

USER MANUAL

PRODUCT MODEL: **DWS-4000 SERIES**
DWL-8600AP
DWL-6600AP
DWL-3600AP

UNIFIED WIRED & WIRELESS ACCESS SYSTEM
RELEASE 2.0

NOVEMBER 2011

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the 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 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.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstörungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo caso, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l'utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l'utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

BSMI Warning

警告使用者

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下使用者會被要求採取某些適當的對策

MIC Warning

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

CCC Warning

此為 A 級產品，在生活環境中，該產品可能會造成無線電干擾，在這種情況下，可能需要用戶對其干擾採取切實可行措施。

Table of Contents

About This Document	45
Audience	45
Organization.....	45
Additional Documentation.....	46
Document Conventions	46
Section 1: Getting Started	47
Connecting the Switch to the Network	47
Booting the Switch	48
Boot Menu Functions.....	49
Start Operational Code	50
Change Baud Rate.....	50
Retrieve Event Log Using XMODEM	51
Load New Operational Code Using XMODEM	51
Load Configuration Using XMODEM.....	52
Display Operational Code Vital Product Data	52
Run Flash Diagnostics	53
Update Boot Code	54
Delete Operational Code	54
Reset the System	55
Restore Configuration To Factory Defaults (Delete Configuration Files)	55
Activate Backup Image	55
Understanding the User Interfaces	56
Using the Web Interface	56
Device View	57
Navigation Tree View.....	58
Configuration and Monitoring Options	59
Help Page Access	60
Using the Command-Line Interface	60
Using SNMP	61
Section 2: System Administration	62
System Description	63
Defining System Information.....	64
Switch Configuration	64
Viewing Inventory Information	65

Card Configuration	65
Slot Summary	67
PoE Configuration	68
PoE Status	69
Serial Port	70
IP Address	71
Network DHCP Client Options	73
HTTP Configuration	74
User Accounts	75
Adding a User Account	77
Changing User Account Information	77
Deleting a User Account	77
Authentication List Configuration	78
Creating an Authentication List	80
Configuring an Authentication List	80
Deleting an Authentication List	80
Authentication List Summary	81
Login Session	82
User Login	83
Assigning a User to an Authentication List	84
Denial of Service Protection	84
Multiple Port Mirroring	86
Adding a Port Mirroring Session	87
Removing or Modifying a Port Mirroring Session	88
Telnet Sessions	88
Outbound Telnet Client Configuration	90
Ping Test	91
TraceRoute	92
Configuring SNTP Settings	93
SNTP Settings	94
SNTP Server Configuration	95
SNTP Server Status	96
SNTP Global Status	97
Time Zone Configuration	99
Summer Time Configuration	100
Summer Time Recurring Configuration	101
Clock Detail	102

Configuring and Viewing Device Port Information	103
Port Configuration	103
Port Summary	106
Port Description	109
Managing and Viewing Logs	110
Buffered Log Configuration.....	110
Viewing Buffered Log Messages	111
Command Logger Configuration	112
Console Log Configuration	113
Event Log.....	114
Hosts Configuration	115
Adding a Remote Logging Host.....	115
Deleting a Remote Logging Host	116
Persistent Log Configuration.....	116
Persistent Log.....	118
Syslog Configuration	119
Trap Log	120
Defining SNMP Parameters	121
SNMP v1 and v2	121
SNMP v3.....	121
SNMP Community Configuration.....	122
Trap Receiver Configuration	123
Trap Flags	124
Supported MIBs	126
Managing the DHCP Server	127
Global Configuration	127
Pool Configuration	129
Pool Options	132
Reset Configuration	133
DHCP Server Summary	134
Bindings Information	134
Server Statistics.....	135
Conflicts Information	136
Configuring Time Ranges	137
Time Range Configuration	137
Time Range Summary	138
Time Range Entry Configuration.....	139

Configuring DNS	141
Global Configuration.....	141
Server Configuration.....	142
DNS Host Name IP Mapping Configuration.....	143
DNS Host Name IP Mapping Summary.....	144
Configuring and Viewing ISDP Information	145
Global Configuration.....	145
Cache Table.....	146
Interface Configuration.....	147
Statistics.....	148
Configuring sFlow	149
sFlow Agent Summary.....	149
sFlow Receiver Configuration.....	150
sFlow Poller Configuration.....	152
Counter Sampling.....	152
sFlow Sampler Configuration.....	153
Packet Flow Sampling.....	153
Viewing System Statistics	154
Switch Detailed.....	154
Switch Summary.....	156
Port Detailed.....	158
Port Summary Statistics.....	164
Section 3: Using System Tools	165
Reset Configuration to Defaults	165
Reset Passwords to Defaults	166
System Reset	166
Save All Applied Changes	167
Download File To Switch (TFTP)	167
Downloading a File to the Switch.....	169
HTTP File Download	170
Upload File From Switch (TFTP)	171
Uploading Files.....	172
Multiple Image Service	172
Viewing the Dual Image Status.....	174
Erase Startup-config File	175
AutoInstall	175

Section 4: Configuring L2 Features.....	177
Configuring and Searching the Forwarding Database.....	178
Configuration	178
MAC Address Table	179
Searching the Forwarding Database.....	180
Managing VLANs	180
VLAN Configuration	180
VLAN Status	182
VLAN Port Configuration.....	183
VLAN Port Summary	184
Managing Protocol-Based VLANs.....	185
Protocol-Based VLAN Summary.....	187
Managing IP Subnet-Based VLANs.....	188
IP Subnet-based VLAN Summary	189
MAC-based VLAN Configuration.....	189
MAC-based VLAN Summary.....	190
Double VLAN Tunneling	191
Double VLAN Tunneling Summary.....	192
Voice VLAN Configuration	193
Reset VLAN Configuration.....	194
Configuring Protected Ports.....	195
Protected Port Configuration.....	195
Assigning Ports to a Group	196
Protected Ports Summary.....	196
Creating MAC Filters.....	197
Adding MAC Filters	198
Modifying MAC Filters	198
Deleting MAC Filters	198
MAC Filter Summary	198
Configuring GARP	199
GARP Status	199
GARP Switch Configuration.....	201
GARP Port Configuration	202
Creating Port Channels (Trunking).....	204
Port Channel Configuration	204
Port Channel Status	206
Configuring IGMP Snooping	208

Global Configuration and Status	209
Interface Configuration.....	210
VLAN Configuration	211
VLAN Status	212
Multicast Router Configuration	213
Multicast Router Status	214
Multicast Router VLAN Configuration.....	215
Multicast Router VLAN Status.....	216
Configuring IGMP Snooping Queriers	217
IGMP Snooping Querier Configuration	217
IGMP Snooping Querier VLAN Configuration	218
IGMP Snooping Querier VLAN Configuration Summary	219
IGMP Snooping Querier VLAN Status	220
Configuring MLD Snooping.....	221
Configuration and Status	221
Interface Configuration.....	222
VLAN Status	223
VLAN Configuration	224
Multicast Router Configuration	225
Multicast Router Status	226
Multicast Router VLAN Configuration.....	227
Multicast Router VLAN Status.....	228
Configuring MLD Snooping Queriers	229
MLD Snooping Querier Configuration.....	229
MLD Snooping Querier VLAN Configuration	230
MLD Snooping Querier VLAN Configuration Summary.....	231
MLD Snooping Querier VLAN Status.....	232
Viewing Multicast Forwarding Database Information	233
MFDB Table.....	233
MFDB GMRP Table.....	234
MFDB IGMP Snooping Table	235
MFDB MLD Snooping Table	236
MFDB Statistics	237
Configuring Spanning Tree Protocol	238
Switch Configuration/Status	238
CST Configuration/Status.....	240
MST Configuration/Status.....	242

CST Port Configuration/Status	244
MST Port Configuration/Status.....	247
Statistics	250
Configuring DHCP Snooping	251
Global DHCP Snooping Configuration	251
DHCP Snooping VLAN Configuration.....	252
DHCP Snooping Interface Configuration	252
Managing LLDP	254
Global Configuration	255
Interface Configuration.....	256
Interface Summary	257
Statistics	258
Local Device Information	259
Local Device Summary	260
Remote Device Information.....	261
Remote Device Summary.....	262
LLDP-MED	263
LLDP-MED Global Configuration	263
LLDP-MED Interface Configuration.....	264
LLDP-MED Interface Summary	265
LLDP Local Device Information	266
LLDP-MED Remote Device Information.....	268
Configuring Dynamic ARP Inspection	270
DAI Configuration	270
DAI VLAN Configuration.....	271
DAI Interface Configuration	272
DAI ARP ACL Configuration	273
DAI ARP ACL Rule Configuration	274
Dynamic ARP Inspection Statistics.....	275
Section 5: Configuring L3 Features.....	276
Managing the BOOTP/DHCP Relay Agent.....	276
BootP/DHCP Relay Agent Configuration.....	277
BOOTP/DHCP Relay Agent Status	278
Configuring the IP Helper Features	279
IP Helper Global Configuration	279
IP Helper Interface Configuration	281

IP Helper Statistics	283
Configuring ARP	284
ARP Create	285
ARP Table Configuration	286
Viewing ARP Cache	288
Configuring Global and Interface IP Settings	289
IP Configuration	289
IP Interface Configuration	291
IP Statistics	293
Loopback Interfaces	296
Loopbacks Configuration	296
Creating a New Loopback (IPv4)	297
Removing a Loopback	298
Removing a Secondary Address	298
Loopbacks Summary	299
Configuring RIP	300
RIP Configuration	300
RIP Interface Configuration	301
Configuring the RIP Interface	303
RIP Interface Summary	304
RIP Route Redistribution Configuration	305
RIP Route Redistribution Summary	306
Router Discovery	307
Router Discovery Configuration	307
Router Discovery Status	308
Router	309
Route Table	309
Best Routes Table	311
Configured (Static) Routes	312
Adding a Static Route	312
Deleting a Route	313
Route Preferences Configuration	314
VLAN Routing	315
VLAN Routing Configuration	315
Creating a VLAN Routing Interface	316
Deleting a VLAN Router Interface	317
VLAN Routing Summary	318

Virtual Router Redundancy Protocol (VRRP)	319
VRRP Configuration.....	319
Virtual Router Configuration.....	320
Configuring a Secondary VRRP Address.....	321
Creating a New Virtual Router.....	322
Modifying a Virtual Router.....	322
VRRP Interface Tracking Configuration.....	322
VRRP Interface Tracking.....	323
VRRP Route Tracking Configuration.....	324
VRRP Route Tracking.....	325
Virtual Router Status.....	325
Virtual Router Statistics.....	327
Section 6: Configuring Quality of Service	329
Configuring Class of Service	329
Mapping 802.1p Priority.....	329
Trust Mode Configuration.....	330
IP DSCP Mapping Configuration.....	332
CoS Interface Configuration.....	333
CoS Interface Queue Configuration.....	334
CoS Interface Queue Status.....	335
Configuring Differentiated Services	336
Diffserv Configuration.....	336
Class Configuration.....	338
DiffServ Class Summary.....	340
Policy Configuration.....	341
DiffServ Policy Summary.....	342
Policy Class Definition.....	343
DiffServ Policy Attribute Summary.....	345
Service Configuration.....	345
DiffServ Service Summary.....	346
Service Statistics.....	346
Service Detailed Statistics.....	347
Configuring Auto VoIP	349
Auto VoIP Configuration.....	349
Auto VoIP Summary.....	350

Section 7: Configuring Access Control Lists	351
Configuring IP Access Control Lists	351
IP ACL Configuration	352
IP ACL Rule Configuration	353
<i>Modifying an IP-based Rule</i>	<i>357</i>
<i>Adding a New Rule to an IP-based ACL.....</i>	<i>358</i>
<i>Deleting a Rule from an IP-based ACL</i>	<i>358</i>
IP ACL Summary	358
IP ACL Rule Summary	359
MAC Access Control Lists	359
MAC ACL Configuration	360
MAC ACL Rule Configuration	361
<i>Adding a New Rule to a MAC-based ACL</i>	<i>364</i>
<i>Removing a Rule From a MAC-based ACL.....</i>	<i>364</i>
MAC ACL Summary	365
MAC ACL Rule Summary	365
ACL Interface Configuration	366
Assigning an ACL to an Interface	367
Removing an ACL from an Interface	367
Section 8: Managing Device Security	368
Configuring Port Security	368
Port Security Administration.....	369
Port Security Interface Configuration	369
Port Security Static.....	371
Port Security Dynamic.....	372
Port Security Violation Status	373
SSL/Secure HTTP Configuration	374
<i>Generating Certificates</i>	<i>375</i>
<i>Downloading SSL Certificates</i>	<i>375</i>
Secure Shell (SSH) Configuration	377
Secure Shell Configuration.....	377
Downloading SSH Host Keys	378
Captive Portal Configuration.....	379
Captive Portal Global Configuration	379
CP Configuration	381
Changing the Captive Portal Settings	382

Customizing the Captive Portal Web Page	384
Local User.....	390
Adding a Local User	391
Configuring Users in the Local Database	392
Configuring Users in a Remote RADIUS Server	393
Interface Association	395
CP Global Status.....	396
Viewing CP Activation and Activity Status	397
Interface Status.....	399
Viewing Interface Activation Status.....	399
Viewing Interface Capability Status	400
Client Connection Status.....	401
Viewing Client Details	402
Viewing the Client Statistics	403
Viewing the Client Interface Association Status	403
Viewing the Client CP Association Status	404
SNMP Trap Configuration	405
RADIUS Settings	406
RADIUS Configuration	406
RADIUS Server Configuration.....	408
Viewing Named Server Status Information	410
RADIUS Server Statistics	411
RADIUS Accounting Server Configuration.....	411
Viewing Named Accounting Server Status	413
RADIUS Server Statistics	414
Clear Statistics.....	414
Port Access Control	415
Global Port Access Control Configuration.....	415
Port Configuration	416
Port Access Entity Capability Configuration.....	418
Supplicant Port Configuration.....	419
Port Status	420
Port Summary	424
Port Access Control Statistics.....	426
Client Summary.....	427
Port Access Privileges	428

TACACS+ Settings	429
TACACS+ Configuration.....	429
TACACS+ Server Configuration	430
Section 9: Configuring the Wireless Features	431
Unified Wired and Wireless Access System Components	431
D-Link DWS-4000 Series Unified Wireless Switch.....	432
DWL-X600AP Unified Access Points.....	432
DWS-4000 Series Switch and AP Discovery Methods	433
L2 Discovery.....	433
IP Address of AP Configured in the Switch	434
IP Address of Switch Configured in the AP	434
Configuring the DHCP Option	435
Discovery and Peer Switches	437
Monitoring Status and Statistics	438
Wireless Global Status/Statistics	438
Viewing Switch Status and Statistics Information	443
Viewing IP Discovery Status.....	447
Viewing the Peer Switch Configuration Received Status.....	449
Viewing the AP Hardware Capability List.....	450
<i>AP Hardware Radio Capability</i>	451
AP Image Capability	452
Peer Switch Status	453
Viewing Peer Switch Configuration Status	454
Viewing Peer Switch Managed AP Status	455
All AP Status	456
Managed AP Status.....	458
Monitoring AP Status.....	459
Viewing Detailed Managed Access Point Status.....	461
Viewing Managed Access Point Radio Summary Information.....	464
Viewing Detailed Managed Access Point Radio Information	464
Viewing Managed Access Point Neighbor APs	466
Viewing Clients Associated with Neighbor Access Points.....	467
Viewing Managed Access Point VAPs.....	468
Viewing Managed Access Point VAP TSPEC Status.....	468
Viewing Distributed Tunneling Information	470
Managed Access Point Statistics.....	471

Viewing Managed Access Point Ethernet Statistics.....	472
Viewing Detailed Managed Access Point Statistics	472
Viewing Managed Access Point Radio Statistics.....	474
Viewing Managed Access Point VAP Statistics	475
Viewing Distributed Tunneling Statistics	476
AP Authentication Failure Status.....	477
Viewing Details About AP Authentication Failures.....	479
AP RF Scan Status.....	480
Viewing Details About an AP Detected in the RF Scan	482
Viewing AP Triangulation Information	484
Viewing WIDS AP Rogue Classification Information.....	485
AP De-Authentication Attack Status	487
Associated Client Status/Statistics.....	488
Viewing Associated Client Summary Status	489
Viewing Detailed Associated Client Status	490
Viewing Associated Client QoS Status	492
Viewing Associated Client Neighbor AP Status.....	493
Viewing Associated Client Distributed Tunneling Status.....	494
Viewing Associated Client TSPEC Status.....	496
Viewing Associated Client RRM Status	497
Viewing Associated Client SSID Status.....	498
Viewing Associated Client VAP Status	499
Switch Associated Client Status.....	500
Viewing Associated Client Statistics	501
Viewing Associated Client Session Summary Statistics	502
Viewing Detailed Associated Client Association Statistics.....	503
Viewing Detailed Associated Client Session Statistics	504
Viewing Detailed Associated Client TSPEC Statistics	505
Ad Hoc Client Status.....	506
Detected Client Status	507
Viewing Detailed Detected Client Status.....	509
Viewing WIDS Client Rogue Classification	511
Viewing Detected Client Pre-Authentication History	513
Viewing Detected Client Triangulation.....	514
Viewing Detected Client Roam History.....	515
Detected Client Pre-Authentication Summary	516

Detected Client Roam History Summary	517
Radio Resource Measurement Status Information	518
Viewing the RRM Channel Load Configuration.....	518
Viewing the RRM Channel Load History	520
Viewing RRM Neighbors	521
WDS-Managed AP Information.....	522
WDS Group Status Summary	522
WDS AP Group Status	523
WDS Group AP Status Summary	525
WDS AP Link Status Summary	526
WDS Group Link Statistics Summary	528
Basic Setup	529
Wireless Global Configuration	529
Wireless Discovery Configuration	534
L3/IP Discovery	535
L2/VLAN Discovery	536
Profile.....	537
Radio Configuration	538
Wireless Default VAP Configuration	543
Managing the Virtual Access Point Configuration	543
Configuring the Default Network	545
Configuring AP Security	551
<i>Using No Security</i>	551
<i>Using Static or Dynamic WEP</i>	551
<i>Static WEP Rules</i>	553
<i>Using WPA/WPA2 Personal or Enterprise</i>	553
Valid Access Point Summary	556
Valid Access Point Configuration	557
Local OUI Database Summary.....	561
AP Management	562
Reset	562
RF Management.....	563
Configuring Channel Plan and Power Settings	563
Viewing the Channel Plan History.....	566
Initiating Manual Channel Plan Assignments	567
Initiating Manual Power Adjustments.....	569

Access Point Software Download	570
Managed AP Advanced Settings	573
Debugging the AP	574
Adjusting the Channel and Power	575
AP Provisioning	577
AP Provisioning Summary Status	577
Detailed AP Provisioning Status	578
Configuring Advanced Settings	581
Advanced Global Settings	581
Wireless SNMP Trap Configuration	584
Distributed Tunneling Configuration	587
Device Location Configuration	588
Wireless Network List	589
Configuring Networks	590
AP Profiles	590
Creating, Copying, and Deleting AP Profiles	591
Applying an AP Profile	593
Configuring the AP Profile Global Settings	595
Access Point Profile Radio Configuration	596
Access Point Profile VAP Configuration	604
Access Point Profile QoS Configuration	606
Access Point Profile TSPEC Configuration	609
Peer Switch	612
Peer Switch Configuration Enable/Disable	613
Mutual Authentication	615
WIDS Security	616
WIDS AP Configuration	616
WIDS Client Configuration	619
Known Client	621
Known Client Configuration	623
Switch Provisioning	624
Provisioning	625
Enabling AeroScout™ Engine Support	626
Configuring the Wireless Distribution System	626
WDS Managed AP Group Configuration	629
WDS Managed AP Configuration	631

WDS Link Configuration	633
WDS Link Create	634
Locating WLAN Devices	635
Managed AP Location	635
Building	635
Building Floor	637
Managed AP Coordinates	638
Managed AP Location Summary	639
On-Demand Location Trigger	640
On-Demand Location Trigger Status	641
On-Demand Location Trigger Global Status	641
On-Demand Location Trigger Floor Status	643
AP Triangulation Location	644
AP Triangulation Summary	644
Detailed AP Triangulation Status	645
Client Triangulation Location	647
Client Triangulation Summary	647
Detailed AP Triangulation Status	648
Visualizing the Wireless Network	650
WLAN Visualization Overview	650
Importing and Configuring a Background Image	651
Setting Up the Graph	652
Creating a New Graph	652
Manually Graphing the Components	654
Checking the Location of an AP or Client	654
Understanding the Menu Options and Icons	657
Legend Menu	660
Viewing Component Information	661
Appendix A: Configuration Examples	662
Configuring VLANs	662
Configuring Multiple Spanning Tree Protocol	665
Configuring VLAN Routing	668
Configuring 802.1X Network Access Control	671
Configuring a Virtual Access Point	673
Configuring Differentiated Services for VoIP	677
Configuring a Network with WDS-Managed APs	680

Configuring a Network to Use WPA2-Enterprise and Dynamic VLANs	689
Configuring Client Information on the RADIUS Server	690
Configuring RADIUS Information and AP Profiles on the Switch	691
Verifying the Configuration.....	696
Optimizing WLAN Traffic	698
Monitoring and Managing Channel Information	698
Running and Applying a Manual Channel Plan.....	700
Monitoring the RF Transmission Power Level	702
Configuring the Automatic Power Adjustment	703
Load Balancing and WLAN Utilization.....	706
Detecting and Preventing Wireless Intrusion	709
Configuring a Radio in Sentry Mode	709
Configuring and Monitoring WIDS/WIPS to Detect Rogue APs	710
Using WIDS/WIPS to Detect Rogue Clients.....	715
Mitigating a Rogue Client Threat	717
Appendix B: Warranty & Support	722

List of Figures

Figure 1: Web Interface Layout	57
Figure 2: Device View—Back	57
Figure 3: Cascading Navigation Menu	58
Figure 4: Navigation Tree View	58
Figure 5: LAN and WLAN Tabs	59
Figure 6: Help Link	60
Figure 7: System Description	63
Figure 8: Switch Configuration	64
Figure 9: Inventory Information	65
Figure 10: Card Configuration	65
Figure 11: Slot Summary	67
Figure 12: PoE Configuration	68
Figure 13: PoE Status	69
Figure 14: Serial Port	70
Figure 15: Network Connectivity—IPv4	71
Figure 16: Network Connectivity—IPv6	71
Figure 17: DHCP Client Options	73
Figure 18: HTTP Configuration	74
Figure 19: User Accounts	75
Figure 20: Authentication List Configuration	78
Figure 21: Login Session	81
Figure 22: Login Session	82
Figure 23: User Login	83
Figure 24: Denial of Service	84
Figure 25: Multiple Port Mirroring	86
Figure 26: Multiple Port Mirroring—Add Source Ports	87
Figure 27: Telnet Session Configuration	88
Figure 28: Outbound Telnet	90
Figure 29: Ping	91
Figure 30: TraceRoute	92
Figure 31: SNTP Global Configuration	94
Figure 32: SNTP Server Configuration	95
Figure 33: SNTP Server Status	96
Figure 34: Global Status	98
Figure 35: Time Zone Configuration	99

Figure 36: Summer Time Configuration	100
Figure 37: Summer Time Recurring Configuration	101
Figure 38: Clock Detail.....	102
Figure 39: Port Configuration	103
Figure 40: Port Summary.....	106
Figure 41: Port Description.....	109
Figure 42: Buffered Log Configuration	110
Figure 43: Buffered Log	111
Figure 44: Command Logger Configuration	112
Figure 45: Console Log Configuration	113
Figure 46: Event Log	114
Figure 47: Host Configuration	115
Figure 48: Host Configuration with Logging Host.....	115
Figure 49: Persistent Log Configuration	116
Figure 50: Persistent Log	118
Figure 51: System Log.....	119
Figure 52: Trap Log	120
Figure 53: SNMP Community Configuration	122
Figure 54: Trap Receiver Configuration.....	123
Figure 55: Trap Flags Configuration.....	125
Figure 56: Supported MIBs	126
Figure 57: DHCP Server Global Configuration	127
Figure 58: Pool Configuration.....	129
Figure 59: Pool Options	132
Figure 60: Reset Configuration.....	133
Figure 61: Bindings Information	134
Figure 62: Server Statistics	135
Figure 63: Conflicts Information.....	136
Figure 64: Time Range Configuration	137
Figure 65: Time Range Summary.....	138
Figure 66: Time Range Entry Configuration	139
Figure 67: DNS Global Configuration.....	141
Figure 68: DNS Server Configuration.....	142
Figure 69: DNS Host Name Mapping Configuration	143
Figure 70: DNS Host Name IP Mapping Summary.....	144
Figure 71: ISDP Global Configuration	145
Figure 72: ISDP Cache Table	146

Figure 73: ISDP Interface Configuration	147
Figure 74: ISDP Statistics	148
Figure 75: sFlow Agent Summary	149
Figure 76: sFlow Receiver Configuration	150
Figure 77: sFlow Poller Configuration	152
Figure 78: sFlow Sampler Configuration	153
Figure 79: Switch Detailed	154
Figure 80: Switch Summary	156
Figure 81: Port Detailed	158
Figure 82: Port Summary	164
Figure 83: Reset Configuration to Defaults	165
Figure 84: Reset Passwords to Defaults	166
Figure 85: System Reset	166
Figure 86: Save All Applied Changes	167
Figure 87: Download File to Switch	167
Figure 88: HTTP File Download	170
Figure 89: Upload File from Switch	171
Figure 90: Multiple Image Service	173
Figure 91: Dual Image Status	174
Figure 92: Erase Startup-config File	175
Figure 93: AutoInstall	175
Figure 94: Forwarding Database Age-Out Interval	178
Figure 95: Forwarding Database Search	179
Figure 96: VLAN Configuration	181
Figure 97: VLAN Status	182
Figure 98: VLAN Port Configuration	183
Figure 99: VLAN Port Summary	184
Figure 100: Create Protocol Group	185
Figure 101: Protocol Group	186
Figure 102: Protocol-based VLAN Summary	187
Figure 103: IP Subnet-based VLAN Configuration	188
Figure 104: IP Subnet-based VLAN Summary	189
Figure 105: MAC-based VLAN Configuration	190
Figure 106: MAC-based VLAN Summary	190
Figure 107: Double VLAN Tunneling	191
Figure 108: Double VLAN Tunneling Summary	192
Figure 109: Voice VLAN Configuration	193

