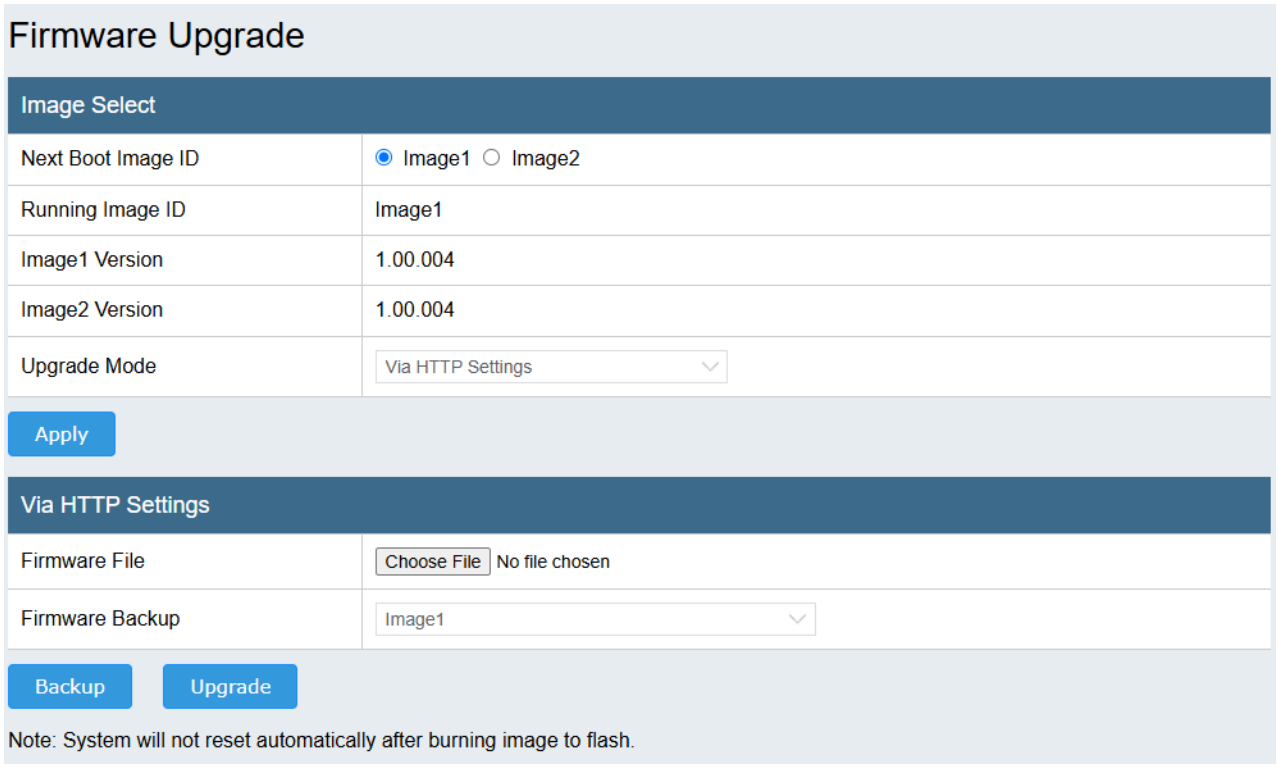


Figure 155. Firmware Upgrade Via HTTP Settings Window

2. In the Upgrade Mode line, click **Via HTTP Settings**. This is the default setting.
3. In the Firmware File line, click **Choose File**.
4. When prompted, locate the new management software file on your computer.
5. Click **Upgrade** to begin the upgrade process.

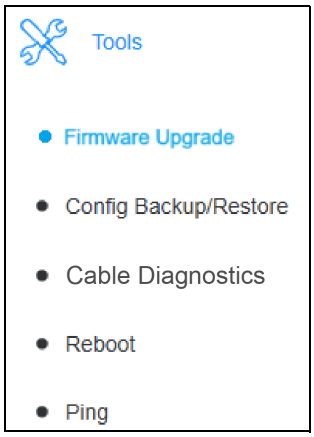
> **Note**
> The switch needs to be restarted manually after downloading and verifying the management software, and writing it to flash memory. The entire process takes several minutes.

6. To resume managing the switch at the completion of the upgrade, start a new management session.

Backing Up the Management Software with HTTP

The procedure in this section instructs the switch to send a copy of its active management software image file to your management workstation using HTTP.

Note
Although the transfer takes only a few seconds, the procedure should be performed only during periods of low or no network activity.



To store a backup copy of the switch's management software on your management workstation, perform the following procedure:

1. Select **Tools** > **Firmware Upgrade** from the menu.
2. In the Upgrade Mode line, select **Via HTTP Settings**. This is the default setting. Refer to Figure 155 on page 524.
3. In the Firmware Backup line, select either **Image1** or **Image2** to backup.
4. Click **Backup**. The switch sends a copy of the designated image file to your management workstation. The transfer takes only a few seconds.