Figure 110: Reset VLAN Configuration 194

Figure 111: Protected Port Configuration 195

Figure 112: Protected Ports Summary 196

Figure 113: MAC Filter Configuration 197

Figure 114: MAC Filter Summary 198

Figure 115: GARP Status 199

Figure 116: GARP Switch Configuration 201

Figure 117: GARP Port Configuration 202

Figure 118: Port Channel Configuration 204

Figure 119: Port Channel Status 206

Figure 120: IGMP Snooping Global Configuration and Status 209

Figure 121: IGMP Snooping Interface Configuration 210

Figure 122: IGMP Snooping VLAN Configuration 211

Figure 123: IGMP Snooping VLAN Status 212

Figure 124: Multicast Router Configuration 213

Figure 125: Multicast Router Status 214

Figure 126: Multicast Router VLAN Configuration 215

Figure 127: Multicast Router VLAN Status 216

Figure 128: IGMP Snooping Querier Configuration 217

Figure 129: IGMP Snooping Querier VLAN Configuration 218

Figure 130: IGMP Snooping Querier VLAN Configuration Summary 219

Figure 131: IGMP Snooping Querier VLAN Status 220

Figure 132: MLD Snooping Global Configuration and Status 221

Figure 133: MLD Snooping Interface Configuration 222

Figure 134: MLD Snooping VLAN Status 223

Figure 135: MLD Snooping VLAN Configuration 224

Figure 136: MLD Snooping Multicast Router Configuration 225

Figure 137: MLD Snooping Multicast Router Status 226

Figure 138: Multicast Router VLAN Configuration 227

Figure 139: MLD Snooping Multicast Router VLAN Status 228

Figure 140: MLD Snooping Querier Configuration 229

Figure 141: MLD Snooping Querier VLAN Configuration 230

Figure 142: MLD Snooping Querier VLAN Configuration Summary 231

Figure 143: MLD Snooping Querier VLAN Status 232

Figure 144: MFDB Table 233

Figure 145: GMRP Table 234

Figure 146: IGMP Snooping Table 235

Figure 147: MFDB MLD Snooping Table	236
Figure 148: Multicast Forwarding Database Statistics	237
Figure 149: Spanning Tree Switch Configuration/Status.....	238
Figure 150: Spanning Tree CST Configuration/Status	240
Figure 151: Spanning Tree MST Configuration/Status	242
Figure 152: Spanning Tree MST Configuration/Status	242
Figure 153: Spanning Tree CST Port Configuration/Status.....	244
Figure 154: Spanning Tree MST Port Configuration/Status	247
Figure 155: Spanning Tree Statistics	250
Figure 156: DHCP Snooping Configuration.....	251
Figure 157: DHCP Snooping VLAN Configuration	252
Figure 158: DHCP Snooping Interface Configuration	253
Figure 159: LLDP Global Configuration.....	255
Figure 160: LLDP Interface Configuration	256
Figure 161: LLDP Interface Summary	257
Figure 162: LLDP Statistics.....	258
Figure 163: LLDP Local Device Information	259
Figure 164: LLDP Local Device Summary.....	260
Figure 165: LLDP Remote Device Information	261
Figure 166: LLDP Remote Device Summary	262
Figure 167: LLDP Global Configuration.....	263
Figure 168: LLDP-MED Interface Configure.....	264
Figure 169: LLDP-MED Interface Summary	265
Figure 170: LLDP-MED Local Device Information.....	266
Figure 171: LLDP Remote Device Information	268
Figure 172: Dynamic ARP Inspection Configuration.....	270
Figure 173: Dynamic ARP Inspection VLAN Configuration	271
Figure 174: Dynamic ARP Inspection Interface Configuration	272
Figure 175: Dynamic ARP Inspection ARP ACL Configuration	273
Figure 176: Dynamic ARP Inspection ARP ACL Rule Configuration	274
Figure 177: Dynamic ARP Inspection Statistics	275
Figure 178: BOOTP/DHCP Relay Agent Configuration.....	277
Figure 179: BOOTP/DHCP Relay Agent Status.....	278
Figure 180: IP Helper Global Configuration.....	279
Figure 181: Adding a Global IP Helper Entry	280
Figure 182: IP Helper Interface Configuration.....	281
Figure 183: Adding an IP Helper Entry to an Interface.....	282

Figure 184: IP Helper Statistics.....	283
Figure 185: ARP Create.....	285
Figure 186: ARP Table Configuration.....	286
Figure 187: ARP Cache.....	288
Figure 188: IP Configuration.....	289
Figure 189: IP Interface Configuration	291
Figure 190: IP Statistics	293
Figure 191: Loopback Configuration—Create	296
Figure 192: Configured Loopback Interface	296
Figure 193: Loopbacks Configuration—IPv4 Entry	298
Figure 194: Loopbacks Summary.....	299
Figure 195: RIP Configuration.....	300
Figure 196: RIP Interface Configuration	301
Figure 197: RIP Interface Authentication Configuration	303
Figure 198: RIP Interface Summary	304
Figure 199: RIP Route Redistribution Configuration	305
Figure 200: RIP Route Redistribution Summary	306
Figure 201: Router Discovery Configuration	307
Figure 202: Router Discovery Status	308
Figure 203: Route Table	309
Figure 204: Best Routes Table	311
Figure 205: Configured Routes.....	312
Figure 206: Create Static Route.....	313
Figure 207: Route Preferences Configuration	314
Figure 208: VLAN Routing Configuration.....	315
Figure 209: VLAN Routing Configuration - Interface Exists	316
Figure 210: VLAN Routing Summary	318
Figure 211: VRRP Configuration	319
Figure 212: Virtual Router Configuration	320
Figure 213: VRRP Interface Tracking Configuration	322
Figure 214: VRRP Interface Tracking	323
Figure 215: VRRP Route Tracking Configuration	324
Figure 216: VRRP Route Tracking	325
Figure 217: Virtual Router Status	325
Figure 218: Virtual Router Statistics—Virtual Router Configured.....	327
Figure 219: 802.1p Priority Mapping.....	330
Figure 220: Trust Mode Configuration	331

Figure 221: IP DSCP Mapping Configuration	332
Figure 222: Interface Configuration	333
Figure 223: Interface Queue Configuration.....	334
Figure 224: Interface Queue Status.....	335
Figure 225: Diffserv Configuration	337
Figure 226: Diffserv Class Configuration	338
Figure 227: Diffserv Class Configuration	338
Figure 228: Class Summary	340
Figure 229: Policy Configuration	341
Figure 230: Policy Configuration	341
Figure 231: Policy Summary	342
Figure 232: Policy Class Definition	343
Figure 233: Policy Attribute Summary	345
Figure 234: Service Configuration	345
Figure 235: Service Summary	346
Figure 236: Service Statistics	346
Figure 237: Service Detailed Statistics.....	347
Figure 238: Auto VoIP Configuration.....	349
Figure 239: Auto VoIP Summary	350
Figure 240: IP ACL Configuration.....	352
Figure 241: IP ACL Rule Configuration (Create Rule).....	353
Figure 242: IP ACL Rule Configuration (Extended ACL Rule)	354
Figure 243: IP ACL Summary	358
Figure 244: IP ACL Rule Summary	359
Figure 245: MAC ACL Configuration	360
Figure 246: MAC ACL Rule Configuration (Create Rule)	361
Figure 247: MAC ACL Rule Configuration (Deny Action)	361
Figure 248: MAC ACL Rule Configuration (Permit Action).....	362
Figure 249: MAC ACL Summary.....	365
Figure 250: MAC ACL Rule Summary.....	365
Figure 251: ACL Interface Configuration	366
Figure 252: Port Security Administration	369
Figure 253: Port Security Interface Configuration.....	369
Figure 254: Port Security Static	371
Figure 255: Port Security Dynamic	372
Figure 256: Port Security Violation Status.....	373
Figure 257: Secure HTTP Configuration.....	374

Figure 258: File Download.....	376
Figure 259: Secure Shell Configuration	377
Figure 260: Captive Portal Global Configuration.....	379
Figure 261: Captive Portal Summary.....	381
Figure 262: Captive Portal Configuration	382
Figure 263: CP Web Page Customization — Global Parameters	385
Figure 264: CP Web Page Customization — Authentication page	386
Figure 265: CP Web Page Customization — Welcome Page	386
Figure 266: CP Web Page Customization — Logout Page	387
Figure 267: CP Web Page Customization — Logout Success Page.....	387
Figure 268: Captive Portal Local User Summary	390
Figure 269: Adding a New User.....	391
Figure 270: Local User Configuration	392
Figure 271: Interface Association.....	395
Figure 272: Global Captive Portal Status.....	396
Figure 273: CP Activation and Activity Status	397
Figure 274: Interface Activation Status.....	399
Figure 275: Interface Capability Status	400
Figure 276: Client Summary	401
Figure 277: Client Detail	402
Figure 278: Client Statistics	403
Figure 279: Interface - Client Status.....	403
Figure 280: CP - Client Status	404
Figure 281: SNMP Trap Configuration.....	405
Figure 282: RADIUS Configuration	406
Figure 283: RADIUS Server Configuration—Add Server	408
Figure 284: RADIUS Server Configuration—Server Added.....	408
Figure 285: Named Server Status.....	410
Figure 286: RADIUS Server Statistics	411
Figure 287: Add RADIUS Accounting Server	411
Figure 288: RADIUS Accounting Server Configuration—Server Added.....	412
Figure 289: RADIUS Server Configuration—Server Added.....	413
Figure 290: RADIUS Accounting Server Statistics	414
Figure 291: RADIUS Clear Statistics	414
Figure 292: Global Port Access Control Configuration	415
Figure 293: Port Access Control Port Configuration.....	416
Figure 294: PAE Capability Configuration.....	418

Figure 295: Port Access Control Supplicant Port Configuration.....	419
Figure 296: Port Access Control Status	420
Figure 297: Port Access Control Status - MAC-based Control Mode	421
Figure 298: Port Access Control Port Summary	424
Figure 299: Port Access Control Statistics	426
Figure 300: Port Access Control Client Summary.....	427
Figure 301: Port Access Privileges	428
Figure 302: TACACS+ Configuration	429
Figure 303: TACACS+ Configuration—No Server.....	430
Figure 304: Global WLAN Status/Statistics.....	439
Figure 305: Switch Status/Statistics	444
Figure 306: Wireless Discovery Status	447
Figure 307: Configuration Received	449
Figure 308: AP Hardware Capability Information.....	450
Figure 309: Radio Detail	451
Figure 310: Image Table	452
Figure 311: Peer Switch Status.....	453
Figure 312: Peer Switch Configuration Status.....	454
Figure 313: Peer Switch Managed AP Status.....	455
Figure 314: All Access Points	456
Figure 315: Managed AP Status	459
Figure 316: Managed AP Statistics	471
Figure 317: AP Authentication Failure Status.....	477
Figure 318: AP Authentication Failure Details.....	479
Figure 319: RF Scan	481
Figure 320: RF Scan AP Details	482
Figure 321: AP Triangulation Status	484
Figure 322: WIDS AP Rogue Classification.....	485
Figure 323: AP De-Authentication Attack Status.....	487
Figure 324: Associated Client Status	488
Figure 325: Associated Client Status	489
Figure 326: Associated Client Status Detail.....	490
Figure 327: Associated Client QoS Status.....	492
Figure 328: Associated Client Neighbor AP Status	493
Figure 329: Associated Client Distributed Tunneling Status	494
Figure 330: Associated Client TSPEC Status	496
Figure 331: Associated Client RRM Status.....	497

Figure 332: SSID Associated Client Status	498
Figure 333: VAP Associated Client Status.....	499
Figure 334: Switch Associated Client Status.....	500
Figure 335: Associated Client Association Summary Statistics	501
Figure 336: Associated Client Statistics Session Summary.....	502
Figure 337: Associated Client Association Detail Statistics	503
Figure 338: Associated Client Session Detail Statistics.....	504
Figure 339: Associated Client Session Detail Statistics.....	505
Figure 340: Ad Hoc Clients	506
Figure 341: Detected Client Status.....	507
Figure 342: Detailed Detected Client Status	509
Figure 343: WIDS Client Rogue Classification.....	511
Figure 344: Detected Client Pre-Authentication History.....	513
Figure 345: Detected Client Triangulation	514
Figure 346: Detected Client Roam History	515
Figure 347: Detected Client Pre-Authentication History Summary	516
Figure 348: Detected Client Roam History Summary	517
Figure 349: RRM Channel Load Configuration	518
Figure 350: RRM Channel Load History.....	520
Figure 351: RRM Neighbors.....	521
Figure 352: WDS Group Status Summary.....	522
Figure 353: WDS AP Group Status.....	523
Figure 354: WDS AP Group Status Summary	525
Figure 355: WDS AP Link Status Summary	526
Figure 356: WDS Group Link Statistics Summary	528
Figure 357: Wireless Global Configuration.....	529
Figure 358: Wireless Discovery Configuration	535
Figure 359: AP Hardware Capabilities	537
Figure 360: Radio Settings.....	539
Figure 361: VAP Settings	543
Figure 362: Configuring Network Settings	545
Figure 363: AP Network Security Options	551
Figure 364: Static WEP Configuration	552
Figure 365: WPA Personal Configuration	554
Figure 366: Adding a Valid AP	556
Figure 367: Configuring a Valid AP	558
Figure 368: Local OUI Database Summary	561

Figure 369: Access Point Reset.....	562
Figure 370: RF Channel Plan and Power Configuration.....	564
Figure 371: Channel Plan History	566
Figure 372: Manual Channel Plan.....	567
Figure 373: Manual Power Adjustments.....	569
Figure 374: Software Download.....	570
Figure 375: Advanced AP Management	573
Figure 376: Managed AP Debug.....	574
Figure 377: Managed AP Debug.....	575
Figure 378: AP Provisioning Summary Status.....	577
Figure 379: AP Provisioning Status—Detail.....	579
Figure 380: Global Configuration	581
Figure 381: SNMP Trap Configuration.....	584
Figure 382: Distributed Tunneling Configuration.....	587
Figure 383: Device Location Configuration	588
Figure 384: Multiple AP Profiles.....	590
Figure 385: Adding a Profile	591
Figure 386: Configuring an AP Profile.....	592
Figure 387: Applying the AP Profile.....	594
Figure 388: AP Profile Global Configuration.....	595
Figure 389: AP Profile Radio Settings	597
Figure 390: AP Profile VAP Configuration	604
Figure 391: QoS Configuration	606
Figure 392: AP Profile TSPEC Configuration	610
Figure 393: Peer Switch Configuration Request Status.....	612
Figure 394: Peer Switch Configuration Enable/Disable.....	613
Figure 395: Mutual Authentication	615
Figure 396: WIDS AP Configuration.....	616
Figure 397: WIDS Client Configuration.....	619
Figure 398: Known Client Summary	621
Figure 399: Known Client Configuration	623
Figure 400: Switch Certificate Request	624
Figure 401: Switch Provisioning	625
Figure 402: WDS-Managed AP Group	627
Figure 403: WDS Managed AP Group Configuration.....	629
Figure 404: Edit WDS Managed AP Group Settings.....	630
Figure 405: WDS Managed AP Configuration.....	631

Figure 406: WDS Managed AP Settings.....	632
Figure 407: WDS AP Link Configuration	633
Figure 408: WDS Link Create	634
Figure 409: Building.....	635
Figure 410: Building Floor.....	637
Figure 411: Managed AP Coordinates.....	638
Figure 412: Managed AP Location Summary	639
Figure 413: On-Demand Location Trigger	640
Figure 414: On-Demand Location Trigger Global Status	641
Figure 415: On-Demand Location Trigger Floor Status	643
Figure 416: AP Triangulation Summary.....	644
Figure 417: Detailed AP Triangulation Status.....	645
Figure 418: Client Triangulation Summary	647
Figure 419: Detailed Client Triangulation Status.....	648
Figure 420: Sample WLAN Visualization.....	650
Figure 421: Live Visualization Control	652
Figure 422: Graphing a Switch.....	654
Figure 423: On-Demand Location Search Window	654
Figure 424: Device Location Progress Timer	655
Figure 425: Device Location Status	655
Figure 426: Probable Device Location – Point Solution	656
Figure 427: Probable Device Location – Circle Solution	656
Figure 428: Probable Device Location – Off Screen	657
Figure 429: Toolbar Icons	659
Figure 430: Legend	660
Figure 431: Sentry Mode—Detailed View.....	661
Figure 432: Wireless Component Attributes.....	661
Figure 433: VLAN Example Network Diagram	663
Figure 434: VLAN Routing Example Network Diagram.....	668
Figure 435: Switch with 802.1X Network Access Control.....	671
Figure 436: DiffServ VoIP Example Network Diagram.....	677
Figure 437: WDS-Managed APs in the Network.....	680
Figure 438: WPA2-Enterprise and Dynamic VLAN Assignment.....	689
Figure 439: Monitoring Managed AP Channels.....	699
Figure 440: Automatic Channel Adjustment	699
Figure 441: Fixed Channel Plan	700
Figure 442: WIDS AP Configuration.....	711

Figure 443: Honeypot AP.....711

Figure 444: All AP Status with Rogue 712

Figure 445: Honeypot AP Rogue Status..... 712

Figure 446: WIDS Test Discovers Rogue..... 713

Figure 447: De-Authentication Attack Enabled 713

Figure 448: Rogue AP Mitigation..... 714

Figure 449: De-Authentication Attack Status 714

Figure 450: WIDS Client Configuration..... 715

Figure 451: Excessive Authentication Failures 716

Figure 452: Client Rogue Classification 716

List of Tables

Table 1: Typographical Conventions	46
Table 2: Common Command Buttons	59
Table 3: System Description Fields	63
Table 4: Switch Configuration Fields	64
Table 5: Card Configuration Fields	66
Table 6: Slot Summary Fields	67
Table 7: PoE Configuration Fields	68
Table 8: Serial Port Fields	70
Table 9: Network Connectivity Fields	72
Table 10: DHCP Client Option Fields	73
Table 11: HTTP Configuration Fields	74
Table 12: User Accounts Fields.....	76
Table 13: Authentication Profile Fields	78
Table 14: Login Fields	81
Table 15: Login Session Fields	82
Table 16: User Login Fields	83
Table 17: Denial of Service Configuration Fields	85
Table 18: Multiple Port Mirroring Fields	86
Table 19: Multiple Port Mirroring—Add Source Fields	87
Table 20: Telnet Session Configuration Fields.....	89
Table 21: Outbound Telnet Fields	90
Table 22: Ping Fields	91
Table 23: TraceRoute Fields	92
Table 24: SNTP Global Configuration Fields	94
Table 25: SNTP Server Configuration Fields	95
Table 26: SNTP Server Status Fields	96
Table 27: Global Status Fields	98
Table 28: Time Zone Configuration Fields	99
Table 29: Summer Time Configuration Fields	100
Table 30: Summer Time Recurring Configuration Fields	101
Table 31: Clock Detail	102
Table 32: Port Configuration Fields	104
Table 33: Port Summary Fields.....	106
Table 34: Port Description Fields.....	109
Table 35: Buffered Log Fields	111

Table 36: Command Logger Configuration Fields	112
Table 37: Console Log Configuration Fields.....	113
Table 38: Event Log Fields	114
Table 39: Persistent Log Configuration Fields	117
Table 40: Persistent Log Fields	118
Table 41: Syslog Configuration Fields.....	119
Table 42: Trap Log Fields	120
Table 43: Community Configuration Fields	122
Table 44: Trap Receiver Configuration Fields.....	124
Table 45: Trap Flags Configuration Fields.....	125
Table 46: Supported MIBs Fields.....	126
Table 47: DHCP Server Global Configuration Fields	127
Table 48: Pool Configuration Fields.....	130
Table 49: Pool Options Fields	132
Table 50: Reset Configuration Fields.....	133
Table 51: Bindings Information Fields	134
Table 52: Server Statistics Fields	135
Table 53: Conflicts Information Fields.....	136
Table 54: Time Range Configuration	137
Table 55: Time Range Summary.....	138
Table 56: Time Range Entry Configuration.....	139
Table 57: DNS Global Configuration Fields.....	141
Table 58: DNS Server Configuration Fields.....	142
Table 59: DNS Host Name Mapping Configuration Fields.....	143
Table 60: DNS Host Name IP Mapping Summary Fields.....	144
Table 61: ISDP Global Configuration	145
Table 62: ISDP Cache Table	146
Table 63: ISDP Interface Configuration	147
Table 64: ISDP Statistics	148
Table 65: sFlow Agent Summary	150
Table 66: sFlow Receiver Configuration	151
Table 67: sFlow Poller Configuration.....	152
Table 68: sFlow Sampler Configuration.....	153
Table 69: Switch Detailed Statistics Fields.....	155
Table 70: Switch Summary Fields.....	156
Table 71: Detailed Port Statistics Fields	158
Table 72: Port Summary Statistics Fields.....	164

Table 73: Download File to Switch Fields	168
Table 74: HTTP File Download Fields.....	170
Table 75: Upload File from Switch Fields	171
Table 76: Multiple Image Service Fields	173
Table 77: Dual Image Status Fields.....	174
Table 78: AutoInstall Fields	176
Table 79: Forwarding Database Search Fields.....	179
Table 80: VLAN Configuration Fields	181
Table 81: VLAN Status Fields	182
Table 82: VLAN Port Configuration Fields	183
Table 83: VLAN Port Summary Fields	184
Table 84: Protocol Group Fields (No Groups).....	185
Table 85: Protocol Group Fields	186
Table 86: Protocol-based VLAN Summary Fields	187
Table 87: IP Subnet-based VLAN Configuration Fields	188
Table 88: IP Subnet-based VLAN Summary Fields.....	189
Table 89: MAC-based VLAN Configuration Fields.....	190
Table 90: MAC-based VLAN Summary Fields	190
Table 91: Double VLAN Tunneling Fields.....	191
Table 92: Double VLAN Tunneling Summary Fields	192
Table 93: Voice VLAN Configuration Fields	193
Table 94: Protected Port Configuration Fields	195
Table 95: Protected Ports Summary Fields	196
Table 96: MAC Filter Configuration Fields.....	197
Table 97: GARP Status Fields	200
Table 98: GARP Switch Configuration Fields	201
Table 99: GARP Port Configuration Fields	202
Table 100: Port Channel Configuration Fields.....	205
Table 101: Port Channel Status Fields.....	206
Table 102: IGMP Snooping Global Configuration and Status Fields.....	209
Table 103: IGMP Snooping Interface Configuration Fields.....	210
Table 104: IGMP Snooping VLAN Configuration Fields	211
Table 105: IGMP Snooping VLAN Status Fields	212
Table 106: Multicast Router Configuration Fields.....	213
Table 107: Multicast Router Status Fields.....	214
Table 108: Multicast Router VLAN Configuration Fields	215
Table 109: Multicast Router VLAN Status Fields	216

Table 110: IGMP Snooping Querier Configuration Fields.....	217
Table 111: IGMP Snooping Querier VLAN Configuration Fields	218
Table 112: IGMP Snooping Querier VLAN Configuration Summary Fields.....	219
Table 113: IGMP Snooping Querier VLAN Status Fields	220
Table 114: MLD Snooping Global Configuration and Status Fields	221
Table 115: MLD Snooping Interface Configuration Fields	222
Table 116: MLD Snooping VLAN Status Fields.....	223
Table 117: MLD Snooping VLAN Configuration Fields.....	224
Table 118: MLD Snooping Multicast Router Configuration Fields.....	225
Table 119: MLD Snooping Multicast Router Status Fields.....	226
Table 120: Multicast Router VLAN Configuration Fields	227
Table 121: MLD Snooping Multicast Router VLAN Status Fields.....	228
Table 122: MLD Snooping Querier Configuration Fields	229
Table 123: MLD Snooping Querier VLAN Configuration Fields	230
Table 124: MLD Snooping Querier VLAN Configuration Summary Fields	231
Table 125: MLD Snooping Querier VLAN Status Fields	232
Table 126: MFDB Table Fields	233
Table 127: GMRP Table Fields	234
Table 128: MFDB IGMP Snooping Table Fields.....	235
Table 129: MLD Snooping Table Fields.....	236
Table 130: Multicast Forwarding Database Statistics Fields	237
Table 131: Spanning Tree Switch Configuration/Status Fields.....	239
Table 132: Spanning Tree CST Configuration/Status Fields.....	240
Table 133: Spanning Tree MST Configuration/Status	243
Table 134: Spanning Tree CST Port Configuration/Status Fields.....	245
Table 135: Spanning Tree MST Port Configuration/Status Fields	248
Table 136: Spanning Tree Statistics Fields.....	250
Table 137: DHCP Snooping Configuration	251
Table 138: DHCP Snooping VLAN Configuration	252
Table 139: DHCP Snooping Interface Configuration.....	253
Table 140: LLDP Global Configuration Fields.....	255
Table 141: LLDP Interface Configuration Fields.....	256
Table 142: LLDP Interface Summary Fields	257
Table 143: LLDP Statistics Fields.....	258
Table 144: LLDP Local Device Information Fields	260
Table 145: LLDP Local Device Summary Columns	261
Table 146: LLDP Remote Device Information Fields.....	261