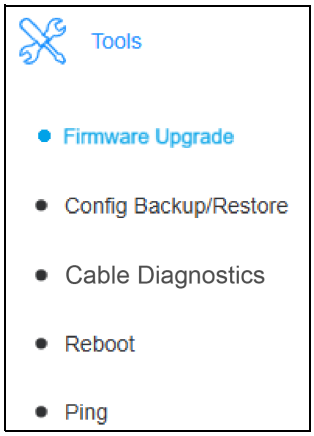
Upgrading the Management Software with TFTP

This section contains the procedure for upgrading the management software on the switch using TFTP. Review the following:

- This procedure assumes that you have already obtained the new management software from the Allied Telesis web site and stored it on your TFTP server.
- The switch retains its current configuration when new management software is installed.
- Start the TFTP server software before beginning the download procedure.
- The switch stores the new firmware as Image1 and renames its previous active firmware as Image2. For background information, refer to “Management Software Overview” on page 522.

Caution
Do not power off the switch during the software upgrade. Interrupting the transfer may corrupt the file on the switch.

Caution
The switch does not forward network traffic while it uploads the management software from your computer and writes it to flash memory. To minimize the disruption of the upgrade procedure to network operations, you should perform this procedure during periods of low traffic activity, such as during non-business hours.



Perform this procedure to download new management software to the switch from a TFTP server:

1. Start the TFTP server on your network.
2. Select **Tools** > **Firmware Upgrade** from the menu to display the Firmware Upgrade window.
3. In the Upgrade Mode line of the window, select **Via TFTP Settings**. The Firmware Upgrade via TFTP window is shown in Figure 156 on page 527.

   The Image1 Version and Image2 Version fields display the version numbers of the active and backup management software, respectively, on the switch. For background information, refer to “Management Software Overview” on page 522

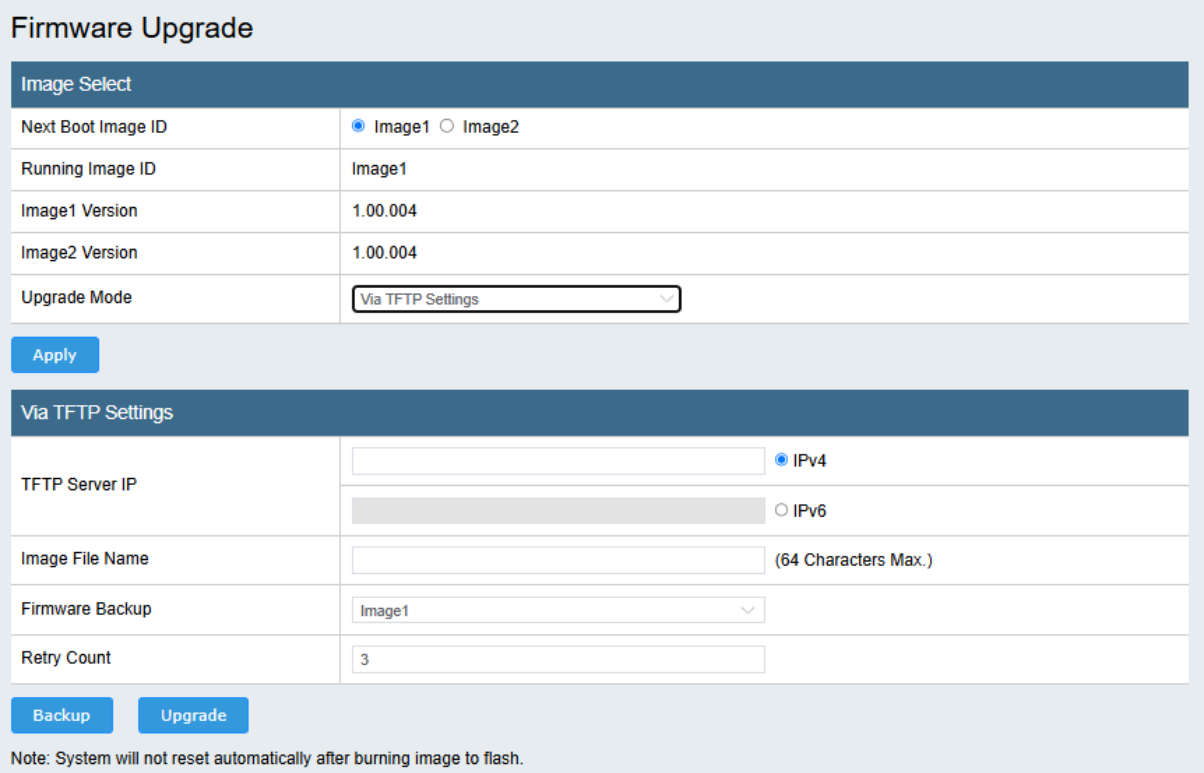


Figure 156. Firmware Upgrade via TFTP Settings Window

4. In the TFTP Server IP line, click either the **IPv4** or **IPv6** radio circle and enter the IP address of the TFTP server.

5. In the Firmware File Name line, enter the filename of the management software on the TFTP server.

6. In the Retry Count field, enter the number of times the switch is to retry the firmware upgrade if it encounters a problem downloading the firmware. The range is 1 to 20.

7. Click **Upgrade**.

Note
The switch needs to be restarted manually after it downloads and verifies the management software, and writes it to flash memory. This entire process takes several minutes.

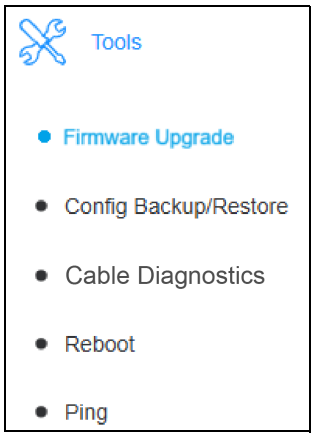
8. To resume managing the switch at the completion of the upgrade, start a new management session.

Backing Up the Management Software with TFTP

The procedure in this section instructs the switch to send a copy of its active management software image file to a TFTP server on your network.

Note
Although the transfer takes only a few seconds, the procedure should be performed only during periods of low or no network activity.

To store a backup copy of the switch's active management software image on a TFTP server, perform the following procedure:



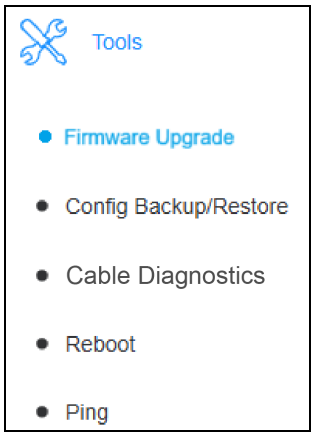
1. Select **Tools** > **Firmware Upgrade** from the menu.
2. In the Upgrade Mode line, select **Via TFTP Settings**. Refer to Figure 156 on page 527.
3. In the TFTP Server IP line, click either the **IPv4** or **IPv6** radio circle and enter the IP address of the TFTP server.
4. In the Firmware File Name line, enter the filename for the management software on the TFTP server.
5. In the Retry Count field, enter the number of times the switch is to retry downloading the firmware if it encounters a problem. The range is 1 to 20.
6. In the Firmware Backup line, select either **Image1** or **Image2** to backup.
7. Click **Backup**. The switch sends a copy of the designated image file to the TFTP server. The transfer takes only a few seconds.

Designating the Boot Management Software

The switch maintains two copies of its management software, labeled image1 and image2. By default, the switch uses image1 as its active management software whenever it starts up. It uses the image2 management software if it detects a problem with image1.

This procedure explains how you can designate which image file the switch is to use the next time it is restarted. You might perform this procedure if there is a problem with the active image file. Refer to “Management Software Overview” on page 522 for background information.

To designate image1 or image2 as the active management software the next time the switch boots, perform the following procedure:



1. Select **Tools** > **Firmware Upgrade** from the menu.

   The Firmware Upgrade via HTTP window is shown in Figure 155 on page 524.

2. Click either the **Image1** or **Image2** radio button to designate which management software is to be the active image file the next time the switch is restarted. The default is Image1.

3. Click **Apply**.

4. To have the switch to load and activate the select image file now, reboot the switch. Refer to “Rebooting the Switch” on page 541. The switch uses the designated image file as its active management software.

Chapter 54

Configuration Files

This chapter explains how to designated the active configuration file on the switch, and how to upload and download switch configuration files to your management workstation or TFTP server. The sections are listed here:

- ❒ “Overview to Switch Configuration Files” on page 532
- ❒ “Designating the Active Configuration File” on page 533
- ❒ “Backing Up Configuration Files from the Switch with HTTP” on page 535
- ❒ “Restoring Configuration Files to the Switch with HTTP” on page 536
- ❒ “Backing Up Configuration Files from the Switch with TFTP” on page 537
- ❒ “Restoring Configuration Files to the Switch with TFTP” on page 538

Overview to Switch Configuration Files

The switch immediately implements your changes to its parameter settings as soon you enter them in the web browser interface and click **Apply**. However, your changes are not permanently saved and will be lost if you reboot or power cycle the switch without first saving them in one of its two configuration files in flash memory, with the **Save** selection at the bottom of the menu. Once your changes are saved in a configuration file, the switch retains them even when rebooted or powered off.