Table 147: LLDP Remote Device Summary Columns.....	262
Table 148: LLDP Global Configuration Fields.....	263
Table 149: LLDP-MED Interface Configuration Fields.....	264
Table 150: LLDP-MED Interface Summary Fields	265
Table 151: LLDP-MED Local Device Information Fields	266
Table 152: LLDP-MED Remote Device Information Fields.....	268
Table 153: Dynamic ARP Inspection Configuration	270
Table 154: Dynamic ARP Inspection VLAN Configuration	271
Table 155: Dynamic ARP Inspection Interface Configuration	272
Table 156: Dynamic ARP Inspection ARP ACL Configuration.....	273
Table 157: Dynamic ARP Inspection ARP ACL Rule Configuration.....	274
Table 158: Dynamic ARP Inspection Statistics.....	275
Table 159: BOOTP/DHCP Relay Agent Configuration Fields.....	277
Table 160: BOOTP/DHCP Relay Agent Status Fields.....	278
Table 161: IP Helper Global Configuration Fields.....	279
Table 162: IP Helper Global Configuration Add Fields	280
Table 163: IP Helper Interface Configuration Fields.....	281
Table 164: IP Helper Interface Configuration Add Fields	282
Table 165: IP Helper – Helper Statistics Fields	283
Table 166: ARP Create Fields.....	285
Table 167: ARP Table Configuration Fields.....	286
Table 168: ARP Table Fields.....	287
Table 169: ARP Cache Fields.....	288
Table 170: IP Configuration Fields.....	289
Table 171: IP Interface Configuration Fields	291
Table 172: IP Statistics Fields.....	293
Table 173: Configured Loopback Interface Fields	297
Table 174: Loopback Interface Secondary Address Fields	297
Table 175: Loopbacks Summary Fields.....	299
Table 176: RIP Configuration Fields.....	300
Table 177: RIP Interface Configuration Fields	302
Table 178: RIP Interface Summary Fields.....	304
Table 179: RIP Route Redistribution Configuration Fields	305
Table 180: RIP Route Redistribution Summary Fields	306
Table 181: Router Discovery Configuration Fields	307
Table 182: Router Discovery Status Fields	308
Table 183: Route Table Fields	309

Table 184: Best Routes Table Fields	311
Table 185: Configured Routes Fields	312
Table 186: Route Entry Create Fields	313
Table 187: Route Preferences Configuration Fields	314
Table 188: VLAN Routing Configuration Fields.....	316
Table 189: VLAN Routing Summary Fields	318
Table 190: VRRP Configuration	319
Table 191: Virtual Router Configuration Fields	320
Table 192: VRRP Interface Tracking Configuration Fields	322
Table 193: VRRP Track Interface Fields	323
Table 194: VRRP Route Tracking Configuration Fields	324
Table 195: VRRP Route Tracking Fields	325
Table 196: Virtual Router Status Fields	326
Table 197: Virtual Router Statistics Fields	327
Table 198: 802.1p Priority Mapping	330
Table 199: Trust Mode Configuration Fields	331
Table 200: IP DSCP Mapping Configuration Fields	332
Table 201: Interface Configuration Fields	333
Table 202: Interface Queue Configuration Fields.....	334
Table 203: Diffserv Configuration Fields	337
Table 204: Diffserv Class Configuration Fields	339
Table 205: Policy Configuration Fields	341
Table 206: Policy Class Definition Fields.....	343
Table 207: Service Configuration Fields	345
Table 208: Service Statistics Fields	346
Table 209: Service Detailed Statistics Fields.....	348
Table 210: Auto VoIP Configuration Fields.....	350
Table 211: IP ACL Configuration Fields.....	352
Table 212: IP ACL Rule Configuration Fields.....	354
Table 213: MAC ACL Configuration Fields	360
Table 214: MAC ACL Rule Configuration Fields	362
Table 215: ACL Interface Configuration Fields	366
Table 216: Port Security Interface Configuration Fields.....	370
Table 217: Port Security Static Fields	371
Table 218: Port Security Dynamic Fields	372
Table 219: Port Security Violation Status Fields.....	373
Table 220: Secure HTTP Configuration Fields.....	374

Table 221: Secure Shell Configuration Fields	377
Table 222: Captive Portal Global Configuration	380
Table 223: Captive Portal Summary	381
Table 224: CP Configuration	383
Table 225: CP Web Page Customization.....	387
Table 226: Local User Summary	390
Table 227: Local User Configuration	391
Table 228: Local User Configuration	392
Table 229: Captive Portal User RADIUS Attributes.....	393
Table 230: Global Captive Portal Configuration	395
Table 231: Global Captive Portal Status	397
Table 232: CP Activation and Activity Status.....	398
Table 233: Interface Activation Status	399
Table 234: Interface and Capability Status.....	400
Table 235: Client Summary	401
Table 236: Client Detail	402
Table 237: Client Interface Association Connection Statistics	403
Table 238: Interface - Client Status	404
Table 239: CP - Client Status.....	404
Table 240: SNMP Trap Configuration	405
Table 241: RADIUS Configuration Fields.....	406
Table 242: RADIUS Server Configuration Fields	409
Table 243: RADIUS Server Configuration Fields	410
Table 244: RADIUS Accounting Server Configuration Fields	412
Table 245: Named Accounting Server Fields.....	413
Table 246: Global Port Access Control Configuration Fields	415
Table 247: Port Access Control Port Configuration Fields.....	417
Table 248: PAE Capability Configuration	418
Table 249: Dot1x Supplicant Port Configuration.....	419
Table 250: Port Access Control Status Fields	421
Table 251: Port Access Control Port Summary Fields	425
Table 252: Port Access Control Statistics Fields	426
Table 253: Port Access Control Client Summary Fields	427
Table 254: Port Access Privileges Fields	428
Table 255: TACACS+ Configuration Fields	429
Table 256: TACACS+ Configuration Fields	430
Table 257: Global WLAN Status/Statistics.....	440

Table 258: Switch Status/Statistics.....	444
Table 259: AP Hardware Capability Radio Detail.....	447
Table 260: Peer Switch Configuration	449
Table 261: AP Hardware Capability Summary.....	451
Table 262: AP Hardware Capability Radio Detail.....	451
Table 263: AP Image Capability.....	452
Table 264: Peer Switch Status	453
Table 265: Peer Switch Configuration Status	454
Table 266: Peer Switch Managed AP Status.....	455
Table 267: Monitoring All Access Points	456
Table 268: Managed Access Point Status.....	459
Table 269: Detailed Managed Access Point Status	461
Table 270: Managed AP Radio Summary	464
Table 271: Managed AP Radio Detail	464
Table 272: Radio Detail Regulatory Domain.....	465
Table 273: Managed AP Neighbor Status.....	466
Table 274: Neighbor AP Clients	467
Table 275: Managed Access Point VAP Status	468
Table 276: Managed Access Point VAP TSPEC Status.....	469
Table 277: Distributed Tunneling Status	470
Table 278: Managed Access Point WLAN Summary Statistics	471
Table 279: Managed Access Point Ethernet Summary Statistics	472
Table 280: Detailed Managed Access Point Statistics	472
Table 281: Managed Access Point Radio Statistics.....	474
Table 282: Managed Access Point VAP Statistics	475
Table 283: Managed Access Point Distributed Tunneling Statistics.....	476
Table 284: Access Point Authentication Failure Status	478
Table 285: Access Point Authentication Failure Details	479
Table 286: Access Point RF Scan Status.....	481
Table 287: Detailed Access Point RF Scan Status	483
Table 288: Access Point Triangulation Status.....	484
Table 289: WIDS AP Rogue Classification.....	486
Table 290: AP De-Authentication Attack Status.....	487
Table 291: Associated Client Status Summary	489
Table 292: Detailed Associated Client Status	491
Table 293: Associated Client QoS Status	492
Table 294: Associated Client Neighbor AP Status	493

Table 295: Associated Client Distributed Tunneling Status.....	495
Table 296: Associated Client TSPEC Status.....	496
Table 297: Associated Client RRM Status.....	497
Table 298: SSID Associated Client Status	498
Table 299: VAP Associated Client Status.....	499
Table 300: Switch Associated Client Status.....	500
Table 301: Associated Client Association Summary Statistics.....	501
Table 302: Associated Client Session Summary Statistics	502
Table 303: Associated Client Association Detail Statistics	503
Table 304: Associated Client Session Detail Statistics.....	504
Table 305: Associated Client TSPEC Statistics	505
Table 306: Ad Hoc Client Status	506
Table 307: Detected Client Status	508
Table 308: Detailed Detected Client Status.....	509
Table 309: WIDS Client Rogue Classification	512
Table 310: Detected Client Pre-Authentication History.....	513
Table 311: Detected Client Triangulation.....	514
Table 312: Detected Client Roam History	515
Table 313: Detected Client Pre-Authentication History Summary.....	516
Table 314: Detected Client Roam History	517
Table 315: RRM Channel Load Configuration.....	518
Table 316: RRM Channel Load History	520
Table 317: RRM Neighbors Summary.....	521
Table 318: WDS Group Status Summary	522
Table 319: WDS AP Group Status	523
Table 320: WDS AP Group Status Summary.....	525
Table 321: WDS AP Link Status Summary	526
Table 322: WDS Group Link Statistics Summary	528
Table 323: Basic Wireless Global Configuration.....	530
Table 324: L3 VLAN Discovery	536
Table 325: Profile	537
Table 326: Radio Settings.....	539
Table 327: Default VAP Configuration.....	544
Table 328: Wireless Network Configuration	546
Table 329: Static WEP.....	552
Table 330: WPA Security	554
Table 331: Valid Access Point Summary.....	556

Table 332: Valid AP Configuration.....	558
Table 333: Valid AP Configuration (Standalone Mode).....	560
Table 334: Local OUI Database Summary	561
Table 335: Reset Fields.....	562
Table 336: RF Channel Plan and Power Adjustment	565
Table 337: Channel Plan History.....	566
Table 338: Manual Channel Plan.....	568
Table 339: Manual Power Adjustments	569
Table 340: Software Download	571
Table 341: Advanced AP Management	573
Table 342: Managed AP Debug	574
Table 343: Managed AP Channel/Power Adjust	576
Table 344: AP Provisioning Summary Status.....	577
Table 345: AP Provisioning Status	579
Table 346: General Global Configurations	582
Table 347: SNMP Traps	585
Table 348: Distributed Tunneling Configuration	587
Table 349: Device Location Configuration.....	588
Table 350: Wireless Network List.....	589
Table 351: Access Point Profile Summary	592
Table 352: Access Point Profile Global Configuration	595
Table 353: Radio Settings.....	598
Table 354: Default VAP Configuration.....	604
Table 355: QoS Settings.....	607
Table 356: TSPEC Configuration	610
Table 357: Peer Switch Configuration Request Status	612
Table 358: Peer Switch Configuration Enable/Disable	613
Table 359: Mutual Authentication	615
Table 360: WIDS AP Configuration	617
Table 361: WIDS Client Configuration	620
Table 362: Known Client Summary	622
Table 363: Known Client Configuration.....	623
Table 364: Switch Certificate Request.....	624
Table 365: Switch Provisioning.....	625
Table 366: WDS Managed AP Group Configuration.....	629
Table 367: Edit WDS Managed AP Group Settings.....	630
Table 368: WDS Managed AP Summary.....	631

Table 369: WDS Managed AP Group Configuration.....	632
Table 370: WDS AP Link Configuration.....	633
Table 371: WDS Link Create	634
Table 372: Building	636
Table 373: Building Floor.....	637
Table 374: Managed AP Coordinates	638
Table 375: Managed AP Location Summary.....	639
Table 376: On-Demand Location Trigger.....	640
Table 377: On-Demand Location Trigger Global Status	642
Table 378: On-Demand Location Trigger Floor Status	643
Table 379: AP Triangulation Summary	645
Table 380: Detailed AP Triangulation Status	646
Table 381: Client Triangulation Summary	648
Table 382: Detailed Client Triangulation Status	649
Table 383: WLAN Visualization Menu Bar Options	657
Table 384: VAP Configuration Example Settings	673
Table 385: VAP Summary	689
Table 386: Wireless LAN Users.....	690
Table 387: WIDS/WIPS VAP Summary.....	709

About This Document

This guide describes how to configure the D-Link DWS-4000 Series Unified Wireless Switch (UWS) software features by using the Web-based graphical user interface (GUI). The Unified Wired and Wireless Access System architecture accommodates a variety of software modules, so D-Link DWS-4000 Series can be a Layer 2 switch in a basic network or a Layer 3 router in a large, complex network. The switch software includes WLAN features that allow it to manage and monitor multiple D-Link DWL-x600AP Access Points.

Audience

The information in this guide is intended for any of the following individuals:

- System administrators who are responsible for configuring and operating a network using D-Link DWS-4000 Series switch
- Level 1 and/or Level 2 Support providers

To obtain the greatest benefit from this guide, you should have an understanding of the base software and should have read the specification for your networking device platform. You should also have basic knowledge of Ethernet and networking concepts.

Organization

This guide contains the following sections:

- [Section 1: “Getting Started,” on page 47](#) contains information about performing the initial system configuration and accessing the user interfaces.
- [Section 2: “System Administration,” on page 62](#) describes how to configure administrative features such as SNMP, DHCP, and port information.
- [Section 3: “Using System Tools,” on page 165](#) describes how to perform the system-maintenance tasks available from the Tools menu.
- [Section 4: “Configuring L2 Features,” on page 177](#) describes how to manage and monitor the layer 2 switching features.
- [Section 5: “Configuring L3 Features,” on page 276](#) describes how to configure the layer 3 routing features.
- [Section 6: “Configuring Quality of Service,” on page 329](#) describes how to configure the Differentiated Services, Class of Service, and Auto VoIP features.
- [Section 7: “Configuring Access Control Lists,” on page 351](#) describes how to manage the D-Link DWS-4000 Series software ACLs.
- [Section 8: “Managing Device Security,” on page 368](#) contains information about configuring switch security information such as captive portal configuration, port access control, TACACS+, and RADIUS server settings.
- [Section 9: “Configuring the Wireless Features,” on page 431](#) describes how to configure the switch so it can manage multiple access points on the network.
- [Appendix A: “Configuration Examples,” on page 662](#) describe how to configure selected features on the switch by using the Web interface, command-line interface, and Simple Network Management Protocol (SNMP).

Additional Documentation

The following documentation provides additional information about D-Link DWS-4000 Series software:

- The *D-Link DWS-4000 Series CLI Command Reference* describes the commands available from the command-line interface (CLI) for managing, monitoring, and configuring the switch.
- The *Unified Wired & Wireless Access System Configuration Guide* contains several configuration scenarios that show how to set up a WLAN network and configure the wireless features.
- Release notes for this D-Link DWS-4000 Series product detail the platform-specific functionality of the software packages, including issues and workarounds.

Document Conventions

This section describes the conventions this document uses.



Note: A note provides more information about a feature or technology.



Caution! A caution provides information about critical aspects of the configuration, combinations of settings, events, or procedures that can adversely affect network connectivity, security, and so on.

This guide uses the typographical conventions described in [Table 1](#).

Table 1: Typographical Conventions

Symbol	Description	Example
Bold	Menu titles, button names, and keyboard names when referred to in steps	Click Submit to apply your settings.
Blue Text	Hyperlinked text.	See Section : "About This Document," on page 45.
<code>courier font</code>	Command-line text and file names	<code>(switch-prompt)#</code>

Section 1: Getting Started

This section describes how to start the switch and access the user interface. It contains the following sections:

- “Connecting the Switch to the Network”
- “Booting the Switch”
- “Understanding the User Interfaces”

Connecting the Switch to the Network

To enable remote management of the switch through telnet, a Web browser, or SNMP, you must connect the switch to the network. The default IP address/subnet mask of the switch management interface is 10.90.90.90/255.0.0.0 and DHCP is disabled on the switch. So you must either connect the switch to a 10.0.0.0 network or you must provide appropriate network parameters, such as the IP address, subnet mask, and default gateway by connecting to the switch command line interface (CLI) using the terminal interface via the EIA 232 port. You can manually configure the network parameters or enable the DHCP client on the switch to get those via DHCP.

After you configure network information, such as the IP address and subnet mask, and the switch is physically and logically connected to the network, you can manage and monitor the switch remotely through SSH, telnet, a Web browser, or an SNMP-based network management system. You can also continue to manage the switch through the terminal interface via the EIA-232 port.

To connect to the switch and configure or view network information, use the following steps:

1. Using a straight-through modem cable, connect a VT100/ANSI terminal or a workstation to the console (serial) port.
If you attached a PC, Apple®, or UNIX® workstation, start a terminal-emulation program, such as HyperTerminal or TeraTerm.
2. Configure the terminal-emulation program to use the following settings:
 - Baud rate: 115200 bps
 - Data bits: 8
 - Parity: none
 - Stop bit: 1
 - Flow control: none
3. Power on the switch.
4. Press the return key, and the User: prompt appears.
Enter admin as the user name. There is no default password. Press ENTER at the password prompt if you did not change the default password.
After a successful login, the screen shows the system prompt, which varies based on the D-Link DWS-4000 Series switch model. For example, the default prompt for a DWS-4026 switch is (DWS-4026)>.
5. At the (DWS-4026)> prompt, enter enable to enter the Privileged EXEC command mode. There is no default password to enter Privileged EXEC mode. Press ENTER at the password prompt if you did not change the

default password.

The command prompt changes to (DWS-4026)#.

6. Configure network information.

- To use a DHCP server to obtain the IP address, subnet mask, and default gateway information, enter:
`network protocol dhcp.`
- To manually configure the IPv4 address, subnet mask, and (optionally) default gateway, enter:
`network parms ipaddress netmask [gateway],` for example:
`network parms 192.168.2.23 255.255.255.0 192.168.2.1`
- To manually configure the IPv6 address, subnet mask, and (optionally) default gateway, enter:
`network ipv6 address address/prefix-length [eui64]`
`network ipv6 gateway gateway`

To view the network information, enter `show network`.

7. To save these changes so they are retained during a switch reset, enter the following command:

`copy system:running-config nvram:startup-config`

or use the command `write memory`.

After the switch is connected to the network, you can use the IP address for remote access to the switch by using a Web browser or through telnet or SSH.

Booting the Switch

When the power is turned on with the local terminal already connected, the switch goes through Power-On Self-Test (POST). POST runs every time the switch is initialized and checks hardware components to determine if the switch is fully operational before completely booting.

If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM.

POST messages are displayed on the terminal and indicate test success or failure.

To boot the switch, perform the following steps:

1. Make sure that the serial cable is connected to the terminal.

2. Power on the switch.

As the switch boots, the bootup test first counts the switch memory availability and then continues to boot.

3. During boot, you can use the Boot menu, if necessary, to run special procedures. To enter the Boot menu, press **2** within the first ten seconds after the following message appears.

Select an option. If no selection in 10 seconds then operational code will start.

1 - Start operational code.

2 - Start Boot Menu.

Select (1, 2):2

For information about the Boot menu, see [““Boot Menu Functions” on page 49.”](#) If you do not start the boot menu, the operational code continues to load. After the switch boots successfully, the User login prompt appears and you can use the local terminal to begin configuring the switch. However, before configuring the switch, make sure that the software version installed on the switch is the latest version. If it is not the latest version, download and install the latest version. See [“Download File To Switch \(TFTP\)” on page 167.](#)

Boot Menu Functions

You can perform many configuration tasks through the Boot menu, which can be invoked after the first part of the POST is completed.

Use the following procedures to display the Boot menu:

1. During the boot process, press **2** within ten seconds after the following message displays:

```
Boot Menu Version: 12 jun 2007
Select an option. If no selection in 10 seconds then
operational code will start.
```

```
1 - Start operational code.
2 - Start Boot Menu.
Select (1, 2):2
```

```
Boot Menu Version: 12 jun 2007
```

```
Options available
1 - Start operational code
2 - Change baud rate
3 - Retrieve event log using XMODEM
4 - Load new operational code using XMODEM
5 - Load configuration using XMODEM
6 - Display operational code vital product data
7 - Run flash diagnostics
8 - Update boot code
9 - Delete operational code
10 - Reset the system
11 - Restore configuration to factory defaults (delete config files)
12 - Activate Backup Image
[Boot Menu]
```

The following sections describe the Boot menu options. If no selection is made within 10 seconds (default), the operational code starts.

Start Operational Code

Use option 1 to resume loading the operational code.

To relaunch the boot process from the Boot menu:

1. On the **Boot menu**, select **1** and press **<Enter>**.

The following prompt displays:

```
Operational Code Date: Thu Jun 8 12:51:44 2006
Uncompressing.....
```

```

                                     50%                               100%
|||||                               |||||||
  1 File: bootos.c                               Line: 462 Task: fffffe00 EC: 2863311530 (0xaaaaaaaa)
(0 d 0 hrs 0 min 13 sec)
Timebase: 24.750275 MHz, MEM: 99.001100 MHz, PCI: 33.000366 MHz, CPU: 198.002200 MHz
PCI device BCM5675_A0 attached as unit 0.
PCI device BCM5695_B0 attached as unit 1.
PCI device BCM5695_B0 attached as unit 2.
PCI device BCM5673_A1 attached as unit 3.
PCI device BCM5673_A1 attached as unit 4.
Adding BCM transport pointers
Configuring CPUTRANS TX
Configuring CPUTRANS RX
st_state(0) = 0x0
st_state(1) = 0x3
st_state(2) = 0x2
```

Change Baud Rate

Use option 2 to change the baud rate of the serial interface.

To change the baud rate from the Boot menu:

1. On the **Boot menu**, select **2** and press **<Enter>**.

The following prompt displays:

```
[Boot Menu]2
Select baud rate:
1 - 1200
2 - 2400
3 - 4800
4 - 9600
5 - 19200
6 - 38400
7 - 57600
8 - 115200
0 - no change
```



Note: The selected baud rate takes effect immediately.

2. The bootup process resumes.

Retrieve Event Log Using XMODEM

Use option 3 to retrieve the event log and download it to your ASCII terminal.

To retrieve the event log from the Boot menu:

1. On the **Boot menu**, select **3** and press **<Enter>**.

The following prompt displays:

```
[Boot Menu] 3
Sending event log, start XMODEM receive.....
File asciilog.bin Ready to SEND in binary mode
Estimated File Size 169K, 1345 Sectors, 172032 Bytes
Estimated transmission time 3 minutes 20 seconds
Send several Control-X characters to cancel before transfer starts.
```

2. The bootup process resumes.

Load New Operational Code Using XMODEM

Use option 4 when a new software version must be downloaded to replace corrupted files, update, or upgrade the system software.

To download software from the Boot menu:

1. On the **Boot menu**, select **4** and press **<Enter>**.

The following prompt displays:

```
[Boot Menu] 4
Ready to receive the file with XMODEM/CRC....
Ready to RECEIVE File xcode.bin in binary mode
Send several Control-X characters to cancel before transfer starts.
```

2. When using HyperTerminal, click **Transfer** on the **HyperTerminal** menu bar.

3. From the **Transfer** menu, click **Send File**.

The **Send File** window displays.

4. Enter the file path for the file to be downloaded.

5. Make sure the protocol is defined as XMODEM.

6. Click **Send**.

The software is downloaded. Software downloading takes several minutes. The terminal emulation application, such as HyperTerminal, may display the loading process progress.

After software downloads, the switch reboots automatically.

Load Configuration Using XMODEM

Use option 5 when a new configuration file must be downloaded to replace the saved system configuration file.

To download software from the Boot menu:

1. On the **Boot menu**, select **5** and press **<Enter>**.

The following prompt displays:

```
[Boot Menu] 4
```

```
Ready to receive the file with XMODEM/CRC....
```

```
Ready to RECEIVE File tempcfg.bin in binary mode
```

```
Send several Control-X characters to cancel before transfer starts.
```

2. When using HyperTerminal, click **Transfer** on the **HyperTerminal** menu bar.
3. From the **Transfer** menu, click **Send File**.

The **Send File** window displays.

4. Enter the file path for the file to be downloaded.
5. Make sure the protocol is defined as XMODEM.
6. Click **Send**.

The configuration file is downloaded. The terminal emulation application, such as HyperTerminal, may display the loading process progress.

Display Operational Code Vital Product Data

Use option 6 to view boot image information.

To display boot image information from the Boot menu:

1. On the **Boot menu**, select **6** and press **<Enter>**.

The following prompt displays:

```
[Boot Menu] 6
```

```
The following image is in the Flash File System:
```

```
File Name.....image1
```

```
CRC.....0xb017 (45079)
```

```
Target Device.....0x00508541
```

```
Size.....0x8ec50c (9356556)
```

```
Number of Components.....2
```

```
Operational Code Size.....0x7ec048 (8306760)
```

```
Operational Code Offset.....0x74 (116)
```

```
Operational Code FLASH flag.....1
```

```
Operational Code CRC.....0x9B4D
```

```
Boot Code Version.....1
```

```
Boot Code Size.....0x100000 (1048576)
```

```
Boot Code Offset.....0x7ec0bc (8306876)
```

```
Boot Code FLASH flag.....0
```

```
Boot Code CRC.....0x1CB8
```

```
VPD - rel 0 ver 31 maint_lvl 0
```

```
Timestamp - Thu Jun 8 12:51:44 2006
```

```
File - pc62xxr0v31.stk[Boot Menu]
```

2. The bootup process resumes.

Run Flash Diagnostics

Use option 7 to run flash diagnostics. User action is confirmed with a Y/N question before executing the command.

To perform a complete test of the flash memory from the Boot menu:

1. On the **Boot menu**, select **6** and press **<Enter>**.

The following prompt displays:

```
[Boot Menu] 7
Do you wish to run flash diagnostics? (Boot code region will not be tested.) (y/n): y
Input number of diagnostic iterations -> 1
Testing 2 x 28F128J3 base: 0xfe000000
Iterations remaining = 1
```

```
Erasing sector 0
Verify sector 0 erased
Writing sector 0
Erasing sector 1
Verify sector 1 erased
Writing sector 1
Erasing sector 2
Verify sector 2 erased
Writing sector 2
Erasing sector 3
Verify sector 3 erased
Writing sector 3
Erasing sector 4
Verify sector 4 erased
Writing sector 4
Erasing sector 5
Verify sector 5 erased
Writing sector 5
Erasing sector 6
Verify sector 6 erased
Writing sector 6
```



Note: This process runs until all sectors have been erased, verified erased, and written.

```
Flash Diagnostics passed
[Boot Menu]
```

2. The bootup process resumes.

Update Boot Code

Use option 8 to update the boot code in the flash memory. This option is only valid after loading new boot code using Boot Menu option 4. User action is confirmed with a Y/N question before executing the command.