The switch has two configuration files labeled Config 1 and Config 2. One file is active and the other is inactive. Config 1 is the default active file. Reasons for having both active and inactive configuration files are given here:

- You might use the inactive file as a backup to the active file so that if the latter becomes damaged or corrupted, you can quickly restore the switch settings.
- You can use the inactive file to return the switch to an earlier configuration. For example, if you make changes to the switch's configuration and save them to Config 1 but not Config 2, you can restore the previous configuration by instructing the switch to boot up with the Config 2 file, if needed. This is explained in "Designating the Active Configuration File" on page 533.
- Finally, you can use the inactive file to download a new configuration for switch, but not immediately implement it on the device. For instance, you might download a new configuration file to the Config 2 file early in the day, but not configure the switch with it until non-business hours, to avoid disrupting the work of your network users. This is explained in "Designating the Active Configuration File" on page 533.

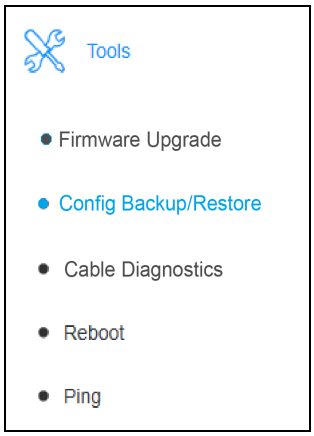
You can upload the Config 1 and Config 2 configuration files from the switch and store them on your computer or TFTP server, and later download them back to the switches, if needed. This is useful in maintaining configuration histories of switches, configuring replacement units, or quickly configuring switches that are to have similar configurations.

Designating the Active Configuration File

As explained in “Overview to Switch Configuration Files” on page 532, the switch has two configuration files, labeled Config 1 and Config 2, for storing its configuration settings. Only one configuration file is active at a time. The other file is inactive. The Config 1 file is the default active file, and Config 2 is default inactive file.

This section contains the procedure for changing the designations of the files. This can be useful if you need to return the switch to an earlier configuration or activate a configuration that you downloaded as the inactive file, and now want to activate.

To change the designated active configuration file, perform the following procedure:



1. Select **Tools** > **Config Backup/Restore** from the menu.

   The Config File Backup/Restore via HTTP window is shown in Figure 157 on page 534.

2. In the Configure Select section of the window, click the dialog circle for either **Config 1** or **Config 2** for Boot Up Configure File.

3. Click **Apply**.

   The selected configuration file is now the active configuration file on the switch.

Note
If you want to reconfigure the switch with the settings in the newly designated active configuration file, reboot the switch. Refer to “Rebooting the Switch” on page 541.

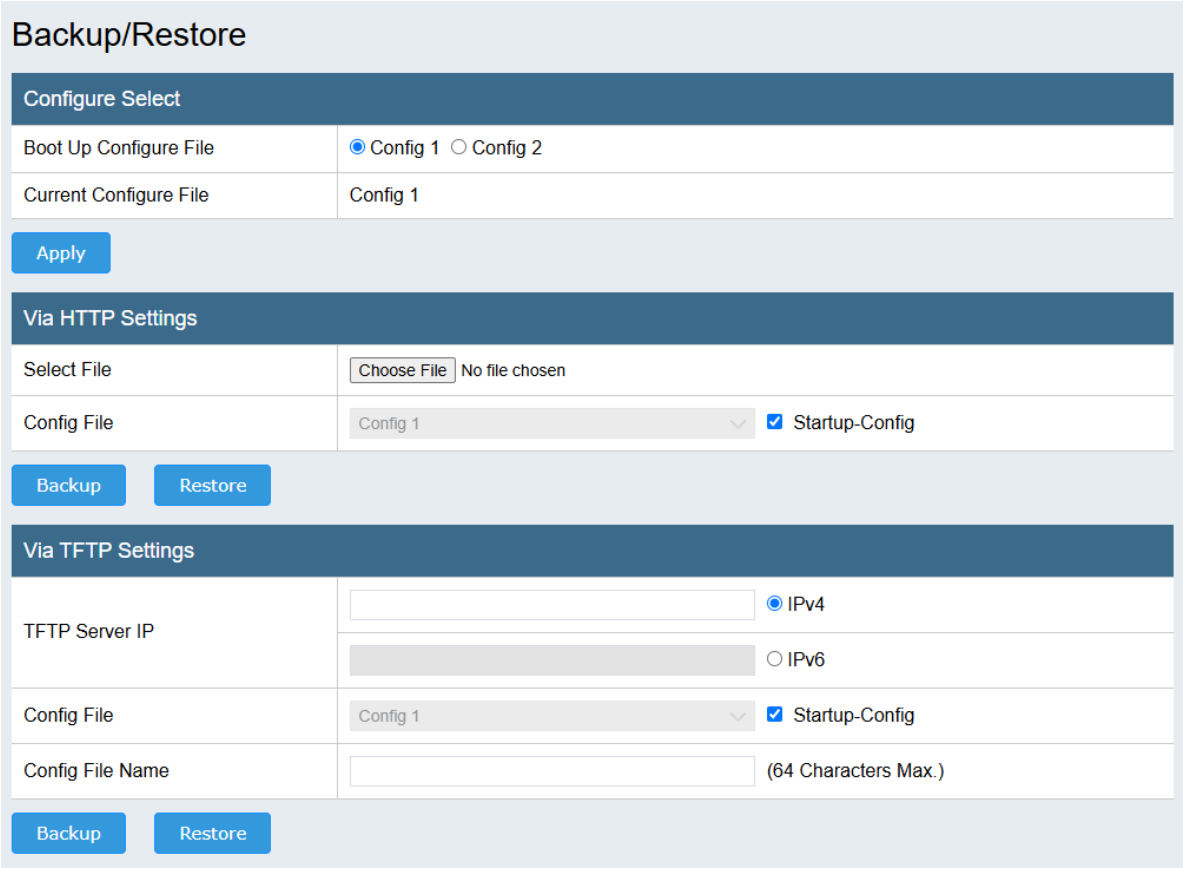
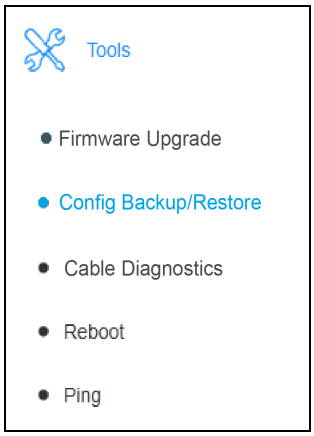


Figure 157. Backup/Restore Window

Backing Up Configuration Files from the Switch with HTTP

This section contains the procedure for uploading the Config 1 or Config 2 configuration file from the switch to your computer using HTTP. You might perform this procedure to maintain configuration histories of the switches so that you can quickly configure replacement units or switches that are to have similar settings. Refer to “Overview to Switch Configuration Files” on page 532.

To upload a configuration file from the switch to your computer using HTTP, perform the following procedure:



1. Select **Tools** > **Config Backup/Restore** from the menu.

   The Backup/Restore window is shown in Figure 157.

2. In the Via HTTP Settings section of the window, use the Config File option to select the configuration file you want to upload:

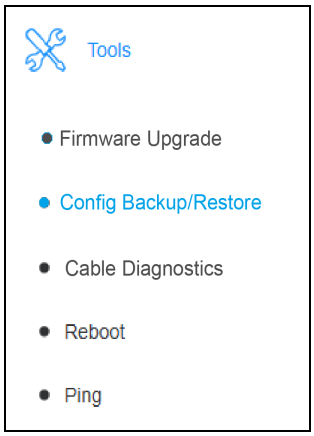
   - ❒ To upload the active configuration file. go to the next step.
   - ❒ To upload the inactive configuration file, click **Startup-Config** to remove the check mark and select the inactive file from the pull-down menu.

3. Click **Backup** in Via HTTP Settings. The switch sends the configuration file to your computer, which stores it in its Downloads folder. The filename extension is BIN.

Restoring Configuration Files to the Switch with HTTP

Perform the following procedure to restore a configuration file on your computer to replace the Config 1 or Config 2 file on the switch:

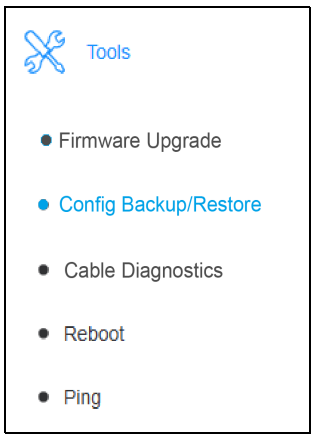
Note
Replacing the active configuration file causes the switch to immediately reboot, disrupting network operations.



1. Select **Tools** > **Config Backup/Restore** from the menu. The Backup/Restore window is shown in Figure 157 on page 534.
2. In the Via HTTP Settings section of the window, click the **Choose File** button in the Select File field.
3. Locate the configuration file on your computer.
4. Use the Config File option to select the configuration file you want to replace on the switch with the downloaded file. The default is the active file. Review the following:
   - ❒ To replace the active configuration file, skip this step and go to step 6.
   - ❒ To replace the inactive configuration file, perform the following:
   a. Click the **Startup-Config** option to remove the check mark from its dialog box.
   b. Select the inactive file (for example, Config2) from the menu.
5. Click **Restore**.

   The switch downloads the file from your computer and replaces the designated Config 1 or Config 2 file. Review the following:
   - ❒ If you replace the active configuration file, the switch automatically reboots to load its new configuration.
   - ❒ If the new configuration file has a different IP address for the switch than the previous configuration, be sure to use the new address when starting future management sessions.