To download software from the Boot menu:

1. On the **Boot menu**, select **8** and press **<Enter>**.

The following prompt displays:

```
Do you wish to update Boot Code? (y/n) y
Erasing Boot Flash.....Done.
Wrote 0x10000 bytes.
Wrote 0x20000 bytes.
Wrote 0x30000 bytes.
Wrote 0x40000 bytes.
Wrote 0x50000 bytes.
Wrote 0x60000 bytes.
Boot code updated
```

2. The bootup process resumes.

Delete Operational Code

Use option 9 to delete the active image from the flash memory. User action is confirmed with a Y/N question before executing the command.

To delete the backup image from the Boot menu:

1. On the **Boot menu**, select **8** and press **<Enter>**.

The following prompt displays:

```
Are you SURE you want to delete operational code : image2 ? (y/n):y
Operational code deleted...
[Boot Menu]
```

2. The bootup process resumes.

Reset the System

Use option 10 to clear all flash and reset the system to its default setting. User action is confirmed with a Y/N question before executing the command.

To reset the system from the Boot menu:

1. On the **Boot menu**, select **10** and press **<Enter>**.

The following prompt displays:

```
[Boot Menu] 10
Are you SURE you want to reset the system? (y/n):y
Boot code.....
SDRAM 256
```

Boot Menu Version: Oct 20 2004

Select an option. If no selection in 10 seconds then operational code will start.

- 1 - Start operational code.
- 2 - Start Boot Menu.

Select (1, 2):2

2. The bootup process resumes.

Restore Configuration To Factory Defaults (Delete Configuration Files)

Use option 11 to load using the system default configuration and to boot without using the current startup configuration. Selecting 11 from the Boot Menu restores system defaults. Boot Sequence can then be started by selecting 1 from the Boot Menu.

To download software from the Boot menu:

1. On the **Boot menu**, select **11** and press **<Enter>**.

The following prompt displays:

```
Are you SURE you want to delete the configuration? (y/n):y
```

2. The bootup process resumes.

Activate Backup Image

Use option 12 to activate the backup image. The active image becomes the backup when this option is selected.

To activate the backup image:

1. From the **Boot menu**, select **12** and press **<Enter>**.

The following message displays:

```
Backup image - image2 activated.
```

2. The bootup process resumes.

Understanding the User Interfaces

D-Link DWS-4000 Series software includes a set of comprehensive management functions for configuring and monitoring the system by using one of the following three methods:

- Web User Interface
- Command-Line Interface (CLI)
- Simple Network Management Protocol (SNMP)

Each of the standards-based management methods allows you to configure and monitor the components of the D-Link DWS-4000 Series software. The method you use to manage the system depends on your network size and requirements, and on your preference.

This guide describes how to use the Web-based interface to manage and monitor the system. For information about how to manage and monitor the system by using the CLI, see the *D-Link DWS-4000 Series CLI Command Reference*.

Using the Web Interface

To access the switch by using a Web browser, the browser must meet the following software requirements:

- HTML version 4.0, or later
- HTTP version 1.1, or later
- JavaScript™ version 1.5, or later

Use the following procedures to log on to the Web Interface:



Note: The switch web UI supports Internet Explorer v6 and v7. Appropriate display of the web pages is not guaranteed for other web browsers.

1. Open a Web browser and enter the IP address of the switch in the Web browser address field.
2. Type the user name and password into the fields on the login screen, and then click **Login**.

The user name and password are the same as those you use to log on to the command-line interface. By default, the user name is **admin**, and there is no password. Passwords are case sensitive.

User Name

Password

3. After the system authenticates you, the System Description page displays.

Figure 1 shows the layout of the switch Web interface. Each Web page contains three main areas: device view, the navigation tree, and the configuration status and options.

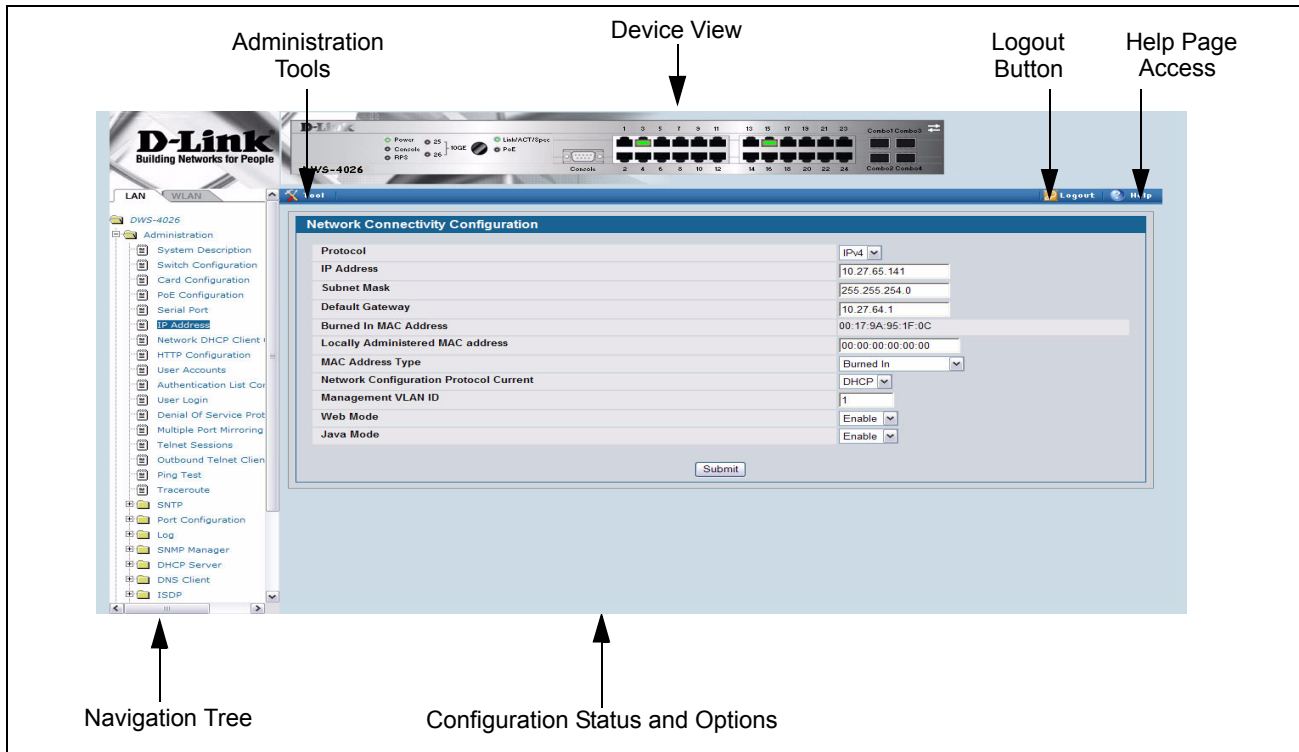


Figure 1: Web Interface Layout

Device View

The Device View is a Java® applet that displays the ports on the switch. This graphic appears at the top of each page to provide an alternate way to navigate to configuration and monitoring options. The graphic also provides information about device ports, current configuration and status, table information, and feature components.

The port coloring indicates if a port is currently active. Green indicates that the port is enabled, red indicates that an error has occurred on the port, and blue indicates that the link is disabled.

Figure 2 shows the Device View for the back of the system.

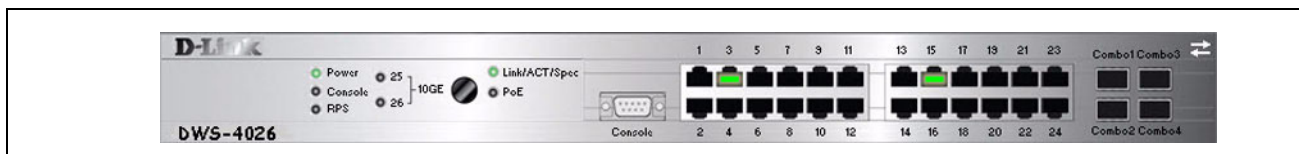


Figure 2: Device View—Back

Click the port you want to view or configure to see a menu that displays statistics and configuration options. Click the menu option to access the page that contains the configuration or monitoring options.

If you click the graphic but do not click a specific port, the main menu appears, as [Figure 3](#) shows. This menu contains the same option as the navigation menu on the left side of the page.

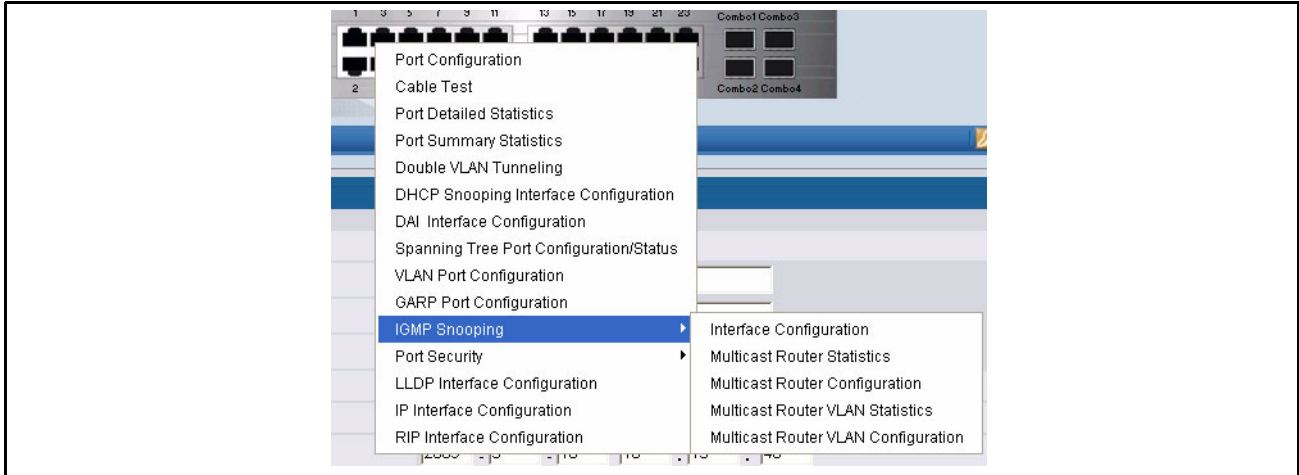


Figure 3: Cascading Navigation Menu

Navigation Tree View

The hierarchical-tree view is on the left side of the Web interface. The tree view contains a list of various device features. The branches in the navigation tree can be expanded to view all the components under a specific feature, or retracted to hide the feature's components.

The tree consists of a combination of folders, subfolders, and configuration and status HTML pages. Click the folder to view the options in that folder. Each folder contains either subfolders or HTML pages, or a combination of both. [Figure 4](#) shows an example of a folder, subfolder, and HTML page in the navigation menu. When you click a folder or subfolder that is preceded by a plus sign (+), the folder expands to display the contents. If you click an HTML page, a new page displays in the main frame. A folder or subfolder has no corresponding HTML page.

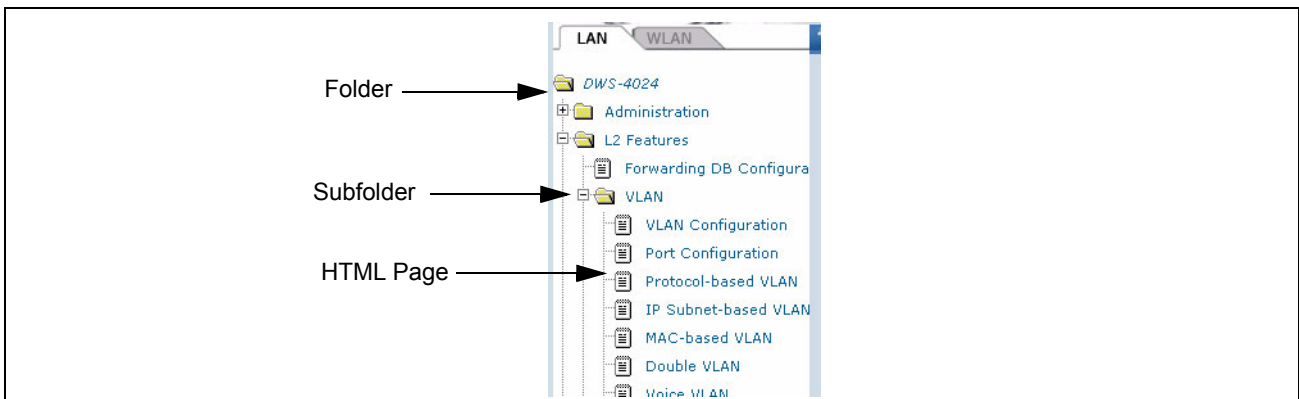


Figure 4: Navigation Tree View

The D-Link DWS-4000 Series switch navigation tree also contains a LAN tab for wired features and a WLAN tab for Wireless features, as the following figure shows.

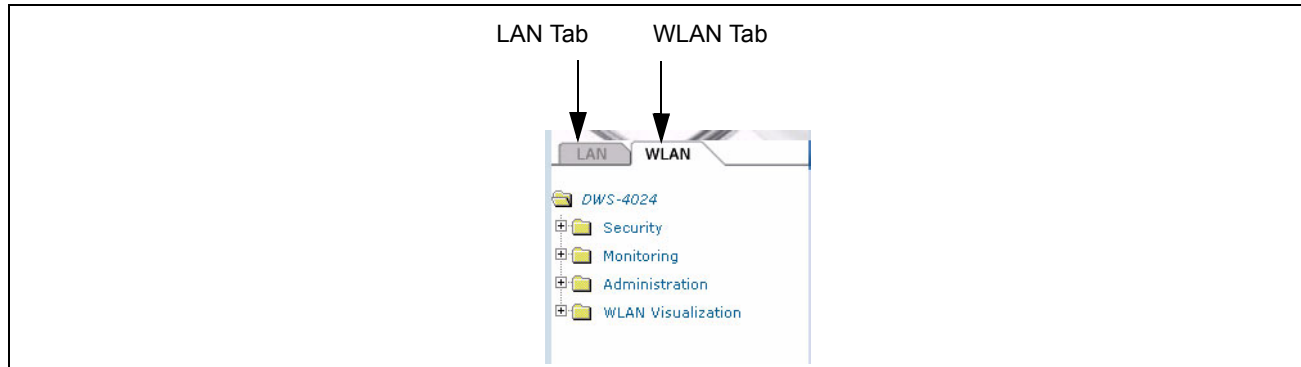


Figure 5: LAN and WLAN Tabs

Configuration and Monitoring Options

The panel directly under the graphic and to the right of the navigation menu displays the configuration information or status for the page you select. On pages that contain configuration options, you can input information into fields or select options from drop-down menus.

Each page contains access to the HTML-based help that explains the fields and configuration options for the page. Many pages also contain command buttons.

The command buttons in the following table are used throughout the pages in the Web interface:

Table 2: Common Command Buttons

Button	Function
Submit	Clicking the Submit button sends the updated configuration to the switch. Configuration changes take effect immediately, but changes are not retained across a power cycle unless you save them to the system configuration file. Note: To save the configuration to non-volatile memory, use the Save Changes option from the Administration Tools menu.
Refresh	Clicking the Refresh button refreshes the page with the latest information from the router.
Logout	Clicking the Logout button ends the session.



Caution! Submitting changes makes them effective during the current boot session only. You must save any changes if you want them to be retained across a power cycle (reboot). To save changes across a power cycle, **use the Save Changes option from the Administration Tools menu.**

Help Page Access

Every page contains a link to the online help, which contains information to assist in configuring and managing the switch. The online help pages are context sensitive. For example, if the IP Addressing page is open, the help topic for that page displays if you click Help. [Figure 6](#) shows the link to click to access online help on each page.



Figure 6: Help Link

[Figure 1](#) on page 57 shows the location of the Help link on the Web interface.

Using the Command-Line Interface

The command-line interface (CLI) is a text-based way to manage and monitor the system. You can access the CLI by using a direct serial connection or by using a remote logical connection with telnet or SSH.

The CLI groups commands into modes according to the command function. Each of the command modes supports specific software commands. The commands in one mode are not available until you switch to that particular mode, with the exception of the User EXEC mode commands. You can execute the User EXEC mode commands in the Privileged EXEC mode.

To display the commands available in the current mode, enter a question mark (?) at the command prompt. To display the available command keywords or parameters, enter a question mark (?) after each word you type at the command prompt. If there are no additional command keywords or parameters, or if additional parameters are optional, the following message appears in the output:

```
<cr>          Press Enter to execute the command
```

For more information about the CLI, see the *D-Link DWS-4000 Series CLI Command Reference*.

The *D-Link DWS-4000 Series CLI Command Reference* lists each command available from the CLI by the command name and provides a brief description of the command. Each command reference also contains the following information:

- The command keywords and the required and optional parameters.
- The command mode you must be in to access the command.
- The default value, if any, of a configurable setting on the device.

The `show` commands in the document also include a description of the information that the command shows.

Using SNMP

You can manage the D-Link DWS-4000 Series switch using SNMP. You can configure SNMP groups and users that can manage traps that the SNMP agent generates.

D-Link DWS-4000 Series uses both standard public MIBs for standard functionality and private MIBs that support additional switch functionality. SNMP is enabled by default.

Any user can connect to the switch using the SNMPv3 protocol, but for authentication and encryption, you need to configure a new user profile. To configure a profile by using the CLI, see the SNMP section in the *D-Link DWS-4000 Series CLI Command Reference*. To configure an SNMPv3 profile by using the Web interface, use the following steps:

1. Select **LAN > Administration > User Accounts** from the hierarchical tree on the left side of the Web interface.
2. From the **User** menu, select **Create** to create a new user.
3. Enter a new user name in the **User Name** field.
4. Enter a new user password in the **Password** field and then retype it in the **Confirm Password** field.
To use SNMPv3 Authentication for this user, set a password of eight or more alphanumeric characters.
5. To enable authentication, use the **Authentication Protocol** menu to select either MD5 or SHA for the authentication protocol.
6. To enable encryption, use the **Encryption Protocol** menu to select **DES** for the encryption scheme. Then, enter an encryption code of eight or more alphanumeric characters in the Encryption Key field.
7. Click **Submit**.

Section 2: System Administration

Use the features in the Administration navigation tree folder to define the switch's relationship to its environment. The **Administration** folder contains links to the following features:

- ["System Description"](#)
- ["Switch Configuration"](#)
- ["Card Configuration"](#)
- ["PoE Configuration"](#)
- ["Serial Port"](#)
- ["IP Address"](#)
- ["Network DHCP Client Options"](#)
- ["HTTP Configuration"](#)
- ["User Accounts"](#)
- ["Authentication List Configuration"](#)
- ["User Login"](#)
- ["Denial of Service Protection"](#)
- ["Multiple Port Mirroring"](#)
- ["Managing and Viewing Logs"](#)
- ["Telnet Sessions"](#)
- ["Outbound Telnet Client Configuration"](#)
- ["Ping Test"](#)
- ["TraceRoute"](#)
- ["Configuring SNMP Settings"](#)
- ["Configuring and Viewing Device Port Information"](#)
- ["Managing and Viewing Logs"](#)
- ["Defining SNMP Parameters"](#)
- ["Managing the DHCP Server"](#)
- ["Configuring Time Ranges"](#)
- ["Configuring DNS"](#)
- ["Configuring and Viewing ISDP Information"](#)
- ["Configuring sFlow"](#)
- ["Viewing System Statistics"](#)

System Description

After a successful login, the System Description page displays. Use this page to configure and view general device information.

To display the System Description page, click **LAN > Administration > System Description** in the navigation tree.

System Description	
System Description	D-Link DWS-4026
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
IP Address	10.27.65.141
System Object ID	1.3.6.1.4.1.171.10.73.5.1
System Time (yyyy-mm-dd h:m:s)	2009 - 12 - 9 16 : 11 : 32
System Up Time	1 days, 0 hours, 51 mins
Current SNTP Synchronized Time	Not Synchronized

Figure 7: System Description

Table 3: System Description Fields

Field	Description
System Description	The product name of this switch.
System Name	Enter the name you want to use to identify this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
System Location	Enter the location of this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
System Contact	Enter the contact person for this switch. You may use up to 31 alpha-numeric characters. The factory default is blank.
IP Address	The IP Address assigned to the network interface. To change the IP address, see “Serial Port” on page 70 .
System Object ID	The base object ID for the switch's enterprise MIB.
System Time (yyyy-mm-dd h:m:s)	Enter the current date and time that the switch will follow using the on-board real-time clock.
System Up Time	Displays the number of days, hours, and minutes since the last system restart.
Current SNTP Synchronized Time	Displays currently synchronized SNTP time in UTC. If no SNTP server has been configured and the time is not synchronized, this field displays “Not Synchronized.” To specify an SNTP server, see “Configuring SNTP Settings” on page 93 .

Defining System Information

1. Open the **System Description** page.
2. Define the following fields: **System Name**, **System Contact**, and **System Location**.
3. Click **Submit**.

The system parameters are applied, and the device is updated.



Note: If you want the switch to retain the new values across a power cycle, you must perform a configuration save, but the System Time does not need a save to retain the new values across a power cycle.

Switch Configuration

From the **Switch Configuration** page, you can control the IEEE 802.3x flow control mode for the switch.

IEEE 802.3x flow control works by pausing a port when the port becomes oversubscribed and dropping all traffic for small bursts of time during the congestion condition. This can lead to high-priority and/or network control traffic loss. When 802.3x flow control is enabled, lower speed switches can communicate with higher speed switches by requesting that the higher speed switch refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

To display the Switch Configuration page, click **LAN > Administration > Switch Configuration** in the navigation tree.

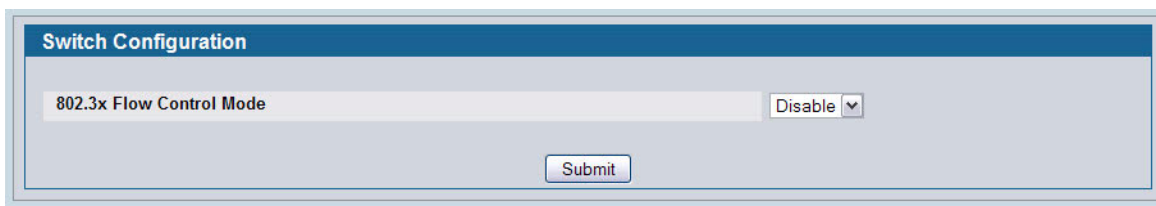


Figure 8: Switch Configuration

Table 4: Switch Configuration Fields

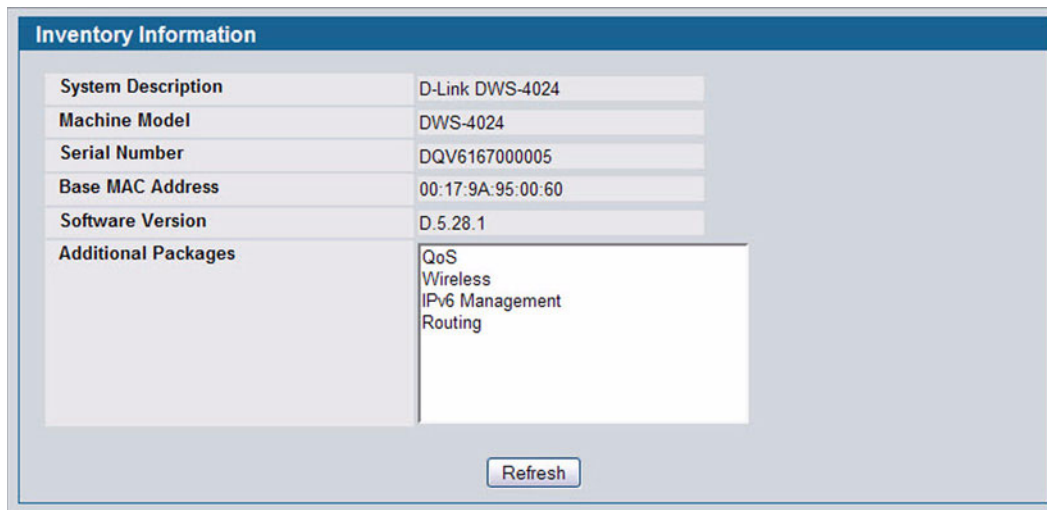
Field	Description
IEEE 802.3x Flow Control Mode	<p>Enables or disables IEEE 802.3x flow control on the system. The factory default is disabled.</p> <ul style="list-style-type: none"> • Enable: Enables flow control so that the switch can communicate with higher speed switches. • Disable: Disables flow control so that the switch does not send pause packets if the port buffers become full.

- If you change the mode, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Viewing Inventory Information

Use the **Inventory Information** page to display the switch's Vital Product Data, which is stored in non-volatile memory at the factory.

To display the inventory information, click **LAN > Monitoring > Inventory Information** page in the navigation tree.



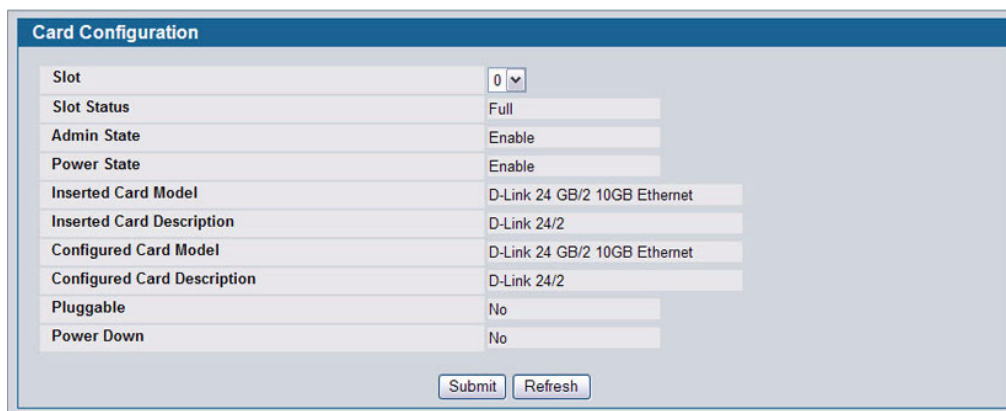
Inventory Information	
System Description	D-Link DWS-4024
Machine Model	DWS-4024
Serial Number	DQV6167000005
Base MAC Address	00:17:9A:95:00:60
Software Version	D.5.28.1
Additional Packages	QoS Wireless IPv6 Management Routing

Figure 9: Inventory Information

Card Configuration

The pages in the Slot folder provide information about the cards installed in the slots on the switch. To access the Card Configuration page, click **LAN > Administration > Card Configuration** in the navigation menu.