Backing Up Configuration Files from the Switch with TFTP



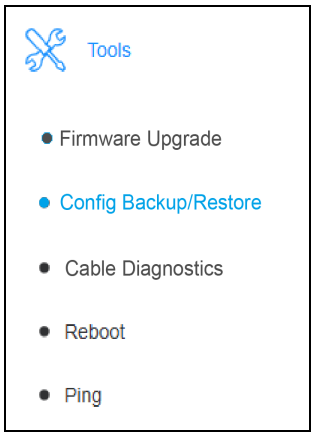
To backup the Config 1 or Config 2 configuration file on the switch to a TFTP server, perform the following procedure:

1. Start the TFTP server on your network.
2. Select **Tools** > **Config Backup/Restore** from the menu. The Backup/Restore window is shown in Figure 157 on page 534.
3. In the Via TFTP Settings section of the window, click either the **IPv4** or **IPv6** dialog circle and enter the IP address of the TFTP server on your network in the adjoining field. The default is IPv4.
4. With the **Config File** option, select the configuration file you want to upload. The default is the active configuration file. To select the inactive configuration file, click the **Startup-Config** dialog box to remove the check mark, and select the configuration file from the pull-down menu.
5. In the **Config File Name** field, enter a filename for the configuration file when stored on the TFTP server. The maximum length is 64 alphanumeric characters. Spaces and special characters are not allowed. The extension has to be “bin”.
6. Click **Backup**. The switch copies the file to the TFTP server.

Restoring Configuration Files to the Switch with TFTP

Perform the following procedure to restore the Config 1 or Config 2 configuration file to the switch from a TFTP server:

Note
Replacing the active configuration file causes the switch to immediately reboot, disrupting network operations.



1. Start the TFTP server on your network and store the configuration file on the server.
2. Select **Tools** > **Config Backup/Restore** from the menu. The Backup/Restore window is shown in Figure 157 on page 534.
3. In the Via TFTP Settings section of the window, click either the **IPv4** or **IPv6** dialog circle for TFTP Server IP and enter the IP address of the TFTP server on your network in the field. The default is IPv4.
4. With the Config File option, select whether the downloaded configuration file is to replace the active or inactive file. The default is the active file. Do one of the following:
   - ❒ To replace the active configuration file, skip to the next step.
   - ❒ To replace the inactive file, perform the following steps:

   a. Click the **Startup-Config** option to remove the check mark from its dialog box.

   b. Select the inactive file from the pull-down menu.
5. In the **Config File Name** field, enter the filename of the configuration file on the TFTP server. If necessary, include the directory path of the file on the server. The extension has to be “bin”.
6. Click **Restore**.

   The switch downloads the file from the TFTP server and replaces the Config 1 or Config 2 file, according to your selection in step 4. Review the following:
   - ❒ If you replace the active configuration file, the switch automatically reboots to load the new configuration.
   - ❒ If the new configuration file has a different IP address for the switch than the previous configuration, be sure to use the new address when starting future management sessions.

Chapter 55

Troubleshooting Tools

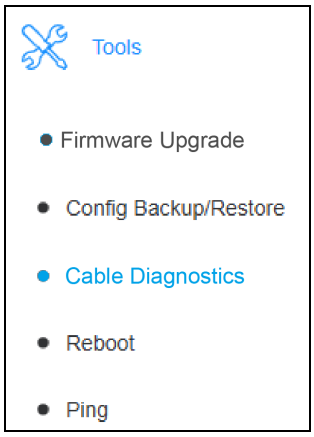
This chapter describes the following troubleshooting tools:

- ❒ “Cable Diagnostics” on page 540
- ❒ “Rebooting the Switch” on page 541
- ❒ “Restoring the Factory Default Values” on page 543
- ❒ “Pinging Network Devices” on page 544

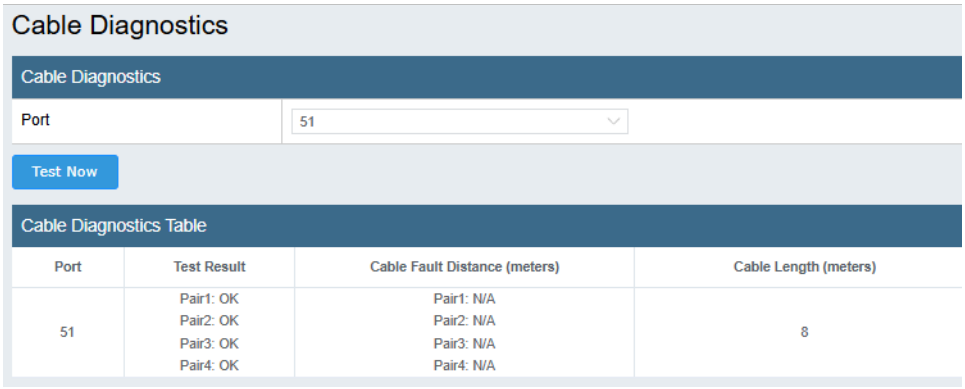
Cable Diagnostics

This feature is designed primarily for administrator or customer service representatives to verify and test copper cables. It can determine the quality of the cables and the types or errors.