Figure 10 shows the fields that display when the slot contains a card.



Card Configuration	
Slot	0
Slot Status	Full
Admin State	Enable
Power State	Enable
Inserted Card Model	D-Link 24 GB/2 10GB Ethernet
Inserted Card Description	D-Link 24/2
Configured Card Model	D-Link 24 GB/2 10GB Ethernet
Configured Card Description	D-Link 24/2
Pluggable	No
Power Down	No

Figure 10: Card Configuration

Table 5: Card Configuration Fields

Field	Description
Slot	Indicates the slot in the selected unit for which data is to be displayed or configured.
Slot Status	Indicates whether a card is in the slot (Full or Empty).
Admin State	Displays whether the slot is administratively enabled or disabled. This field is non-configurable for read-only users.
Power State	Displays whether the slot is powered on or off. This field is non-configurable for read-only users.
Inserted Card Model	Displays the model identifier of the card plugged into the selected slot. If no card has been plugged in, this field is not shown.
Inserted Card Description	Displays the description of the card plugged into the selected slot. If no card has been plugged in, this field is not shown.
Configured Card Model	Displays the model identifier of the card pre-configured for the selected slot. If no card has been pre-configured, this field is not shown.
Configured Card Description	Displays the model identifier of the card pre-configured for the selected slot. If no card has been pre-configured, this field is not shown.
Pluggable	Displays the pluggable indicator of the specified slot.
Power Down	Displays the power down indicator of the specified slot.

- If you make any changes to the page, click **Submit** to apply the changes to the system.
- Click **Clear** to clear any pre-configuration of a card in a slot which does not have any card plugged into it. If there is a card plugged into the slot or the slot has no card plugged and has not been pre-configured yet, this button is not shown.

Slot Summary

The **Slot Summary** page displays information about the slots present in the switch.

To access the Slot Summary page, click **LAN > Monitoring > Slot Summary** in the navigation tree.



Slot	Status	Administrative State	Power State	Card Model ID	Card Description
1/0	Full	Enable	Enable	D-Link 24 Port Gigabit Ethernet	D-Link 24

Figure 11: Slot Summary

Table 6: Slot Summary Fields

Field	Description
Slot	Identifies the slot using the format unit/slot.
Status	Displays whether the slot is empty or full.
Administrative State	Displays whether the slot is administratively enabled or disabled
Power State	Displays whether the slot is powered on or off.
Card Model ID	Displays the model ID of the card configured for the slot.
Card Description	Displays the description of the card configured for the slot.

- Click **Refresh** to display the most current information from the router.

PoE Configuration

Use the PoE Configuration page to configure the Power over Ethernet (PoE) features.

To access the PoE Configuration page, click **LAN > Administration > PoE Configuration** in the navigation menu.

The following figure shows the fields that display.

Slot/Port	Admin Mode	Priority	Power Limit (Watts)
0/1	Enable	Low	16.0
0/2	Enable	Low	16.0
0/3	Enable	Low	16.0
0/4	Enable	Low	16.0
0/5	Enable	Low	16.0
0/6	Enable	Low	16.0
0/7	Enable	Low	16.0

Figure 12: PoE Configuration

Table 7: PoE Configuration Fields

Field	Description
System Usage Threshold	Sets threshold level at which a trap is sent if the total power consumed is greater than or equal to the specified percentage of total power available.
Slot/Port	Select the slot and port with the information to configure.
Admin Mode	Enables or disables the ability of the port to deliver power.
Priority	The switch may not be able to supply power to all connected devices. So, priority is used to determine which ports can supply power. For ports with the same priority, the lower numbered port will have a higher priority.
Power Limit	Defines the maximum power which can be delivered by a port.

- If you make any changes to the page, click **Submit** to apply the changes to the system.

PoE Status

Power over Ethernet (PoE) technology allows IP telephones, wireless LAN Access Points, Web-Cameras and many other appliances to receive power as well as data over existing LAN cabling, without needing to modify the existing Ethernet infrastructure.

To display the PoE status, click **LAN > Monitoring > PoE Status** page in the navigation tree.

PoE Status								
Max System Power Available							144	Watts
Current System Power Used							14.0	Watts
Slot/Port	Admin Mode	Class	Priority	Output Power (Watts)	Output Current (mA)	Output Voltage (Volts)	Power Limit (watts)	Status
0/1	Enabled	0	Low	0.0	0	0	16.0	Searching
0/2	Enabled	0	Low	0.0	0	0	16.0	Searching
0/3	Enabled	0	Low	0.0	0	0	16.0	Searching
0/4	Enabled	0	Low	0.0	0	0	16.0	Searching
0/5	Enabled	3	Low	7.1	141	50	16.0	Delivering Power
0/6	Enabled	0	Low	0.0	0	0	16.0	Searching
0/7	Enabled	3	Low	7.6	150	50	16.0	Delivering Power

Figure 13: PoE Status

Serial Port

The Serial Port Configuration page allows you to change the switch's serial port settings. In order for a terminal or terminal emulator to communicate with the switch, the serial port settings on both devices must be the same. Some settings on the switch cannot be changed.

To view or configure the serial port settings on the switch, click **LAN > Administration > Serial Port** in the navigation tree.

Figure 14: Serial Port

Table 8: Serial Port Fields

Field	Description
Serial Port Login Timeout (minutes)	Indicates how many minutes of inactivity should occur on a serial port connection before the switch closes the connection. Enter a number between 0 and 160. The factory default is 5. Entering 0 disables the timeout.
Baud Rate (bps)	Select the default baud rate for the serial port connection from the menu. The factory default is 115200.
Character Size (bits)	The number of bits in a character. This is always 8.
Flow Control	Whether hardware flow control is enabled or disabled. It is always disabled.
Stop Bits	The number of stop bits per character. Its is always 1.
Parity	The parity method used on the serial port. It is always None.

- If you change any data, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

IP Address

The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

The Network Connectivity page allows you to change the IP information using the Web interface.

To access the page, click **LAN > Administration > IP Address** in the navigation tree.

Note that the page displays differently depending on the IP protocol version chosen.

Network Connectivity Configuration	
Protocol	IPv4
IP Address	8.0.1.22
Subnet Mask	255.255.255.0
Default Gateway	8.0.1.1
Burned In MAC Address	00:1A:9B:9C:1D:2E
Locally Administered MAC address	00:00:00:00:00:00
MAC Address Type	Burned In
Network Configuration Protocol Current	DHCP
Management VLAN ID	1
Web Mode	Enable
Java Mode	Enable
Submit	

Figure 15: Network Connectivity—IPv4

Network Connectivity Configuration	
Protocol	IPv6
IPv6 Mode	Enable
IPv6 Prefix	FE80::21A:9BFF:FE9C:1D2E/64
IPv6 Gateway	
Default Routers	
Submit	

Figure 16: Network Connectivity—IPv6

Table 9: Network Connectivity Fields

Field	Description
Protocol	Selects the IP protocol version you want to configure on the interface. Depending on your selection, different fields display. Both protocols can be configured.
IPv4 Fields: These display when IPv4 is selected as the protocol.	
IP Address	The IP address of the network interface. The factory default value is 0.0.0.0 Note: Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are not valid.
Subnet Mask	The IP subnet mask for the interface. The factory default value is 0.0.0.0.
Default Gateway	The default gateway for the IP interface. The factory default value is 0.0.0.0.
Burned-in MAC Address	This read-only field displays the MAC address that is burned-in to the network card at the factory. This MAC address is used for in-band connectivity if you choose not to configure a locally administered address.
Locally Administered MAC Address	You can optionally configure a locally administered MAC address for in-band connectivity instead of using the burned-in universally administered MAC address. In addition to entering an address in this field, you must also set the MAC address type to locally administered. Enter the address as twelve hexadecimal digits (6 bytes) with a colon between each byte. Bit 1 of byte 0 must be set to a 1 and bit 0 to a 0; i.e., byte 0 must have a value between x'40' and x'7F'.
MAC Address Type	Select the MAC address to use for in-band connectivity. The factory default is to use the burned-in MAC address. <ul style="list-style-type: none"> • Burned-In: Use the factory default MAC address. • Locally Administered: Use the MAC address you entered in the Locally Administered MAC Address field.
Network Configuration Protocol Current	Specify what the switch should do following power-up. The factory default is None. The options are as follows: <ul style="list-style-type: none"> • BootP: Transmit a Bootp request • DHCP: Transmit a DHCP request • None: Do not send any requests following power-up.
Management VLAN ID	Specifies the management VLAN ID of the switch. The range is 1-3965. The management VLAN is used for management of the switch. This field is configurable for administrative users and read-only for other users.
Web Mode	Controls whether the switch user interface can be accessed from a Web browser. The factory default is enabled. <ul style="list-style-type: none"> • Enable: Permits Web-based management of the switch. • Disable: Prohibits Web-based management of the switch. If the Web mode is disabled, you must manage the switch by using SNMP or the CLI.
Java Mode	Controls whether to display the Java applet that displays a picture of the switch at the top right of the screen. The factory default is enabled: <ul style="list-style-type: none"> • Enable: Permits the applet to display. The Java applet lets click on the picture of the switch to select configuration screens instead of using the navigation tree at the left side of the screen. • Disable: Does not allow the Java applet to display. The applet is replaced by a blank area.

Table 9: Network Connectivity Fields (Cont.)

Field	Description
IPv6 Fields: These display when IPv6 is selected as the protocol.	
IPv6 Mode	Enables or disables IPv6 mode on the interface.
IPv6 Prefix	If no IPv6 address displays, select Add and then enter an IPv6 prefix/length. Select the EUI64 option if the last 64 bits are to be derived from the MAC address. For example, you can enter 2001::/64 and select the EUI64 option to have the 64-bit address calculated from the MAC address.
IPv6 Gateway	Enter the IPv6 gateway address (do not include a prefix).
Default Routers	Displays the address(es) entered in the IPv6 Gateway field.

- If you change any of the network connection parameters, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Network DHCP Client Options

Use the fields on this page to enable and configure vendor class identifier information that the DHCP client on the switch sends to the DHCP server when it requests a lease.

To access this page, click **LAN > Administration > Network DHCP Client Options**.

Figure 17: DHCP Client Options**Table 10: DHCP Client Option Fields**

Field	Description
DHCP Vendor Class ID Mode	Specify whether to enable or disable the vendor class identifier mode.
DHCP Vendor Class ID String	Enter the text to add to DHCP requests as Option-60, which is the Vendor Class Identifier option.

HTTP Configuration

Use the HTTP Configuration page to configure the HTTP server settings on the system.

To access the HTTP Configuration page, click **LAN > Administration > HTTP Configuration** in the navigation menu.

Figure 18: HTTP Configuration

Table 11: HTTP Configuration Fields

Field	Description
HTTP Admin Mode	This select field is used to Enable or Disable the Administrative Mode of HTTP. The currently configured value is shown when the web page is displayed. The default value is Enable. If you disable the HTTP admin mode, access to the web interface is limited to secure HTTP, which is disabled by default.
Java Mode	This select field is used to Enable or Disable the web Java Mode. This applies to both secure and un-secure HTTP connections. The currently configured value is shown when the web page is displayed. The default value is Enable.
HTTP Session Soft Timeout	This field is used to set the inactivity timeout for HTTP sessions. The value must be in the range of (0 to 60) minutes. A value of zero corresponds to an infinite timeout. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.
HTTP Session Hard Timeout	This field is used to set the hard timeout for HTTP sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (0 to 168) hours. A value of zero corresponds to an infinite timeout. The default value is 24 hours. The currently configured value is shown when the web page is displayed.
Maximum Number of HTTP Sessions	This field is used to set the maximum allowable number of HTTP sessions. The value must be in the range of (0 to 16). The default value is 16. The currently configured value is shown when the web page is displayed.

- If you make changes to the page, click **Submit** to apply the changes to the system.

User Accounts

By default, the switch contains two user accounts:

- admin, with 'Read/Write' privileges
- guest, with 'Read Only' privileges

Both of these accounts have blank passwords by default. The names are not case sensitive.

If you log on to the switch with the user account that Read/Write privileges (i.e., as admin), you can use the **User Accounts** page to assign passwords and set security parameters for the default accounts. You can also add up to five read-only accounts. You can delete all accounts except for the Read/Write account.



Note: Only a user with Read/Write privileges may alter data on this screen, and only one account can exist with Read/Write privileges.

To access the User Accounts page, click **LAN > Administration > User Accounts** in the navigation tree.

User Accounts	
User	admin
User Name	admin
Password	<input type="text"/> (8 to 64 Alphanumeric Characters)
Confirm Password	<input type="text"/> (8 to 64 Alphanumeric Characters)
Access Mode	Read/Write
Lockout Status	False
Password Expiration Date	----
SNMP v3 User Configuration	
SNMP v3 Access Mode	Read/Write
Authentication Protocol	None
Encryption Protocol	None
Encryption Key	<input type="text"/> <input type="checkbox"/> Apply
<input type="button" value="Submit"/>	

Figure 19: User Accounts

Table 12: User Accounts Fields

Field	Description
User	From the User menu, select an existing user to configure, or select Create to create a new user account. The system can have a maximum of five 'Read Only' accounts and one Read/Write account.
User Name	Enter the name to give to the account. User names are up to eight characters in length and are not case sensitive. Valid characters include all the alphanumeric characters as well as the dash ('-') and underscore ('_') characters. User name <i>default</i> is not valid. Note: You can change the Read/Write user name from "admin" to something else, but when you click Submit, you must re-authenticate with the new username.
Password	Enter the optional new or changed password for the account. It will not display as it is typed, and only asterisks (*) will show on the screen. Passwords are up to eight alpha numeric characters in length and are case sensitive.
Confirm Password	Enter the password again, to confirm that you entered it correctly. This field will not display, but will show asterisks (*)
Access Mode	Indicates the user's access mode. The admin account always has Read/Write access, and all other accounts have Read Only access.
Lockout Status	Indicates whether the user is currently locked out. A user is locked out after a certain number of failed login attempts.
Password Expiration Date	Indicates the date when this user's current password will expire. This is determined by the date the password was created and the number of days specified in the aging Password Aging setting on the Password Management page.
SNMPv3 User Configuration	
SNMPv3 Access Mode	Indicates the SNMPv3 access privileges for the user account. The admin account always has 'Read/Write' access, and all other accounts have 'Read Only' access.
Authentication Protocol	Specify the SNMPv3 Authentication Protocol setting for the selected user account. The valid Authentication Protocols are None, MD5 or SHA. If you select None, the user will be unable to access the SNMP data from an SNMP browser. If you select MD5 or SHA, the user login password will be used as the SNMPv3 authentication password, and you must therefore specify a password, and it must be eight characters long.
Encryption Protocol	Specify the SNMPv3 Encryption Protocol setting for the selected user account. The valid Encryption Protocols are None or DES. If you select the DES Protocol you must enter a key in the Encryption Key field. If None is specified for the Protocol, the Encryption Key is ignored.
Encryption Key	If you selected DES in the Encryption Protocol field enter the SNMPv3 Encryption Key here. Otherwise this field is ignored. Valid keys are 0 to 15 characters long. The Apply check box must be selected in order to change the Encryption Protocol and Encryption Key.

Adding a User Account

Use the following procedures to add a user account. The system supports one Read/Write user and five Read Only users.

1. From the **User** menu, select **Create**.
The screen refreshes.
2. Enter a username and password for the new user, then re-enter the password in the **Confirm Password** field.
3. Click **Submit** to update the switch with the values on this screen.
If you want the switch to retain the new values across a power cycle, you must perform a save.

Changing User Account Information

You cannot add or delete the Read/Write user, but you can change the username and password. To change the password for an existing account or to overwrite the username on an existing account, use the following procedures.

1. From the **User** menu, select the user to change.
The screen refreshes.
2. To alter the username or, delete the existing name in the **Username** field and enter the new username.
To change the password, delete any asterisks (*) in the **Password** and **Confirm Password** fields, and then enter and confirm the new password.
3. Click **Submit** to update the switch with the values on this screen.
If you want the switch to retain the new values across a power cycle, you must perform a save.

Deleting a User Account

Use the following procedures to delete any of the Read Only user accounts.

1. From the **User** menu, select the user to delete.
The screen refreshes.
2. Click **Delete** to delete the user.
This button is only visible when you have selected a user account with 'Read Only' access. You cannot delete the 'Read/Write' user.
If you want the switch to retain the new values across a power cycle, you must perform a save.

Authentication List Configuration

Use the Authentication List page to configure login lists. A login list specifies one or more authentication methods to validate switch or port access for the users associated with the list.



Note: The preconfigured users, admin and guest, are assigned to a pre-configured list named defaultList, which you cannot delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list

To access the Authentication Profiles page, click **LAN > Administration > Authentication List Configuration** in the navigation tree.

Figure 20: Authentication List Configuration

Table 13: Authentication Profile Fields

Field	Description
Access Mode	Select the access mode to configure, which can be either Login or Enable. A login list or enable list specifies the authentication method(s) you want used to validate switch or port access for the users associated with the list. The pre-configured users, <i>admin</i> and <i>guest</i> , are assigned to a pre-configured list named defaultList, which you may not delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list
Authentication List	Select an existing list to view or configure, or select Create to create and configure a new authentication list.

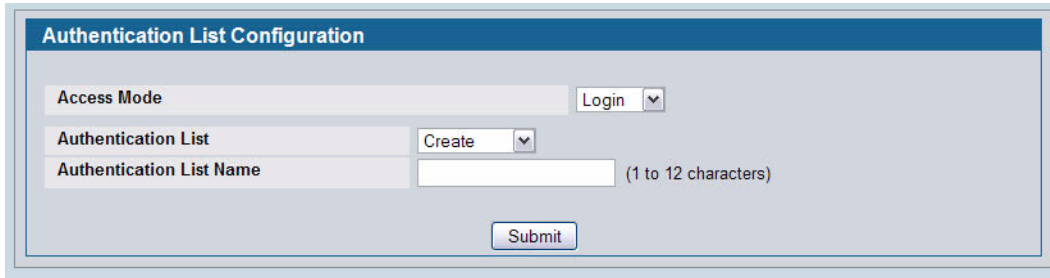
Table 13: Authentication Profile Fields (Cont.)

Field	Description
Method 1	<p>Use the menu to select the method that should appear first in the selected authentication login list. User authentication occurs in the order the methods are selected. Each method can be selected only once. Possible methods are as follows:</p> <ul style="list-style-type: none"> • UNDEFINED: The authentication method is unspecified. This option is not available for Method 1. • ENABLE: Uses the enable password for authentication. • LINE: Uses the Line password for authentication. • LOCAL: The user's locally stored ID and password will be used for authentication. Since the local method does not time out, if you select this option as the first method, no other method will be tried, even if you have specified more than one method. • NONE: No authentication is used. • RADIUS: The user's ID and password will be authenticated using the RADIUS server(s) configured on the LAN > Security > RADIUS > RADIUS Authentication Server Configuration page. If you have multiple RADIUS servers configured, the switch will attempt to contact the primary RADIUS server. If the primary RADIUS server fails, the switch automatically attempts to contact a backup RADIUS server. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch uses Method 2 to authenticate the user. • Tacacs+: The user's ID and password will be authenticated using the TACACS+ server configured on the LAN > Security > TACACS+ > Configuration page. If you select RADIUS or TACACS+ as the first method and an error occurs during the authentication, the switch attempts user authentication Method 2.
Method 2	Use the menu to select the method, if any, that should appear second in the selected authentication login list. This is the method that will be used if the first method times out. If you select a method that does not time out as the second method, the third method will not be tried.
Method 3	Use the menu to select the method, if any, that should appear third in the selected authentication login list.
Method 4	Use the menu to select the method, if any, that should appear fourth in the selected authentication login list.
Method 5	Use the menu to select the method, if any, that should appear fifth in the selected authentication login list.
Method 6	Use the menu to select the method, if any, that should appear sixth in the selected authentication login list.

Creating an Authentication List

To create a new authentication list, use the following procedures.

1. Select **Create** from the **Authentication List** field. The page refreshes, and different fields are available.



2. In the **Authentication List Name** field, enter a name of 1 to 12 characters.
The name is not case sensitive, but it cannot include spaces.
3. Click **Submit** to create the name and display the Method fields for the new list.
You are now ready to configure the authentication list. By default, local is set as the initial authentication method.

To retain the changes across a power cycle, you must perform a save.

Configuring an Authentication List

To modify an authentication list, use the following procedures.

1. Select an existing list from the **Authentication List** menu.
2. From the **Method 1** field, select the initial login method.
3. If desired, select the additional subsequent login method.
4. Click **Submit** to apply the changes to the system.

To retain the changes across a power cycle, you must perform a save.

Deleting an Authentication List

Use the following procedures to remove an authentication login list from the configuration.

1. Select an existing list from the **Authentication List** menu.
2. Click **Delete**.

The delete will fail if the selected login list is assigned to any user (including the default user) for system login or IEEE 802.1X port access control. You can only use this button if you have Read/Write access.

To retain the changes across a power cycle, you must perform a save.

Authentication List Summary

Use the **Authentication List Summary** page to view information about the authentication lists on the system and which users are associated with each list. The page also displays information about 802.1X port security users.

To access the Authentication List Summary page, click **LAN > Monitoring > Authentication List Summary** in the navigation tree.



Authentication List	Method List	Login Users	802.1x Port Security Users
defaultList	local	admin guest default	admin guest default

Figure 21: Login Session

The **Authentication List Summary** page has the following read-only fields:

Table 14: Login Fields

<i>Field</i>	<i>Description</i>
Authentication List	Identifies the name of the authentication login list summarized in this row.
Method List	Shows the order of the login methods configured for the list.
Login Users	Shows the users assigned to this login list on the User Login Configuration screen. This list is used to authenticate the users for system login access.
802.1X Port Security Users	Shows the port access control users assigned to this login list. This list is used to authenticate the users for port access by using the IEEE 802.1X protocol.

- Click **Refresh** to update the information on the screen.
- To assign users to a specific authentication list, see [“User Login” on page 83](#). To configure the 802.1X port security users, see [“Port Access Control” on page 381](#).

Login Session

Use the Login Session page to view information about users who have logged on to the switch.

To access the **Login Session** page, click **LAN > Monitoring > Login Session** in the navigation tree.



ID	User Name	Connection From	Idle Time	Session Time	Session Type
11	admin	10.27.65.93	00:00:00	01:36:01	HTTP

Figure 22: Login Session

The **Login Session** page has the following read-only fields:

Table 15: Login Session Fields

Field	Description
ID	Identifies the ID of this row.
User Name	Shows the user name of the user who is currently logged on to the switch.
Connection From	Shows the IP address of the system from which the user is connected. If the connection is a local serial connection, the Connection From field entry is EIA-232.
Idle Time	Shows the idle session time.
Session Time	Shows the total session time.
Session Type	Shows the type of session, which can be Telnet, Serial Port, HTTP, or SSH.

- Click **Refresh** to update the information on the screen.

User Login

Each configured user is assigned to a login list that specifies how the user should be authenticated when attempting to access the switch or a port on the switch. After creating a new user account on the User Account screen, you can use the User Login page to assign the user to a login list for the switch.

The pre-configured users, admin and guest, are assigned to a pre-configured list named defaultList, which you may not delete. All newly created users are also assigned to the defaultList until you specifically assign them to a different list. To create a new authentication list, see [“Use the Authentication List page to configure login lists. A login list specifies one or more authentication methods to validate switch or port access for the users associated with the list.” on page 78.](#)

To access the User Login page, click **LAN > Administration > User Login** in the navigation tree.

Figure 23: User Login

Table 16: User Login Fields

Field	Description
User	The menu contains all configured users in the system and a Non-Configured user. The Non-configured user is a user who does not have an account configured on the switch. If you assign the Non-configured user to a login list that specifies authentication via the RADIUS server, you will not need to create an account for all users on each switch. However, by default the Non-configured user is assigned to defaultList, which by default uses local authentication.
Authentication List	Select the authentication login list you want to assign to the user for system login.

Assigning a User to an Authentication List

The admin (Read/Write) user is always associated with the default list, which forces the admin user to always be authenticated locally to prevent full lockout from switch configuration. If you assign a user to a login list that requires remote authentication, the user's access to the switch from all CLI, Web, and telnet sessions will be blocked until the authentication is complete. For more information, see the **Max Number of Retransmits** field in [“RADIUS Settings” on page 389](#).

1. Select the user name from the User field's menu, or select Non-configured user to assign all users that are not configured on the switch to an authentication list.

The screen refreshes. The list that the user is currently assigned to is highlighted in the **Authentication List** field.

2. To assign the user to a different list, click the list name in the **Authentication List** field to select the list.
3. Click **Submit** to apply the changes to the switch.

Denial of Service Protection

Use the Denial of Service (DoS) page to configure DoS control. D-Link DWS-4000 Series software provides support for classifying and blocking specific types of DoS attacks. You can configure your system to monitor and block a variety of DoS attacks.

To access the **Denial of Service** page, click **LAN > Administration > Denial of Service Protection** in the navigation menu.