Perform the following procedure to run cable diagnostics:



1. Select **Tools** > **Cable Diagnostics** from the menu. Refer to Figure 158.



2. From the Port pull-down menu, select a port and cable to test. You can select only one port.
3. Click the **Test Now** button. The results are displayed in the window.

Figure 158. Cable Diagnostics Window

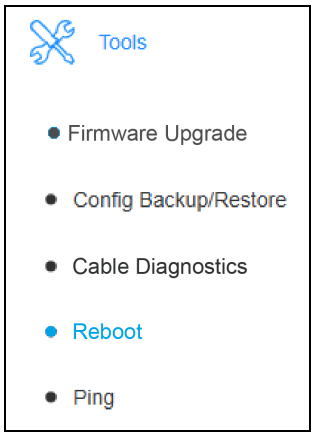
Rebooting the Switch

This section contains the procedure for rebooting the switch. You might reboot the switch if it is experiencing a problem or to discard unsaved configuration changes. You can also reboot the device by pressing the Reset button on the front panel for five to nine seconds, as explained in the *iGS950 Series Installation Guide*.

Note
Configuration settings not saved in the configuration file are discarded when the switch is rebooted. To save the current configuration, select **Save** from the menu before rebooting the switch.

Caution
The switch stops forwarding network traffic for approximately two minutes while it initializes its management software. Some network traffic may be lost.

Perform the following procedure to reboot the switch:



1. Select **Tools** > **Reboot** from the menu.

   The Factory Default Reset/Reboot window is shown in Figure 159.

2. Select **Normal** from the Reboot Type menu. This is the default selection.

Note
The Factory Default and Factory Default Except IP selections in the Reboot Type menu are described in “Restoring the Factory Default Values” on page 543.

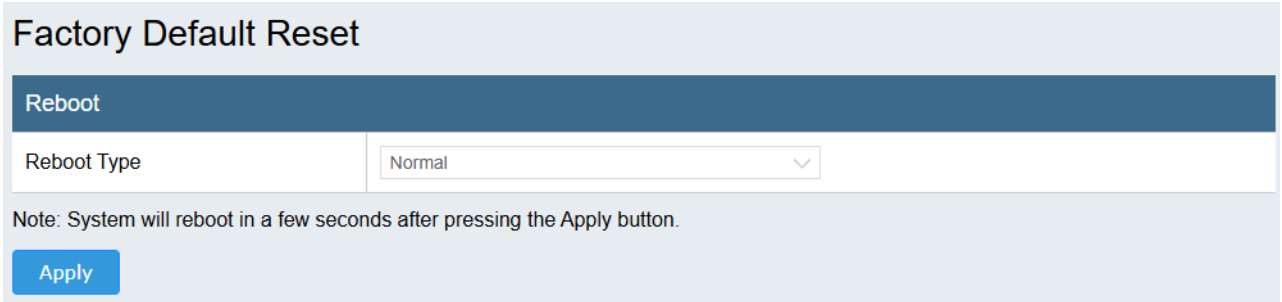


Figure 159. Factory Default Reset/Reboot Window

3. Click **Apply**.

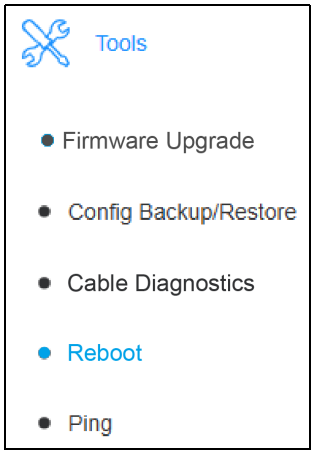
   The switch reboots and initializes its management program, a process that takes approximately two minutes to complete. After the reboot is finished, you can log in again to resume managing the switch.

Restoring the Factory Default Values

This section contains the procedure for restoring the factory default settings to the switch. You might perform this procedure to discard the current configuration before configuring the switch with new settings.

Caution
The switch stops forwarding network traffic for approximately two minutes while it initializes the management software. Some network traffic may be lost.

Perform the following procedure to restore the default settings:



1. Select **Tools** > **Reboot** from the main. The Factory Default Reset window is shown in Figure 159 on page 541.
2. Select one of the following from the Reboot Type menu:
   - **Factory Default** - Returns all the switch parameters, including the IPv4 and IPv6 addresses, to the factory default settings. The IPv4 address is return to the default 192.168.1.1 and the DHCP client is disabled. There is no default IPv6 address.
   - **Factory Default Except IP** - Returns all the switch parameters, excluding the IPv4 and IPv6 addresses, to the factory default settings. If the DHCP client is enabled, it remains enabled after this reset.
3. Click **Apply**.