Denial of Service Configuration	
Denial of Service First Fragment	Disable
Denial of Service Min TCP Hdr Size	20 (0 to 255)
Denial of Service ICMP	Disable
Denial of Service Max ICMP Size	512 (0 to 1023)
Denial of Service L4 Port	Disable
Denial of Service SIP=DIP	Disable
Denial of Service TCP Flag	Disable
Denial of Service TCP Fragment	Disable

Figure 24: Denial of Service

Table 17: Denial of Service Configuration Fields

Field	Description
Denial of Service First Fragment	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling First Fragment DoS prevention causes the switch to drop packets that have a TCP header smaller than the configured Min TCP Hdr Size. The factory default is disabled.
Denial of Service Min TCP Hdr Size	Specify the Min TCP Hdr Size allowed. If First Fragment DoS prevention is enabled, the switch will drop packets that have a TCP header smaller than this configured Min TCP Hdr Size. The factory default is disabled.
Denial of Service ICMP	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling ICMP DoS prevention causes the switch to drop ICMP packets that have a type set to ECHO_REQ (ping) and a size greater than the configured ICMP Pkt Size. The factory default is disabled.
Denial of Service Max ICMP Size	Specify the Max ICMP Pkt Size allowed. If ICMP DoS prevention is enabled, the switch will drop ICMP ping packets that have a size greater than this configured Max ICMP Pkt Size. The factory default is disabled.
Denial of Service L4 Port	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling L4 Port DoS prevention causes the switch to drop packets that have TCP/UDP source port equal to TCP/UDP destination port. The factory default is disabled.
Denial of Service SIP=DIP	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling SIP=DIP DoS prevention causes the switch to drop packets that have a source IP address equal to the destination IP address. The factory default is disabled.
Denial of Service TCP Flag	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Flag DoS prevention causes the switch to drop packets that have TCP flag SYN set and TCP source port less than 1024 or TCP control flags set to 0 and TCP sequence number set to 0 or TCP flags FIN, URG, and PSH set and TCP sequence number set to 0 or both TCP flags SYN and FIN set. The factory default is disabled.
Denial of Service TCP Fragment	Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Fragment DoS prevention causes the switch to drop packets that have an IP fragment offset equal to 1. The factory default is disabled.

- If you change any of the DoS settings, click **Submit** to apply the changes to the switch. To preserve the changes across a switch reboot, you must perform a save.

Multiple Port Mirroring

Port mirroring selects the network traffic for analysis by a network analyzer. This is done for specific ports of the switch. As such, many switch ports are configured as source ports and one switch port is configured as a destination port. You have the ability to configure how traffic is mirrored on a source port. Packets that are received on the source port, that are transmitted on a port, or are both received and transmitted, can be mirrored to the destination port.

The packet that is copied to the destination port is in the same format as the original packet on the wire. This means that if the mirror is copying a received packet, the copied packet is VLAN tagged or untagged as it was received on the source port. If the mirror is copying a transmitted packet, the copied packet is VLAN tagged or untagged as it is being transmitted on the source port.

Use the Multiple Port Mirroring page to define port mirroring sessions.

To access the Multiple Port Mirroring page, click **LAN > Administration > Multiple Port Mirroring** in the navigation menu.

Figure 25: Multiple Port Mirroring

Table 18: Multiple Port Mirroring Fields

Field	Description
Session	Specifies the monitoring session.
Mode	Enables you to turn on or off Multiple Port Mirroring. The default is Disabled (off).
Source Port	Lists the source ports that have been added from the Add Source Port page.
Destination Port	Select the port to which port traffic may be copied.

Adding a Port Mirroring Session



Note: A Port will be removed from a VLAN or LAG when it becomes a destination mirror.

1. From the **LAN > Administration > Multiple Port Mirroring** page, click **Add Source Port** to display the **Add Source Port** page.

Figure 26: Multiple Port Mirroring—Add Source Ports

2. Configure the following fields:

Table 19: Multiple Port Mirroring—Add Source Fields

Field	Description
Session	Specifies the monitoring session.
Source Port	Select the unit and port from which traffic is mirrored. Up to eight source ports can be mirrored to a destination port.
Direction	Select the type traffic monitored on the source port, which can be one of the following: <ul style="list-style-type: none"> • Tx: Monitors transmitted packets only. • Rx: Monitors received packets only. • Tx and Rx: Monitors transmitted and received packets.

3. Click **Add** to apply the changes to the system.

The new port mirroring session is enabled for the unit and port, and the device is updated. The source port appears in the Source Port list on the Multiple Port Mirroring page.

Removing or Modifying a Port Mirroring Session

1. From the Port Mirroring page, click **Remove Source Port**.
2. Select one or more source ports to remove from the session.
Use the CTRL key to select multiple ports to remove.
3. Click **Remove**.

The source ports are removed from the port mirroring session, and the device is updated.

Telnet Sessions

Telnet is a terminal emulation TCP/IP protocol. ASCII terminals can be virtually connected to the local device through a TCP/IP protocol network. Telnet is an alternative to a local login terminal where a remote login is required.

The switch supports up to five simultaneous telnet sessions. All CLI commands can be used over a telnet session.

The Telnet Session Configuration page allows you to control inbound telnet settings on the switch. Inbound telnet sessions originate on a remote system and allow a user on that system to connect to the switch CLI. To configure outbound telnet settings, which are telnet sessions that originate on the switch to access a remote system, see [“Outbound Telnet Client Configuration” on page 90](#).

To display the Telnet Session Configuration page, click **LAN > Administration > Telnet Session** in the navigation tree.



Telnet Session Configuration	
Telnet Session Timeout (minutes)	<input type="text" value="5"/> (1 to 160)
Maximum Number of Telnet Sessions	<input type="text" value="5"/>
Allow New Telnet Sessions	<input type="text" value="Yes"/>
Telnet Server Admin Mode	<input type="text" value="Enable"/>

Figure 27: Telnet Session Configuration

Table 20: Telnet Session Configuration Fields

Field	Description
Telnet Session Timeout (minutes)	Specify how many minutes of inactivity should occur on a telnet session before the session is logged off. You may enter any number from 1 to 160. The factory default is 5. Note: When you change the timeout value, the new value is applied to all active and inactive sessions immediately. Any sessions that have been idle longer than the new timeout value are disconnected immediately.
Maximum Number of Telnet Sessions	From the drop-down menu, select how many simultaneous telnet sessions to allow. The maximum is 5, which is also the factory default. A value of 0 indicates that no outbound Telnet session can be established.
Allow New Telnet Sessions	Controls whether to allow new telnet sessions: <ul style="list-style-type: none"> • Yes: Permits new telnet sessions until the maximum number allowed is reached. • No: New telnet sessions will not be allowed, but existing sessions are not disconnected.
Telnet Server Admin Mode	Administrative mode for inbound telnet sessions. Setting this value to disable shuts down the telnet port. If the admin mode is set to disable, then all existing telnet connections are disconnected. The default value is Enable.

- If you change any of the telnet parameters, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Outbound Telnet Client Configuration

The outbound telnet feature is not available on all platforms.

Use the outbound telnet client settings to control the telnet sessions that originate from the switch and connect to a remote system.

To access the Outbound Telnet Client Configuration page, click **LAN > Administration > Outbound Telnet Client Configuration** in the navigation menu.

Figure 28: Outbound Telnet

Table 21: Outbound Telnet Fields

Field	Description
Admin Mode	Specifies whether the Outbound Telnet service is Enabled or Disabled. The default value is Enabled. <ul style="list-style-type: none"> • Enable: Users can initiate outbound telnet sessions from the switch CLI. • Disable: No outbound telnet sessions can originate from the switch.
Maximum Sessions	Specifies the maximum number of Outbound Telnet Sessions allowed. The default value is 5. The valid range is 0 to 5 sessions.
Session Timeout	Specifies the Outbound Telnet login inactivity timeout. The default value is 5. The valid range is 1 to 160 minutes.

- If you change any data, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a save.

Ping Test

Use the Ping page to tell the switch to send a Ping request to a specified IP address. You can use this feature to check whether the switch can communicate with a particular network host.

To access the Ping page, click **LAN > Administration > Ping Test** in the navigation menu.

Figure 29: Ping

Table 22: Ping Fields

Field	Description
Hostname/IP Address	Enter the IP address or the host name of the station you want the switch to ping. The initial value is blank. This information is not retained across a power cycle.
Count	Specify the number of pings to send.
Interval	Specify the number of seconds between pings sent.
Size	Specify the size of the ping packet to send.
Ping	Displays the results of the ping.

- Click **Submit** to send the ping. If successful, the results display as shown in [Figure 30](#).

TraceRoute

You can use the TraceRoute utility to discover the paths that a packet takes to a remote destination.

To display this page, click **LAN > Administration > TraceRoute** in the navigation tree.

Figure 30: TraceRoute

Table 23: TraceRoute Fields

	<i>Definition</i>
Hostname/IP Address	Enter the IP address or the hostname of the station you want the switch to discover path for.
Probes Per Hop	Enter the number of times each hop should be probed.
MaxTTL	Enter the maximum time-to-live for a packet in number of hops.
InitTTL	Enter the initial time-to-live for a packet in number of hops.
MaxFail	Enter the maximum number of failures allowed in the session.
Interval	Enter the time between probes in seconds.
Port	Enter the UDP destination port in probe packets.
Size	Enter the size of probe packets.
TraceRoute	Displays the output from a traceroute.

- Click **Submit** to initiate the traceroute. The results display in the TraceRoute box.

Configuring SNTP Settings

D-Link DWS-4000 Series switch software supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. D-Link DWS-4000 Series software operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by Stratum. Stratum defines the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above since it is itself a stratum 2 device.

The following is an example of stratum:

- **Stratum 0:** A real time clock is used as the time source, for example, a GPS system.
- **Stratum 1:** A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2:** The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the time level and server type.

SNTP time definitions are assessed and determined by the following time levels:

- **T1:** Time at which the original request was sent by the client.
- **T2:** Time at which the original request was received by the server.
- **T3:** Time at which the server sent a reply.
- **T4:** Time at which the client received the server's reply.

The device can poll Unicast and Broadcast server types for the server time.

Polling for Unicast information is used for polling a server for which the IP address is known. SNTP servers that have been configured on the device are the only ones that are polled for synchronization information. T1 through T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the SNTP Server Configuration page.

Broadcast information is used when the server IP address is unknown. When a Broadcast message is sent from an SNTP server, the SNTP client listens to the message. If Broadcast polling is enabled, any synchronization information is accepted, even if it has not been requested by the device. This is the least secure method.

The device retrieves synchronization information, either by actively requesting information or at every poll interval. If Unicast and Broadcast polling are enabled, the information is retrieved in this order:

- Information from servers defined on the device is preferred. If Unicast polling is not enabled or if no servers are defined on the device, the device accepts time information from any SNTP server that responds.
- If more than one Unicast device responds, synchronization information is preferred from the device with the lowest stratum.
- If the servers have the same stratum, synchronization information is accepted from the SNTP server that responded first.

MD5 (Message Digest 5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

SNTP Settings

Use the SNTP Global Configuration page to view and adjust SNTP parameters.

To display the SNTP Global Configuration page, click **LAN > Administration > SNTP > SNTP Settings** in the navigation menu.

SNTP Global Configuration	
Client Mode	Disable
Port	123 (1 to 65535)
Unicast Poll Interval	6 (6 to 10 secs)
Broadcast Poll Interval	6 (6 to 10 secs)
Unicast Poll Timeout	5 (1 to 30 secs)
Unicast Poll Retry	1 (0 to 10)
Submit	

Figure 31: SNTP Global Configuration

Table 24: SNTP Global Configuration Fields

Field	Description
Client Mode	Use drop-down list specify the SNTP client mode, which is one of the following modes: <ul style="list-style-type: none"> • Disable: SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed. • Unicast: SNTP operates in a point to point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally the round-trip delay and local clock offset relative to the server. • Broadcast: SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has Internet wide scope.
Port	Specifies the local UDP port to listen for responses/broadcasts. Allowed range is (1 to 65535). Default value is 123.
Unicast Poll Interval	Specifies the number of seconds between unicast poll requests expressed as a power of two when configured in unicast mode. Allowed range is (6 to 10). Default value is 6.
Broadcast Poll Interval	Specifies the number of seconds between broadcast poll requests expressed as a power of two when configured in broadcast mode. Broadcasts received prior to the expiry of this interval are discarded. Allowed range is (6 to 10). Default value is 6.

Table 24: SNTP Global Configuration Fields (Cont.)

Field	Description
Unicast Poll Timeout	Specifies the number of seconds to wait for an SNTP response when configured in unicast mode. Allowed range is (1 to 30). Default value is 5.
Unicast Poll Retry	Specifies the number of times to retry a request to an SNTP server after the first time-out before attempting to use the next configured server when configured in unicast mode. Allowed range is (0 to 10). Default value is 1.

- If you change any of the settings on the page, click **Submit** to apply the changes to system.

SNTP Server Configuration

Use the SNTP Server Configuration page to view and modify information for adding and modifying Simple Network Time Protocol SNTP servers.

To display the SNTP Server Configuration page, click **LAN > Administration > SNTP > SNTP Server Configuration** in the navigation tree.

The screenshot shows a web form titled "SNTP Server Configuration". It contains the following fields and values:

- Server:** 10.27.65.162 (dropdown menu)
- Address Type:** IPv4 (dropdown menu)
- Port:** 123 (text input, range 1 to 65535)
- Priority:** 1 (text input, range 1 to 3)
- Version:** 4 (text input, range 1 to 4)

At the bottom of the form are two buttons: "Submit" and "Delete".

Figure 32: SNTP Server Configuration**Table 25: SNTP Server Configuration Fields**

Field	Description
Server	Select the IP address of a user-defined SNTP server to view or modify information about an SNTP server, or select Create to configure a new SNTP server. You can define up to three SNTP servers.
Address / Hostname	Enter the IP address or the hostname of the SNTP server.
Address Type	Select IPv4 if you entered an IPv4 address or DNS if you entered a hostname.
Port	Enter a port number from 1 to 65535. The default is 123.
Priority	Specifies the priority of this server entry in determining the sequence of servers to which SNTP requests are sent. Values are 1 to 3, and the default is 1. Servers with lowest numbers have priority
Version	Enter the protocol version number. Values are 1 to 4, and the default is 4.

- To add an SNTP server, select **Create** from the **Server** list, complete the remaining fields as desired, and click **Submit**. The SNTP server is added, and is now reflected in the Server list. You must perform a save to retain your changes over a power cycle.
- To removing an SNTP server, select the IP address of the server to remove from the **Server** list, and then click **Delete**. The entry is removed, and the device is updated.

SNTP Server Status

The SNTP Server Status page displays status information about the SNTP servers configured on your switch.

To access the SNTP Server Status page, click **LAN > Monitoring > SNTP Summary > Server Status** in the navigation menu.

SNTP Server Status	
Address	10.27.65.162
Last Update Time	
Last Attempt Time	JAN 01 00:00:00 1970
Last Attempt Status	Other
Unicast Server Num Requests	0
Unicast Server Num Failed Requests	0
Refresh	

Figure 33: SNTP Server Status

Table 26: SNTP Server Status Fields

Field	Description
Address	Specifies all the existing Server Addresses. If no Server configuration exists, a message saying "No SNTP server exists" flashes on the screen.
Last Update Time	Specifies the local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	Specifies the local date and time (UTC) that this SNTP server was last queried.

Table 26: SNTP Server Status Fields (Cont.)

Field	Description
Last Attempt Status	<p>Specifies the status of the last SNTP request to this server. If no packet has been received from this server, a status of Other is displayed:</p> <ul style="list-style-type: none"> • Other: None of the following enumeration values. • Success: The SNTP operation was successful and the system time was updated. • Request Timed Out: A directed SNTP request timed out without receiving a response from the SNTP server. • Bad Date Encoded: The time provided by the SNTP server is not valid. • Version Not Supported: The SNTP version supported by the server is not compatible with the version supported by the client. • Server Unsynchronized: The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • Server Kiss Of Death: The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Unicast Server Num Requests	Specifies the number of SNTP requests made to this server since last agent reboot.
Unicast Server Num Failed Requests	Specifies the number of failed SNTP requests made to this server since last reboot.

- Click **Refresh** to display the latest information from the router.

SNTP Global Status

Use the SNTP Global Status page to view information about the system's SNTP client.

To access the SNTP Global Status page, click **LAN > Monitoring > SNTP Summary > Global Status** in the navigation menu.

SNTP Global Status	
Version	4
Supported Mode	Unicast and Broadcast
Last Update Time	JAN 01 00:00:00 1970
Last Attempt Time	JAN 01 00:00:00 1970
Last Attempt Status	Other
Server IP Address	
Address Type	Unknown
Server Stratum	0 - Unspecified
Reference Clock Id	
Server Mode	Reserved
Unicast Server Max Entries	3
Unicast Server Current Entries	0
Broadcast Count	0

Figure 34: Global Status

Table 27: Global Status Fields

Field	Description
Version	Specifies the SNTP Version the client supports.
Supported Mode	Specifies the SNTP modes the client supports. Multiple modes may be supported by a client.
Last Update Time	Specifies the local date and time (UTC) the SNTP client last updated the system clock.
Last Attempt Time	Specifies the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.
Last Attempt Status	Specifies the status of the last SNTP request or unsolicited message for both unicast and broadcast modes. If no message has been received from a server, a status of Other is displayed. These values are appropriate for all operational modes: <ul style="list-style-type: none"> • Other: None of the following enumeration values. • Success: The SNTP operation was successful and the system time was updated. • Request Timed Out: A directed SNTP request timed out without receiving a response from the SNTP server. • Bad Date Encoded: The time provided by the SNTP server is not valid. • Version Not Supported: The SNTP version supported by the server is not compatible with the version supported by the client. • Server Unsynchronized: The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • Server Kiss Of Death: The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Server IP Address	Specifies the IP address of the server for the last received valid packet. If no message has been received from any server, an empty string is shown.

Table 27: Global Status Fields (Cont.)

Field	Description
Address Type	Specifies the address type of the SNTP Server address for the last received valid packet.
Server Stratum	Specifies the claimed stratum of the server for the last received valid packet.
Reference Clock Id	Specifies the reference clock identifier of the server for the last received valid packet.
Server Mode	Specifies the mode of the server for the last received valid packet.
Unicast Sever Max Entries	Specifies the maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	Specifies the number of current valid unicast server entries configured for this client.
Broadcast Count	Specifies the number of unsolicited broadcast SNTP messages that have been received and processed by the SNTP client since last reboot.

- Click **Refresh** to display the latest information from the router.

Time Zone Configuration

Use the Time Zone Configuration page to configure the time zone difference from Coordinated Universal Time (UTC).

To display the Time Zone Configuration page, click **LAN > Administration > SNTP > Time Zone Configuration** in the navigation menu.

Figure 35: Time Zone Configuration**Table 28: Time Zone Configuration Fields**

Field	Description
Hours-offset	Set the hours difference from UTC. (Range: -12 to +13)
Minutes-offset	Set the minutes difference from UTC. (Range: 0–59)
Zone	Set the acronym of the time zone. (Range: 0–4 characters)

- If you change any of the settings on the page, click **Submit** to apply the changes to system.

Summer Time Configuration

Use the Summer Time Configuration page to specify a defined summer time duration and offset.

To display the Summer Time Configuration page, click **LAN > Administration > SNTP > Summer Time Configuration** in the navigation menu.

Figure 36: Summer Time Configuration

Table 29: Summer Time Configuration Fields

Field	Description
Summertime	Enable or disable summer time mode.
Recurring	Select the check box to indicate that the configuration is to be repeated every year.
Location	This field displays only when the Recurring check box is selected. The summer time configuration is predefined for the United States and European Union. To set the summer time for a location other than the USA or EU, select None.
Start Month	Select the starting month.
Start Date	Select the starting date. This field displays only when the Recurring check box is cleared.
Start Year	Select the starting year. This field displays only when the Recurring check box is cleared.
Start Time	Select the starting time in hh:mm format.
End Month	Select the ending month.
End Date	Select the ending date. This field displays only when the Recurring check box is cleared.
End Year	Select the ending year. This field displays only when the Recurring check box is cleared.
End Time	Select the ending time in hh:mm format.
Offset	Set the number of minutes to add during summer time in the range 0 to 1440.
Zone	Set the acronym of the time zone to be displayed when summer time is in effect. The range is 0 to 4 characters.

If you change any of the settings on the page, click **Submit** to apply the changes to system.

Summer Time Recurring Configuration

Clicking the Recurring check box indicates that the configuration is to be repeated every year. When you select Recurring, the fields shown in the following table occur.

Summer Time Configuration	
Summertime	Enable ▾
Recurring	<input checked="" type="checkbox"/>
Location	USA ▾
Start Week	1 ▾
Start Day	Sun ▾
Start Month	Jan ▾
Start Time(hh:mm)	0 ▾ : 0 ▾
End Week	1 ▾
End Day	Sun ▾
End Month	Jan ▾
End Time(hh:mm)	0 ▾ : 0 ▾
Offset (0 - 1440)	0
Zone (0 - 4 characters)	EST
<input type="button" value="Submit"/> <input type="button" value="Refresh"/>	

Figure 37: Summer Time Recurring Configuration

Table 30: Summer Time Recurring Configuration Fields

Field	Description
Summertime	Enable or disable summer time mode.
Recurring	Select the check box to indicate that the configuration is to be repeated every year.
Location	This field displays only when the Recurring check box is selected. The summer time configuration is predefined for the United States and European Union. To set the summer time for a location other than the USA or EU, select None.
Offset	Set the number of minutes to add during summer time in the range 0 to 1440.
Zone	Set the acronym of the time zone to be displayed when summer time is in effect. The range is 0 to 4 characters.

Clock Detail

Use the Clock Detail page to view information about the current time, time zone, and summer time settings.

To display the Clock Detail page, click **LAN > Monitoring > Clock Detail** in the navigation menu. The following figure shows the Clock Detail page when Summertime is enabled.



Clock Detail	
Current Time	
Time(hh:mm)	05:21:46
Zone	(UTC + 0.00)
Date	1 Jan 1970
Time Source	No time source
Time Zone	
Zone	Acronym not configured
Offset	UTC + 0.00
Summertime	
Recurring	No
Start Date	1 Jan 2000
Start Time(hh:mm)	00:00
End Date	1 Jan 2000
End Time(hh:mm)	00:00
Offset	0
Zone	Acronym not configured

Refresh

Figure 38: Clock Detail

Table 31: Clock Detail

Field	Description
Current Time	This section displays the current time.
Time Zone	This section displays the time zone settings.
Summertime	This section displays the summer time settings.

- Click **Refresh** to update the page with the most current information.

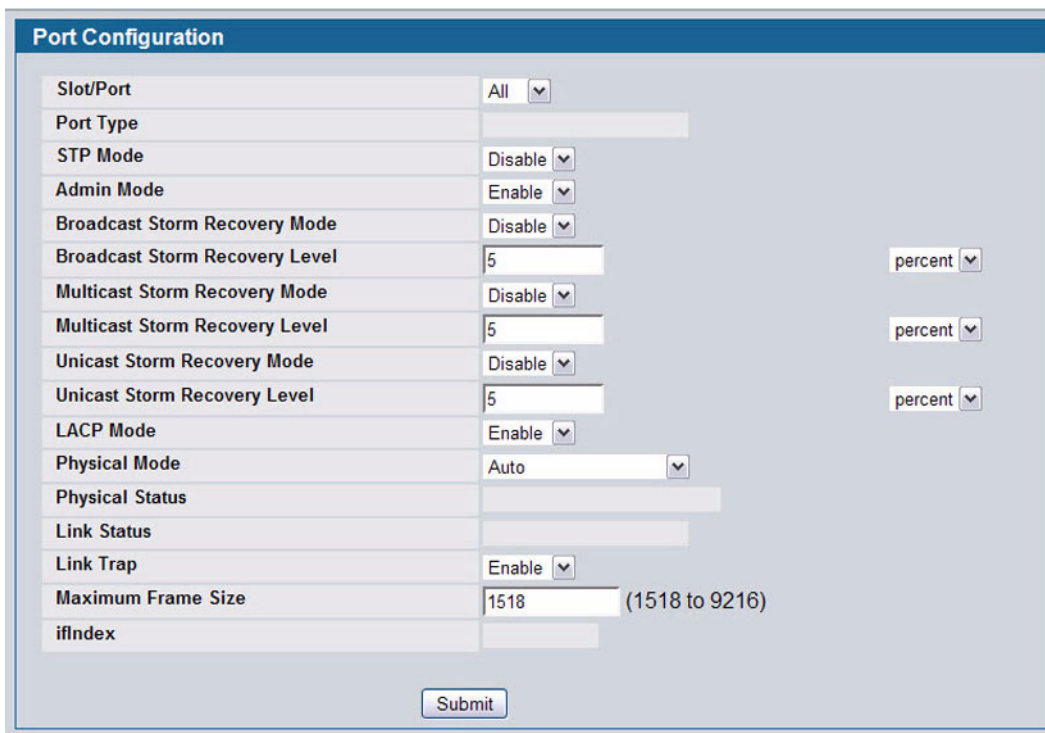
Configuring and Viewing Device Port Information

The pages in the Port folder allow you to view and monitor the physical port information for the ports available on the switch.

Port Configuration

Use the Port Configuration page to configure the physical interfaces on the switch.

To access the Port Configuration page, click **LAN > Administration > Port Configuration > Port Configuration** in the navigation tree.



The screenshot displays the 'Port Configuration' web interface. It features a table of configuration options for a port. The 'Slot/Port' is set to 'All'. Other settings include STP Mode (Disable), Admin Mode (Enable), Broadcast Storm Recovery Mode (Disable), Broadcast Storm Recovery Level (5 percent), Multicast Storm Recovery Mode (Disable), Multicast Storm Recovery Level (5 percent), Unicast Storm Recovery Mode (Disable), Unicast Storm Recovery Level (5 percent), LACP Mode (Enable), Physical Mode (Auto), Physical Status, Link Status, Link Trap (Enable), and Maximum Frame Size (1518). A 'Submit' button is located at the bottom of the form.