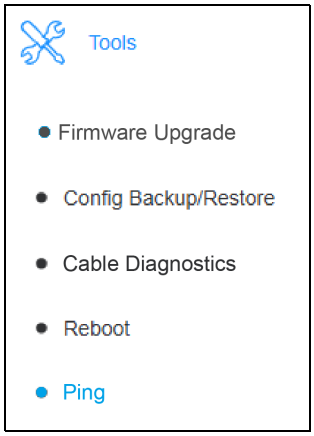
   The switch reboots, initializes the management program, and restores the default settings, a process that takes approximately two minutes to complete. When the reboot is finished, you can log in again to continue managing the switch. For instructions, refer to “Starting a Web Browser Management Session” on page 54.

Pinging Network Devices

This section contains the procedure for instructing the switch to transmit ICMP Echo Requests to IPv4 or IPv6 devices on the network. You might perform this procedure to test for active physical links between the switch and other network devices. This can be useful when troubleshooting network communications problems between devices.

ICMP Echo Requests are supported on ports of 802.1Q Tagged VLANs that are designated as Management VLANs, including the Default VLAN. They are not supported on Port-based VLANs.

To instruct the switch to issue ICMP Echo Requests from ports in 802.1 Q Tagged VLANs:



1. Select **Tools** > **Ping**. from the menu.
2. The Ping Test Settings window is shown in Figure 160 on page 545.
3. Enter the fields in Table 123.

Table 123. Ping Test Settings Window

Field	Description
Destination IP Address	Enter the IPv4 or IPv6 address of the remote network device. The format for an IPv4 address is shown here: nnn nnn nnn nnn Each N is a decimal number from 0 to 255. The format for an IPv6 address is shown here: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx Each x is a hexadecimal digit representing four bits. The eight groups of digits have to be separated by colons. Groups where all four digits are ‘0’ can be omitted. Leading ‘0’s in groups can also be omitted. As an example, the following IPv6 addresses are equivalent: 3710:421e:09a8:0000:0000:0000:00a4:1c50 3710:421e:9a8::a4:1c50
Timeout Value	Enter the length of time, in seconds, the switch waits for a response before assuming pings failed.

Table 123. Ping Test Settings Window (Continued)

Field	Description
Number of Ping Requests	Enter the number of ping requests the switch is to transmit.

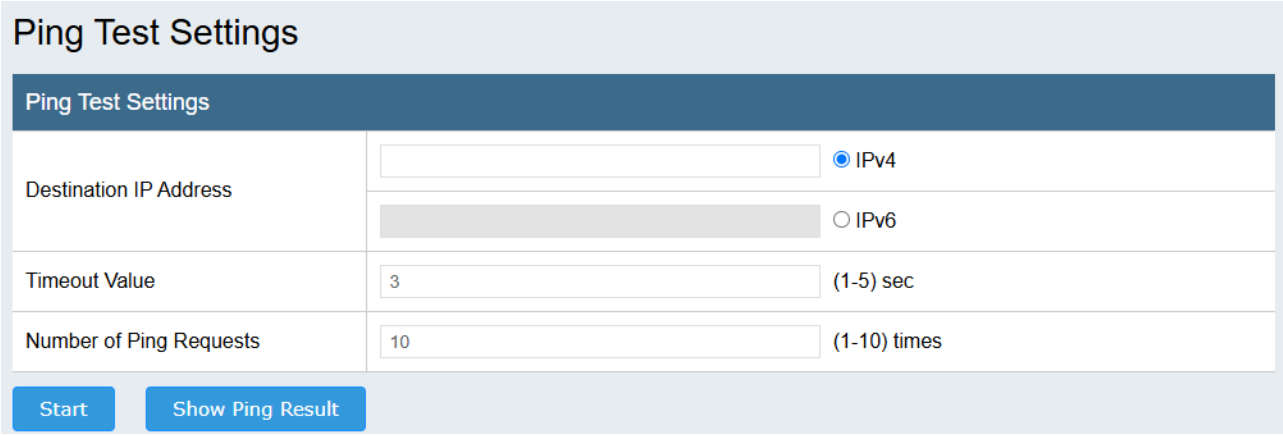


Figure 160. Ping Test Settings Window

4. Click **Start**.
5. Click **Show Ping Results** to view the ping results. Table 124 defines the information.

Table 124. Ping Test Results Window

Field	Description
Destination IP Address	Displays the IPv4 or IPv6 address of the remote network device.
Pass	Displays the percentage of successful pings.
Average Time	Displays the average transit time (milliseconds) of the ping responses.

6. Click **Back to Ping Test** to return to the Ping Test Settings window.