Configuration Item	Value
Slot/Port	All
Port Type	
STP Mode	Disable
Admin Mode	Enable
Broadcast Storm Recovery Mode	Disable
Broadcast Storm Recovery Level	5 percent
Multicast Storm Recovery Mode	Disable
Multicast Storm Recovery Level	5 percent
Unicast Storm Recovery Mode	Disable
Unicast Storm Recovery Level	5 percent
LACP Mode	Enable
Physical Mode	Auto
Physical Status	
Link Status	
Link Trap	Enable
Maximum Frame Size	1518 (1518 to 9216)
ifIndex	

Figure 39: Port Configuration

Table 32: Port Configuration Fields

Field	Description
Slot/Port	Select the port from the menu to display or configure data for that port. If you select All , the changes you make to the Port Configuration page apply to all physical ports on the system.
Port Type	For most ports this field is blank. Otherwise the possible values are: <ul style="list-style-type: none"> • Mirrored: Indicates that the port has been configured as a monitoring port and is the source port in a port mirroring session. • Probe: Indicates that the port has been configured as a monitoring port and is the destination port in a port mirroring session. • Port Channel: Indicates that the port has been configured as a member of a port-channel, which is also known as a link Aggregation Group (LAG). For more information about port monitoring and probe ports, see “Multiple Port Mirroring” on page 86 . For information about configuring port channels, see “Creating Port Channels (Trunking)” on page 204 .
STP Mode	Shows the Spanning Tree Protocol (STP) Administrative Mode for the port or LAG. For more information about STP, see “Configuring Spanning Tree Protocol” on page 238 . The possible values for this field are: <ul style="list-style-type: none"> • Enable: Enables the Spanning Tree Protocol for this port. • Disable: Disables the Spanning Tree Protocol for this port.
Admin Mode	Use the pulldown menu to select the port control administration state, which can be one of the following: <ul style="list-style-type: none"> • Enable: The port can participate in the network (default). • Disable: The port is administratively down and does not participate in the network.
Broadcast Storm Recovery Mode	Enable or disable this option by selecting one of the following options on the pulldown entry field: <ul style="list-style-type: none"> • Enable: When the broadcast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. • Disable: The port does not block broadcast traffic if traffic on the port exceeds the configured threshold. The factory default is disabled.
Broadcast Storm Recovery Level	Specify the data rate at which storm control activates. The value is a percentage of port speed and ranges from 0-100. The factory default is 5 percent of port speed.
Multicast Storm Recovery Mode	Enable or disable this option by selecting one of the following options on the pulldown entry field: <ul style="list-style-type: none"> • Enable: When the multicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. • Disable: The port does not block multicast traffic if traffic on the port exceeds the configured threshold. The factory default is disabled.
Multicast Storm Recovery Level	Specify the data rate at which storm control activates. The value is a percentage of port speed and ranges from 0-100. The factory default is 5 percent of port speed.

Table 32: Port Configuration Fields (Cont.)

Field	Description
Unicast Storm Recovery Mode	Enable or disable this option by selecting one of the following options on the pulldown entry field: <ul style="list-style-type: none"> • Enable: When the unicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. • Disable: The port does not block unicast traffic if the unicast traffic on the port exceeds the configured threshold. The factory default is disabled.
Unicast Storm Recovery Level	Specify the data rate at which storm control activates. The value is a percentage of port speed and ranges from 0-100. The factory default is 5 percent of port speed.
LACP Mode	Selects the Link Aggregation Control Protocol administration state: <ul style="list-style-type: none"> • Enable: Specifies that the port is allowed to participate in a port channel (LAG), which is the default mode. • Disable: Specifies that the port cannot participate in a port channel (LAG).
Physical Mode	Use the pulldown menu to select the port's speed and duplex mode. If the Slot/Port field is set to All and you apply a physical mode other than Auto , the mode is applied to all applicable interfaces only: <ul style="list-style-type: none"> • Auto: The duplex mode and speed will be set by the auto-negotiation process. The port's maximum capability (full duplex and 100 Mbps) will be advertised. • <Speed> Half Duplex: The port speeds available from the menu depend on the platform on which the D-Link DWS-4000 Series software is running and which port you select. In half-duplex mode, the transmissions are one-way. In other words, the port does not send and receive traffic at the same time. • <Speed> Full Duplex: The port speeds available from the menu depend on the platform on which the D-Link DWS-4000 Series software is running and which port you select. In half-duplex mode, the transmissions are two-way. In other words, the port can send and receive traffic at the same time.
Physical Status	Indicates the port speed and duplex mode.
Link Status	Indicates whether the Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled: <ul style="list-style-type: none"> • Enable: Specifies that the system sends a trap when the link status changes. • Disable: Specifies that the system does not send a trap when the link status changes.
Maximum Frame Size	Indicates the maximum Ethernet frame size the interface supports or is configured to support. The frame size includes the Ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.
ifIndex	The ifIndex of the interface table entry associated with this port. If the Slot/Port field is set to All , this field is blank.

- If you make any changes to the page, click **Submit** to apply the changes to the system.

Port Summary

Use the **Port Summary** page to view the settings for all physical ports on the platform.

To access the **Port Summary** page, click **LAN > Monitoring > Port Utilization** in the navigation menu.

The table on the **Port Summary** page does not fit on one screen. Use the scroll bar at the bottom of the browser to view all the columns on the page. [Figure 40](#) shows the first six rows of all the columns on the page. Although the table is split into three separate images in the figure, the columns are continue horizontally across the page.

Port Summary					
MST ID : CST					
Slot/Port	Port Type	STP Mode	Forwarding State	Port Role	Media Type
0/1		Disabled	Manual forwarding	Disabled	1000Base-T
0/2		Disabled	Disabled	Disabled	100Base-TX
0/3		Disabled	Disabled	Disabled	100Base-TX
0/4		Disabled	Disabled	Disabled	100Base-TX
0/5		Disabled	Manual forwarding	Disabled	1000Base-T

Figure 40: Port Summary

Table 33: Port Summary Fields

Field	Description
MST ID	If Spanning Tree Protocol is enabled on the switch, you can select the Multiple Spanning Tree instance ID from the list of all currently configured MST ID's to determine the values displayed for the Spanning Tree parameters. Changing the selected MST ID will generate a screen refresh. If STP is disabled, which is the default, the MST ID field shows the static value "CST" instead of a menu.
Slot/Port	Identifies the port that the information in the rest of the row is associated with.
Port Type	For most ports this field is blank. Otherwise, the possible values are: <ul style="list-style-type: none"> • Mirrored: Indicates that the port has been configured as a monitoring port and is the source port in a port mirroring session. • Probe: Indicates that the port has been configured as a monitoring port and is the destination port in a port mirroring session. For more information about port monitoring and probe ports, see "Multiple Port Mirroring" on page 86. • Port Channel: Indicates that the port has been configured as a member of a port-channel, which is also known as a link Aggregation Group (LAG). For information about configuring port channels, see "Creating Port Channels (Trunking)" on page 204.
STP Mode	Shows the Spanning Tree Protocol (STP) Administrative Mode for the port or LAG, which can be Enabled or Disabled . For more information about STP, see "Configuring Spanning Tree Protocol" on page 238 .

Table 33: Port Summary Fields (Cont.)

Field	Description
Forwarding State	<p>The port's current state Spanning Tree state. This state controls what action a port takes on receipt of a frame. If the bridge detects a malfunctioning port it will place that port into the broken state. The other five states are defined in IEEE 802.1D:</p> <ul style="list-style-type: none"> • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Port Role	<p>Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port, or Disabled Port.</p>
Media Type	The Port Media Type.
ARP Type	The ARP Type of the port.
Admin Mode	<p>Shows the port control administration state, which can be one of the following:</p> <ul style="list-style-type: none"> • Enabled: The port can participate in the network (default). • Disabled: The port is administratively down and does not participate in the network.
Bcast Storm Mode	<p>Shows whether the Broadcast Storm Recovery Mode, which can be one of the following:</p> <ul style="list-style-type: none"> • Enabled: When the broadcast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. • Disabled: The port does not block broadcast traffic if traffic on the port exceeds the configured threshold. The factory default is disabled.
Bcast Storm Level	Shows the Broadcast Storm Recovery Level, which is the data rate at which storm control activates. The value is a percentage of port speed and ranges from 0-100. The factory default is 5 percent of port speed.
Mcast Storm Mode	<p>Shows the Multicast Storm Recovery Mode, which is one of the following:</p> <ul style="list-style-type: none"> • Enabled: When the multicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. • Disabled: The port does not block multicast traffic if traffic on the port exceeds the configured threshold. The factory default is disabled.
Mcast Storm Level	Shows the Multicast Storm Recovery Level, which is the data rate at which storm control activates. The value is a percentage of port speed and ranges from 0-100. The factory default is 5 percent of port speed.
Ucast Storm Mode	<p>Shows the Unicast Storm Recovery Mode, which can be one of the following:</p> <ul style="list-style-type: none"> • Enabled: When the unicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. • Disabled: The port does not block unicast traffic if the unicast traffic on the port exceeds the configured threshold. The factory default is disabled.

Table 33: Port Summary Fields (Cont.)

Field	Description
Ucast Storm Level	Shows the Unicast Storm Recovery Level , which is the data rate at which storm control activates. The value is a percentage of port speed and ranges from 0-100. The factory default is 5 percent of port speed.
LACP Mode	Indicates the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation. This field can have the following values: <ul style="list-style-type: none"> • Enable: Specifies that the port is allowed to participate in a port channel (LAG), which is the default mode. • Disable: Specifies that the port cannot participate in a port channel (LAG).
Physical Mode	Shows the speed and duplex mode at which the port is configured: <ul style="list-style-type: none"> • Auto: The duplex mode and speed will be set by the auto-negotiation process. The port's maximum capability (full duplex and 100 Mbps) will be advertised. • <Speed> Half Duplex: The port speeds available from the menu depend on the platform on which the D-Link DWS-4000 Series software is running and which port you select. In half-duplex mode, the transmissions are one-way. In other words, the port does not send and receive traffic at the same time. • <Speed> Full Duplex: The port speeds available from the menu depend on the platform on which the D-Link DWS-4000 Series software is running and which port you select. In half-duplex mode, the transmissions are two-way. In other words, the port can send and receive traffic at the same time.
Physical Status	Indicates the port speed and duplex mode at which the port is operating.
Link Status	Indicates whether the Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled. <ul style="list-style-type: none"> • Enable: Specifies that the system sends a trap when the link status changes. • Disable: Specifies that the system does not send a trap when the link status changes.

- Click **Refresh** to display the most current information from the router.

Port Description

Use the Port Description page to configure a human-readable description of the port.

To access the Port Description page, click **LAN > Administration > Port Configuration > Port Description** in the navigation tree.

Slot/Port	Physical Address	PortList Bit Offset	ifIndex	Port Description
0/1	00:17:9A:95:00:62	1	1	
0/2	00:17:9A:95:00:62	2	2	
0/3	00:17:9A:95:00:62	3	3	
0/4	00:17:9A:95:00:62	4	4	
0/5	00:17:9A:95:00:62	5	5	

Figure 41: Port Description

Table 34: Port Description Fields

Field	Description
Slot/Port	Select the interface for which data is to be displayed or configured.
Port Description	Enter text to describe a port. It can be up to 64 characters in length. The description can contain spaces and non-alphanumeric characters.
Slot/Port	Identifies the port.
Physical Address	Displays the physical address of the specified interface.
PortList Bit Offset	Displays the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.
IfIndex	Displays the interface index associated with the port.
Port Description	Shows the configured port description. By default, the port does not have an associated description.

- If you change a port description, click **Submit** to apply the change to the system.
- Click **Refresh** to display the page with the latest information from the router.

Managing and Viewing Logs

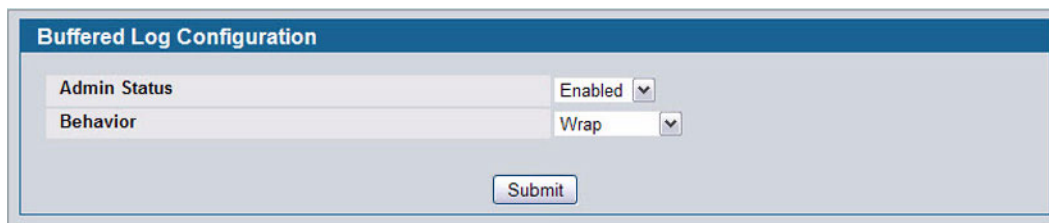
The switch may generate messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored both locally on the platform and forwarded to one or more centralized points of collection for monitoring purposes as well as long term archival storage. Local and remote configuration of the logging capability includes filtering of messages logged or forwarded based on severity and generating component.

The *in-memory* log stores messages in memory based upon the settings for message component and severity.

Buffered Log Configuration

The buffered log stores messages in memory based upon the settings for message component and severity. Use the Buffered Log Configuration page to set the administrative status and behavior of logs in the system buffer.

To access the Buffered Log Configuration page, click **LAN > Administration > Log > Buffered Log Configuration** in the navigation tree.



Buffered Log Configuration	
Admin Status	Enabled ▾
Behavior	Wrap ▾
<input type="button" value="Submit"/>	

Figure 42: Buffered Log Configuration

- If you change the buffered log settings, click **Submit** to apply the changes to the system. To preserve the changes after a system reboot, you must perform a save.

Viewing Buffered Log Messages

Use the **Buffered Log** page to view the log messages in the system buffer. The newest messages are displayed at the bottom of the page.

To access the **Buffered Log** page, click **LAN > Monitoring > Log > Buffered Log** in the navigation menu.

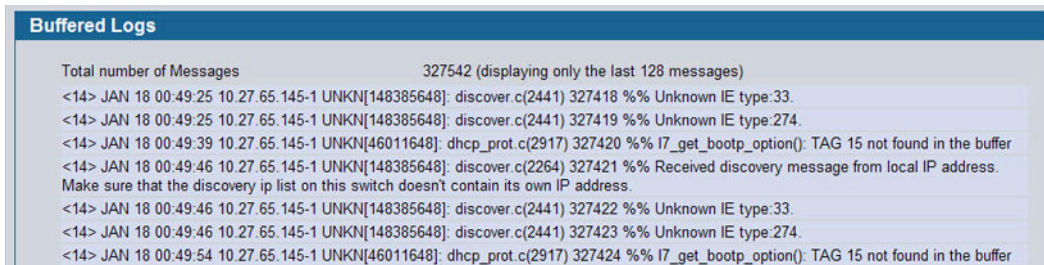


Figure 43: Buffered Log

Table 35: Buffered Log Fields

Field	Description
Total Number of Messages	Shows the number of buffered messages the system has logged. Only the 128 most recent entries are displayed on the page.

The rest of the page displays the buffered log messages. The following example shows a log message:

```
<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry
```

This log message has a severity level of 7 (15 mod 8), which is a debug message. The system is not stacked (STK0). The message was generated by the MSTP component running in thread ID 2110. The message was generated on August 24 05:34:05 by line 318 of file mspt_api.c. This is the 237th message logged.

- Click **Refresh** to update the page with the latest messages.

Command Logger Configuration

Use the Command Logger Configuration page to enable the system to log all CLI commands issued on the system. The command log messages are interleaved with the other system logs messages.

To access the Command Logger Configuration page, click **LAN > Administration > Log > Command Logger Configuration** in the navigation menu.

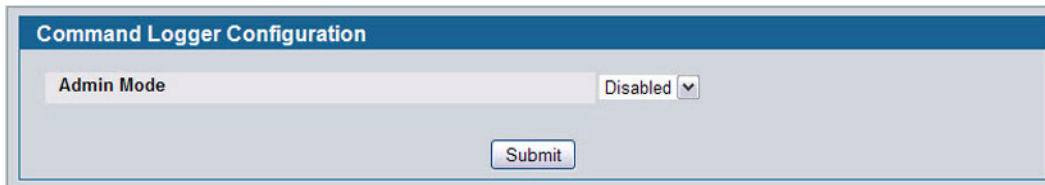


Figure 44: Command Logger Configuration

Table 36: Command Logger Configuration Fields

Field	Description
Admin Mode	<p>This field determines whether to log CLI commands in the system log file.</p> <ul style="list-style-type: none"> Enable: The system logs CLI commands. The commands appear in messages on the Buffered Log page. For example, the following log messages shows when the CLI command <code>show logging buffered</code> was issued, from which IP address the command was issued, and the name of the user who issued the command: <pre><5> NOV 29 22:25:00 10.254.24.172-1 UNKN[243420816]: cmd_logger_api.c(87) 34 %% CLI:10.254.24.65:admin:show logging buffered</pre> Disable: This system does not log CLI commands.

- If you change the administrative mode, click **Submit** to apply the change to the system.

Console Log Configuration

Use the Console Log Configuration page to control logging to any serial device attached to the switch.

To access the Console Log Configuration page, click **LAN > Administration > Log > Console Log Configuration** in the navigation menu.

Figure 45: Console Log Configuration

Table 37: Console Log Configuration Fields

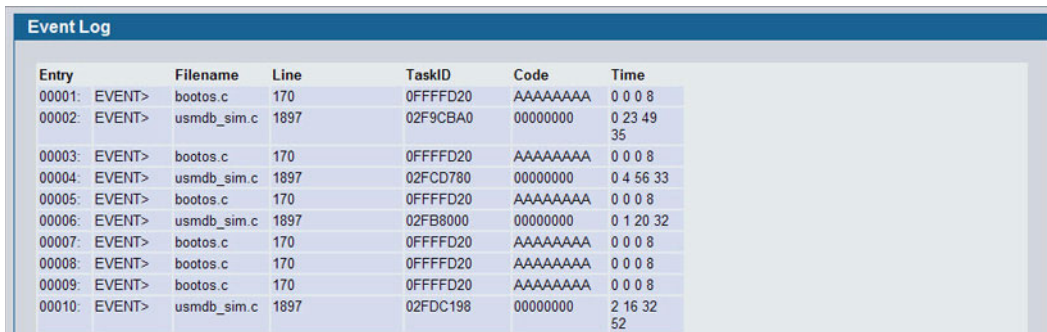
Field	Description
Admin Status	<p>From the menu, select whether to enable or disable console logging. The default is disabled.</p> <ul style="list-style-type: none"> • Enabled: Prints log messages to the device attached to the switch serial port. • Disabled: Log messages do not print to the device attached to the switch serial port.
Severity Filter	<p>Use the menu to select the severity of the logs to print to the console. Logs with the severity level you select and all logs of greater severity print. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert(1). The severity can be one of the following levels:</p> <ul style="list-style-type: none"> • Emergency (0): The highest level warning level. If the device is down or not functioning properly, an emergency log is saved to the device. • Alert (1): The second highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down. • Critical (2): The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional. • Error (3): A device error has occurred, such as if a port is offline. • Warning (4): The lowest level of a device warning. • Notice (5): Provides the network administrators with device information. • Informational (6): Provides device information. • Debug (7): Provides detailed information about the log. Debugging should only be entered by qualified support personnel.

- If you make any changes to the page, click **Submit** to apply the change to the system.

Event Log

Use the **Event Log** page to display the event log, which is used to hold error messages for catastrophic events. After the event is logged and the updated log is saved in flash memory, the switch will be reset. The log can hold at least 2,000 entries (the actual number depends on the platform and OS), and is erased when an attempt is made to add an entry after it is full. The event log is preserved across system resets.

To access the **Event Log** page, click **LAN > Monitoring > Log > System Log** in the navigation tree.



Entry	Filename	Line	TaskID	Code	Time
00001: EVENT>	bootos.c	170	0FFFFD20	AAAAAAAA	0 0 0 8
00002: EVENT>	usmdb_sim.c	1897	02F9CBA0	00000000	0 23 49 35
00003: EVENT>	bootos.c	170	0FFFFD20	AAAAAAAA	0 0 0 8
00004: EVENT>	usmdb_sim.c	1897	02FCD780	00000000	0 4 56 33
00005: EVENT>	bootos.c	170	0FFFFD20	AAAAAAAA	0 0 0 8
00006: EVENT>	usmdb_sim.c	1897	02FB8000	00000000	0 1 20 32
00007: EVENT>	bootos.c	170	0FFFFD20	AAAAAAAA	0 0 0 8
00008: EVENT>	bootos.c	170	0FFFFD20	AAAAAAAA	0 0 0 8
00009: EVENT>	bootos.c	170	0FFFFD20	AAAAAAAA	0 0 0 8
00010: EVENT>	usmdb_sim.c	1897	02FDC198	00000000	2 16 32 52

Figure 46: Event Log

Table 38: Event Log Fields

Field	Description
Entry	The number of the entry within the event log. The most recent entry is first.
Filename	The D-Link DWS-4000 Series source code filename identifying the code that detected the event.
Line	The line number within the source file of the code that detected the event.
Task ID	The OS-assigned ID of the task reporting the event.
Code	The event code passed to the event log handler by the code reporting the event.
Time	The time the event occurred, measured from the previous reset.

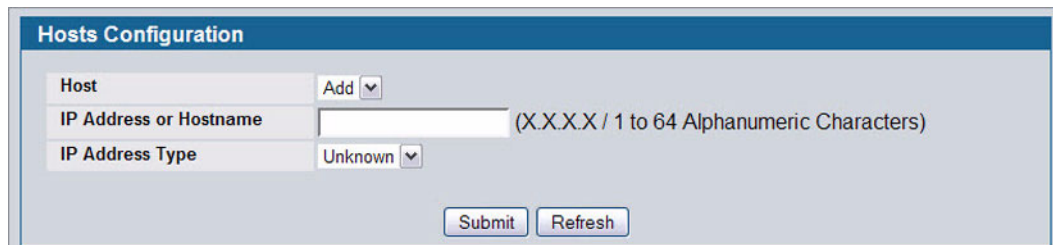
- Click **Refresh** to update the page with the latest log entries.

Hosts Configuration

Use the Host Configuration page to configure remote logging hosts where the switch can send logs. To enable remote logging, see “[Syslog Configuration](#)” on page 119.

To access the Host Configuration page, click **LAN > Administration > Log > Host Configuration** in the navigation tree.

[Figure 47](#) shows the Host Configuration page in its default state, before any logging hosts are added.



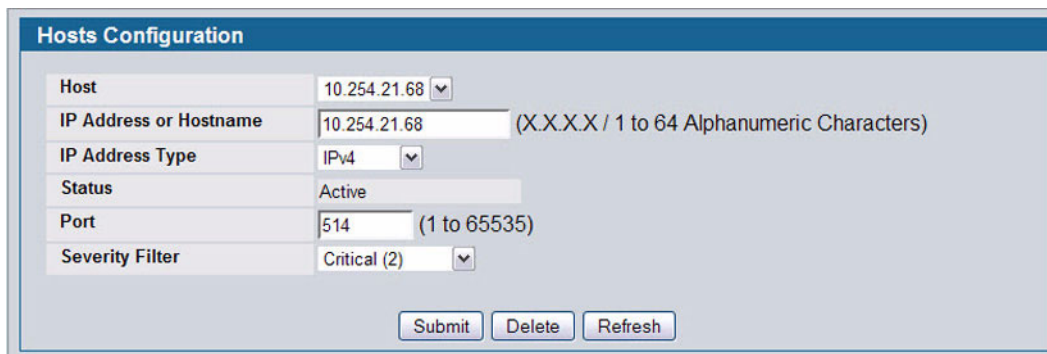
The screenshot shows the 'Hosts Configuration' page with the following fields and controls:

Host	Add	
IP Address or Hostname		(X.X.X.X / 1 to 64 Alphanumeric Characters)
IP Address Type	Unknown	

Buttons: Submit, Refresh

Figure 47: Host Configuration

After you add a logging host, the screen displays additional fields, as [Figure 48](#) shows



The screenshot shows the 'Hosts Configuration' page with the following fields and controls:

Host	10.254.21.68	
IP Address or Hostname	10.254.21.68	(X.X.X.X / 1 to 64 Alphanumeric Characters)
IP Address Type	IPv4	
Status	Active	
Port	514	(1 to 65535)
Severity Filter	Critical (2)	

Buttons: Submit, Delete, Refresh

Figure 48: Host Configuration with Logging Host

Adding a Remote Logging Host

Use the following procedures to add, configure, or delete a remote logging host.

1. From the **Host** field, select **Add** to add a new host, or select the IP address of an existing host to configure the host.
If you are adding a new host, enter the IP address of the host in the **IP Address** field and click **Submit**. The screen refreshes, and additional fields appear.
2. In the **Port** field, type the port number on the remote host to which logs should be sent.
3. Select the severity level of the logs to send to the remote host.
4. Click **Submit** to apply the changes to the system.

Deleting a Remote Logging Host

To delete a remote logging host from the configured list, select the IP address of the host from the Host field, and then click **Delete**.

Persistent Log Configuration

The persistent log is stored in persistent storage, which means that the log messages are retained across a switch reboot.

- The first log type is the **system startup log**. The system startup log stores the first N messages received after system reboot. This log always has the log full operation attribute set to stop on full and can store up to 32 messages.
- The second log type is the **system operation log**. The system operation log stores the last N messages received during system operation. This log always has the log full operation attribute set to overwrite. This log can store up to 1000 messages.

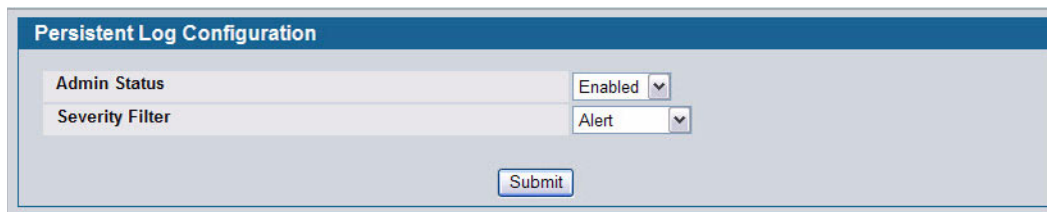
Either the system startup log or the system operation log stores a message received by the log subsystem that meets the storage criteria, but not both. In other words, on system startup, if the startup log is configured, it stores messages up to its limit. The operation log, if configured, then begins to store the messages.

The system keeps up to three versions of the persistent logs, named <FILE>1.txt, <FILE>2.txt, and <FILE>3.txt. Upon system startup, <FILE>3.txt is removed, <FILE>2.txt is renamed <FILE>3.txt, <FILE>1.txt is renamed <FILE>2.txt, <FILE>1.txt is created and logging begins into <FILE>1.txt. (Replace <FILE> in the above example to specify o1og for the operation log and s1og for the startup log.)

The local persistent logs can be retrieved via the Web or CLI, or via xmodem over the local serial cable.

Use the **Persistent Log Configuration** page to enable or disable persistent logging and to set the severity filter.

To access the **Persistent Log Configuration** page, click **LAN > Administration > Log > Persistent Logger Configuration** in the navigation menu.



Persistent Log Configuration	
Admin Status	Enabled
Severity Filter	Alert
<input type="button" value="Submit"/>	

Figure 49: Persistent Log Configuration

Table 39: Persistent Log Configuration Fields

Field	Description
Admin Status	<p>Select whether to enable or disable persistent logging. The default is disabled.</p> <ul style="list-style-type: none"> • Enabled: Prints log messages to the device attached to the switch serial port. • Disabled: Log messages do not print to the device attached to the switch serial port.
Severity Filter	<p>Use the menu to select the severity of the logs to print to the console. Logs with the severity level you select and all logs of greater severity print. For example, if you select Error, the logged messages include Error, Critical, Alert, and Emergency. The default severity level is Alert(1). The severity can be one of the following levels:</p> <ul style="list-style-type: none"> • Emergency (0): The highest level warning level. If the device is down or not functioning properly, an emergency log is saved to the device. • Alert (1): The second highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down. • Critical (2): The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional. • Error (3): A device error has occurred, such as if a port is offline. • Warning (4): The lowest level of a device warning. • Notice (5): Provides the network administrators with device information. • Informational (6): Provides device information. • Debug (7): Provides detailed information about the log. Debugging should only be entered by qualified support personnel.

- If you make any changes to the page, click **Submit** to apply the change to the system.

Persistent Log

Use the Persistent Log page to view the persistent log messages.

To access the Persistent Log page, click **LAN > Monitoring > Log > Persistent Log** in the navigation tree menu.

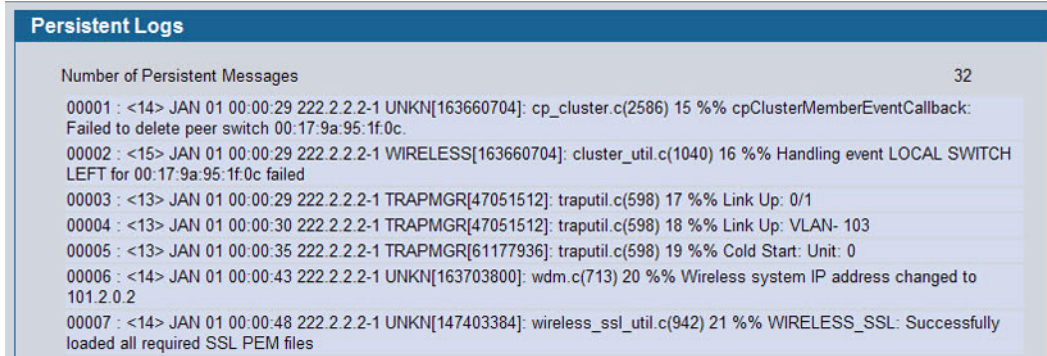


Figure 50: Persistent Log

Table 40: Persistent Log Fields

<i>Field</i>	<i>Description</i>
Total Number of Messages	Shows the number of persistent messages the system has logged.

The rest of the page displays the log messages. The following example shows a log message:

```
<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry
```

This log message has a severity level of 7 (15 mod 8), which is a debug message. The system is not stacked (STK0). The message was generated by the MSTP component running in thread ID 2110. The message was generated on August 24 05:34:05 by line 318 of file mspt_api.c. This is the 237th message logged.

- Click **Refresh** to refresh the page with the latest log entries.

Syslog Configuration

Use the Syslog Configuration page to allow the switch to send log messages to the remote logging hosts configured on the system.

To access the **System Log Configuration** page, click **LAN > Administration > Log > System Log Configuration** in the navigation tree.

Syslog Configuration	
Admin Status	Disable ▾
Local UDP Port	514 (1 to 65535)
Messages Received	64664
Messages Dropped	0
Messages Relayed	0
<input type="button" value="Submit"/> <input type="button" value="Refresh"/>	

Figure 51: System Log

Table 41: Syslog Configuration Fields

Field	Description
Admin Status	Specifies whether to send log messages to the remote syslog hosts configured on the switch: <ul style="list-style-type: none"> • Enable: Messages will be sent to all configured hosts (syslog collectors or relays) using the values configured for each host. For information about syslog host configuration, see “Hosts Configuration” on page 115. • Disable: Stops logging to all syslog hosts. Disable means no messages will be sent to any collector/relay.
Local UDP Port	Specifies the port on the switch from which syslog messages are sent. The default port is 514.
Messages Received	The number of messages received by the log process. This includes messages that are dropped or ignored.
Messages Dropped	The number of messages that could not be processed due to error or lack of resources.
Messages Relayed	The number of messages forwarded by the syslog function to a syslog host. Messages forwarded to multiple hosts are counted once for each host.

- If you make any changes to the page, click **Submit** to apply the change to the system.

Trap Log

Use the Trap Log page to view the entries in the trap log. For information about how to copy the file to a TFTP server, see [“Upload File From Switch \(TFTP\)” on page 171](#).

To access the Trap Log page, click **LAN > Monitoring > Log > Trap Log** in the navigation menu.

Trap Log		
Number of Traps Since Last Reset		3
Trap Log Capacity		256
Number of Traps Since Log Last Viewed		3
Log	System Up Time	Trap
0	0 days 02:24:31	Failed User Login: Unit: 1 User ID: @
1	0 days 00:25:08	Link Up: 0/1
2	0 days 00:00:30	Cold Start: Unit: 0
<input type="button" value="Clear Log"/>		

Figure 52: Trap Log

Table 42: Trap Log Fields

Field	Description
Number of Traps Since Last Reset	The number of traps generated since the trap log entries were last cleared.
Trap Log Capacity	The maximum number of traps stored in the log. If the number of traps exceeds the capacity, the entries will overwrite the oldest entries.
Number of Traps Since Log Last Viewed	The number of traps that have occurred since the traps were last displayed. Displaying the traps by any method (terminal interface display, Web display, upload file from switch, etc.) will cause this counter to be cleared to 0.
Log	The sequence number of this trap.
System Up Time	The time at which this trap occurred, expressed in days, hours, minutes and seconds since the last reboot of the switch.
Trap	Displays the information identifying the trap.

- Click **Clear Log** to clear all entries in the log. Subsequent displays of the log will only show new log entries.

Defining SNMP Parameters

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports SNMP version 1, SNMP version 2, and SNMP version 3. The Web interfaces supports configuration of SNMPv1 and v2; SNMPv3 is supported only in the CLI.

SNMP v1 and v2

The SNMP agent maintains a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agent are controlled by access strings.

SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, the User Security Model (USM) is defined for SNMPv3 and includes:

- **Authentication:** Provides data integrity and data origin authentication.
- **Privacy:** Protects against disclosure of message content. Cipher-Block-Chaining (CBC) is used for encryption. Either authentication is enabled on an SNMP message, or both authentication and privacy are enabled on an SNMP message. However privacy cannot be enabled without authentication.
- **Timeliness:** Protects against message delay or message redundancy. The SNMP agent compares incoming message to the message time information.
- **Key Management:** Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage device features. SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

Authentication or Privacy Keys are modified in the SNMPv3 User Security Model (USM).

Use the SNMP page to define SNMP parameters. To display the SNMP page, click **LAN > Administration > SNMP Manager** in the navigation tree.

SNMP Community Configuration

Access rights are managed by defining communities on the SNMPv1, 2 Community page. When the community names are changed, access rights are also changed. SNMP Communities are defined only for SNMP v1 and SNMP v2.

Use the Community Configuration page to enable SNMP and Authentication notifications.

To display the Community Configuration page, click **LAN > Administration > SNMP Manager > SNMP Community Table** in the navigation tree.

SNMP Community Name	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read Only	Enable
private	0.0.0.0	0.0.0.0	Read/Write	Enable

Figure 53: SNMP Community Configuration

Table 43: Community Configuration Fields

Field	Description
Community	<p>Contains the predefined and user-defined community strings that act as a password and are used to authenticate the SNMP management station to the device. A community string can contain a maximum of 20 characters. By default, the options available in the menu are as follows:</p> <ul style="list-style-type: none"> • public: This SNMP community has Read Only privileges and its status set to enable • private: This SNMP community has Read/Write privileges and its status set to enable. • Create: Use this option to create a new user-defined community string.
SNMP Community Name	Use this field to reconfigure an existing community or to create a new one. A valid entry is a case-sensitive string of up to 16 characters.
Client IP Address	<p>Taken together, the Client IP Address and Client IP Mask denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (IP Address or IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, every client's IP address is ANDed with the mask, as is the Client IP Address, and, if the values are equal, access is allowed. For example, if the Client IP Address and Client IP Mask parameters are 192.168.1.0/255.255.255.0, then any client whose IP address is 192.168.1.0 through 192.168.1.255 (inclusive) will be allowed access. To allow access from only one station, use a Client IP Mask value of 255.255.255.255, and use that machine's IP address for Client IP Address.</p>

Table 43: Community Configuration Fields (Cont.)

Field	Description
Client IP Mask	Along with the Client IP Address , the Client IP Mask denotes a range of IP addresses from which SNMP clients may use that community to access this device.
Access Mode	Specify the access level for this community: <ul style="list-style-type: none"> • Read-Only: The Community has read only access to the MIB objects configured in the view. • Read-Write: The Community has read/modify access to the MIB objects configured in the view.
Status	Specify the status of this community: <ul style="list-style-type: none"> • Enable: The community is enabled, and the Community Name must be unique among all valid Community Names or the set request will be rejected. • Disable: The Community is disabled and the Community Name becomes invalid.

- If you make any changes to the page, click **Submit** to apply the changes to the system. If you create a new Community, it is added to the table below the **Submit** button.
- Click **Delete** to delete the selected SNMP Community.

Trap Receiver Configuration

Use the Trap Receiver Configuration page to configure information about the SNMP community and the trap manager that will receive its trap packets.

To access the Trap Receiver Configuration page, click **LAN > Administration > SNMP Manager > Trap Receiver Configuration** from the navigation tree.

Figure 54: Trap Receiver Configuration

Table 44: Trap Receiver Configuration Fields

Field	Description
SNMP Trap Name	Select Create , to configure the SNMP trap name for the SNMP trap packet to be sent to the trap manager. If you have already configured an SNMP trap name, you can select it from the drop-down menu to change the settings or delete it.
SNMP Trap Name	When the previous field is set to Create , enter the SNMP trap name for the SNMP trap packet to be sent to the trap manager. This may be up to 16 characters and is case sensitive.
SNMP Version	Select the trap version to be used by the receiver from the pull down menu: <ul style="list-style-type: none"> • SNMP v1. Uses SNMP v1 to send traps to the receiver. • SNMP v2. Uses SNMP v2 to send traps to the receiver.
Protocol	Select the type of protocol used for the SNMP Trap Receiver Configuration: <ul style="list-style-type: none"> • IPv4. Choose IPv4 to enter the address in IPv4 format. • IPv6. Choose IPv6 to enter the address in IPv6 format.
IP Address/Host Name	Enter the IP address in dotted-decimal format of the system that receives SNMP traps from the switch. Alternatively, you can enter the hostname of the trap receiver
Status	Select the receiver's status from the pulldown menu: <ul style="list-style-type: none"> • Enable: Send traps to the receiver • Disable: Do not send traps to the receiver.

If you make any changes to the page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a **save**.

Trap Flags

Use the Trap Flags page to enable or disable traps at a component level that the switch can send to an SNMP manager. When the condition identified by an active trap is encountered by the switch, a trap message is sent to any enabled SNMP Trap Receivers, and a message is written to the trap log. If the component level trap flag is disabled, then no trap is sent to the SNMP Manager even if the individual traps in that component are enabled.

To access the Trap Flags page, click **LAN > Administration > SNMP Manager > Trap Flags** page.

Trap Flags Configuration	
Authentication	Enable ▾
Link Up/Down	Enable ▾
Multiple Users	Enable ▾
Spanning Tree	Enable ▾
ACL Traps	Disable ▾
Captive Portal Trap Mode	Disable ▾

Submit

Figure 55: Trap Flags Configuration

Table 45: Trap Flags Configuration Fields

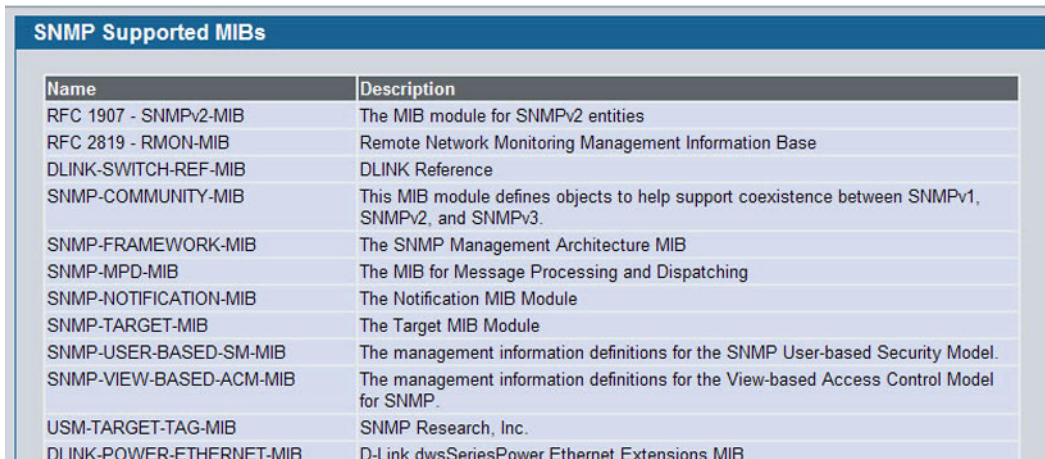
Field	Description
Authentication	Enable or disable activation of authentication failure traps by selecting the corresponding line on the pulldown entry field. The factory default is enabled.
Link Up/Down	Enable or disable activation of link status traps by selecting the corresponding line on the pulldown entry field. The factory default is enabled.
Multiple Users	Enable or disable activation of multiple user traps by selecting the corresponding line on the pulldown entry field. The factory default is enabled. This trap is triggered when the same user ID is logged into the switch more than once at the same time (either via telnet or the serial port).
Spanning Tree	Enable or disable activation of spanning tree traps by selecting the corresponding line on the pulldown entry field. The factory default is enabled.
ACL Traps	Enable or disable activation of ACL traps by selecting the corresponding line on the pulldown entry field. The factory default is disabled.
Captive Portal	Enable or disable allowing the SNMP agent on the switch to generate captive portal SNMP traps. The factory default is Disable which prevents the SNMP agent on the switch from generating any captive portal SNMP traps, even if they are individually enabled.

If you make any changes to this page, click **Submit** to apply the changes to the system.

Supported MIBs

The **Supported MIBs** page lists the MIBs that the system currently supports.

To access the **Supported MIBs** page, click **LAN > Monitoring > Supported MIBs** in the navigation menu. A portion of the web screen is shown [Figure 56](#).



SNMP Supported MIBs	
Name	Description
RFC 1907 - SNMPv2-MIB	The MIB module for SNMPv2 entities
RFC 2819 - RMON-MIB	Remote Network Monitoring Management Information Base
DLINK-SWITCH-REF-MIB	DLINK Reference
SNMP-COMMUNITY-MIB	This MIB module defines objects to help support coexistence between SNMPv1, SNMPv2, and SNMPv3.
SNMP-FRAMEWORK-MIB	The SNMP Management Architecture MIB
SNMP-MPD-MIB	The MIB for Message Processing and Dispatching
SNMP-NOTIFICATION-MIB	The Notification MIB Module
SNMP-TARGET-MIB	The Target MIB Module
SNMP-USER-BASED-SM-MIB	The management information definitions for the SNMP User-based Security Model.
SNMP-VIEW-BASED-ACM-MIB	The management information definitions for the View-based Access Control Model for SNMP.
USM-TARGET-TAG-MIB	SNMP Research, Inc.
DLINK-POWER-ETHERNET-MIB	D-Link dwsSeriesPower Ethernet Extensions MIB

Figure 56: Supported MIBs

Table 46: Supported MIBs Fields

<i>Field</i>	<i>Description</i>
Name	The RFC number if applicable and the name of the MIB.
Description	The RFC title or MIB description.

Managing the DHCP Server

DHCP is generally used between clients (e.g., hosts) and servers (e.g., routers) for the purpose of assigning IP addresses, gateways, and other networking definitions such as DNS, NTP, and/or SIP parameters. The DHCP Server folder contains links to web pages that define and display DHCP parameters and data.

Global Configuration

Use the Global Configuration page to configure DHCP global parameters.

To display the page, click **LAN > Administration > DHCP Server > Global Configuration** in the navigation tree.

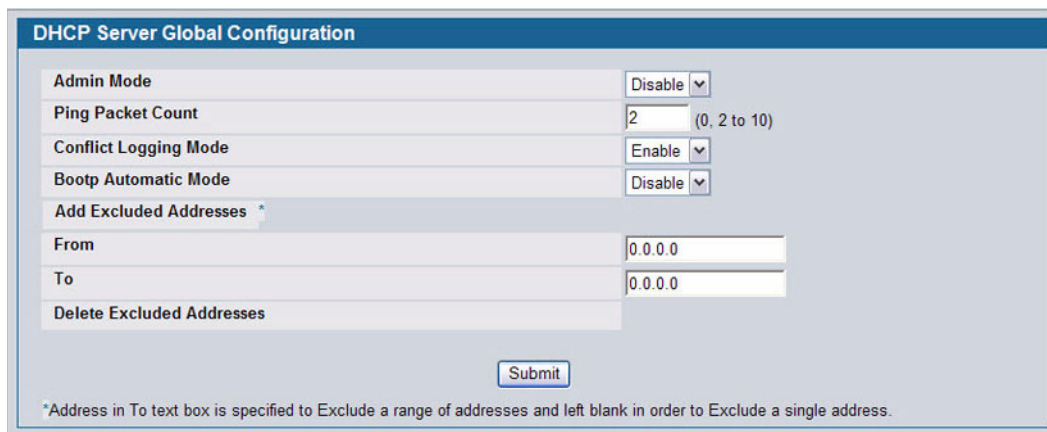


Figure 57: DHCP Server Global Configuration

Table 47: DHCP Server Global Configuration Fields

Field	Description
Admin Mode	Enables or disables DHCP server operation on the switch. The default value is Disable.
Ping Packet Count	Specifies the number of packets a server sends to a Pool address to check for duplication as part of a ping operation. Default value is 2. The valid range is (0, 2 to 10). Setting the value to 0 disables the function.
Conflict Logging Mode	Specifies whether to enable or disable conflict logging on a DHCP Server. The default value is Enable.
Bootp Automatic Mode	Specifies whether to enable or disable Bootp for dynamic pools.
Enable	Allows the allocation of the addresses in the automatic address pool to the BootP client.
Disable	Does not use the automatic address pool addresses for BootP clients. This is the default value.

Table 47: DHCP Server Global Configuration Fields (Cont.)

Field	Description
Add Excluded Addresses	Use the From and To fields to specify the IP addresses that the server should not assign to the client. If you want to exclude a range of addresses, set the range boundaries. Note: It is strongly recommended not to add thousands of addresses in the range. The larger the range, more time will be taken by the DHCP server to assign an IP address.
From	To exclude an address range, specify the low address in the range. To specify a single address to exclude, enter the address in the From field and leave the To field at the default value of 0.0.0.0. For example, in Figure 58 on page 129 , the user is adding the address 192.168.17.100 to the excluded addresses list.
To	To exclude an address range, specify the high address in the range. To exclude a single address, do not enter a value in this field.
Delete Excluded Addresses	After you add excluded addresses, they appear below this field title, as Figure 58 on page 129 shows. Each address or address range has a check box next to it.

- If you change any settings or add an excluded address range, click **Submit** to apply the changes to the system. Each time you enter a value in the **From** or **To** fields, click **Submit** to add the address or address range to the excluded address list.
- To Delete an address or address range from the excluded address list, select one or more check box beneath the Delete **Excluded Addresses** field and click **Submit**.

Pool Configuration

Use the DHCP Pool Configuration page to create the pools of addresses that can be assigned by the server.

To access the Pool Configuration page, click **LAN > Administration > DHCP Server > Pool Configuration** in the navigation tree.

In [Figure 58](#), some of the blank fields where you add IP addresses have been edited out of the image for display purposes. You can add up to eight addresses in the Default Router Addresses, DNS Server Addresses, NetBIOS name Server Addresses and IP Address Value fields.

If you select **Dynamic** or **Manual** from the **Type of Binding** drop-down menu, the screen refreshes and a slightly different set of fields appears.

The screenshot shows the 'DHCP Server Pool Configuration' web page. At the top, there's a title bar. Below it, the form is organized into several sections. The first section contains 'Pool Name' with a 'Create' dropdown menu. The second section is another 'Pool Name' field with a note '(1 to 31 Alphanumeric Characters)'. The third section is 'Type of Binding' with a dropdown menu set to 'Unallocated'. The fourth section is 'Lease Time' with a dropdown menu set to 'Specified Duration'. Below this are three input fields for 'Days' (range 0 to 59), 'Hours' (range 0 to 22), and 'Minutes' (range 0 to 86399). The next section is 'Default Router Addresses', followed by 'DNS Server Addresses', and finally 'NetBIOS Name Server Addresses'. Each of these three sections contains a vertical stack of eight input fields for IP addresses.

Figure 58: Pool Configuration

Table 48: Pool Configuration Fields

Field	Description
Pool Name	For a user with read/write permission, this field would show names of all the existing pools along with an additional option Create. When the user selects Create, another text box, Pool Name, appears where the user may enter name for the Pool to be created. For a user with read-only permission, this field would show names of the existing pools only.
Pool Name	This field appears when the user with read-write permission has selected Create in the Drop Down list against Pool Name. Specifies the Name of the Pool to be created. Pool Name can be up to 31 characters in length.
Type of Binding	Specifies the type of binding for the pool. <ul style="list-style-type: none"> • Unallocated: The addresses are not assigned to a client. • Dynamic: The IP address is automatically assigned to a client by the DHCP server. • Manual: You statically assign an IP address to a client based on the client's MAC address.
Network Number	If you specify Dynamic as the type of binding, this field appears. Specifies the network number (host bits) for a DHCP address of a dynamic pool. For example, if 192.168.5.0 is the network number and 255.255.255.0 is the network mask (or a prefix length of 24) for the pool, the IP addresses in the pool range from 192.168.5.1 - 192.168.5.254.
Network Mask	For dynamic bindings, this field specifies the subnet mask for a DHCP address of a dynamic pool. You can enter a value in Network Mask or Prefix Length to specify the subnet mask, but do not enter a value in both fields.
Prefix Length	For dynamic bindings, this field specifies the subnet number for a DHCP address of a dynamic pool. You can enter a value in Network Mask or Prefix Length to specify the subnet mask, but do not enter a value in both fields. The valid range is 0 to 32.
Client Name	For manual bindings, this field specifies a name for the client to which the DHCP server will statically assign an IP address. This field is optional.
Hardware Address	For manual bindings, this field specifies the MAC address of the hardware platform of the DHCP client.
Hardware Address Type	For manual bindings, this field specifies the protocol of the hardware platform of the DHCP client. Valid types are ethernet and ieee802. Default value is ethernet.
Client ID	For manual bindings, this field specifies the Client Identifier for DHCP manual Pool.
Host Number	For manual bindings, this field specifies the IP address to be statically assigned to a DHCP client. The host can be set only if at least one among of Client Identifier or Hardware Address is specified. Deleting Host would delete Client Name, Client ID, Hardware Address for the Manual Pool and set the Pool Type to Unallocated.
Host Mask	For manual bindings, this field specifies the subnet mask to be statically assigned to a DHCP client. You can enter a value in Host Mask or Prefix Length to specify the subnet mask, but do not enter a value in both fields.
Prefix Length	For manual and dynamic bindings, this field specifies the subnet mask for a manual binding to a DHCP client. You can enter a value in Network Mask or Prefix Length to specify the subnet mask, but do not enter a value in both fields. The valid range is 0 to 32.

Table 48: Pool Configuration Fields (Cont.)

Field	Description
Lease Time	Specifies the type of lease to assign clients: <ul style="list-style-type: none"> • Infinite: For dynamic bindings, an infinite lease time is a lease period of 60 days. For manual bindings, an infinite lease time means the lease period does not expire. • Specified Duration: Allows you to specify the lease period. The default value is Specified Duration. • Db-node Broadcast: Uses broadcasted queries.
Days	For a Specified Duration lease time, this field specifies the number of days for the lease period. The default value is 1, and the valid range is 0-59.
Hours	For a Specified Duration lease time, this field specifies the number of hours for the lease period. The default value is 1, and the valid range is 0-1439.
Minutes	For a Specified Duration lease time, this field specifies the number of minutes for the lease period. The default value is 1, and the valid range is 0-86399.
Default Router Addresses	Specifies the list of default router IP addresses for the pool. You can specify up to eight addresses in order of preference.
DNS Server Addresses	Specifies the list of DNS server IP addresses for the pool. You can specify up to eight addresses in order of preference.
NetBIOS Name Server Addresses	Specifies the list of NetBIOS name server IP addresses for the pool. You can specify up to eight addresses in order of preference.
NetBIOS Node Type	Specifies the NetBIOS node type for DHCP clients: <ul style="list-style-type: none"> • p-node Peer-to-Peer: Uses point-to-point name queries to a name server. • m-node Mixed: Uses broadcasts first, then uses queries the name server. • h-node Hybrid: Uses queries the name server first, and then uses broadcasts.
Next Server Address	Specifies the IP address of the next server in the client's boot process, such as a TFTP server.
Domain Name	Specifies the domain name for a DHCP client. The domain name can be up to 255 characters in length.
Bootfile	Specifies the name of the default boot image for a DHCP client. The file name can be up to 128 characters in length.
Add Options	The rest of the fields on the page allow you to add and configure DHCP options. See RFC 2132 for more information about DHCP options.
Code	Specifies the DHCP option code. The valid range is 1-254.
Ascii Value	Specifies an NVT ASCII character string.
Hex Value	Specifies dotted hexadecimal data. Each byte in hexadecimal character strings is 2 hexadecimal digits. Each byte can be separated by a colon or white space. A period separates 2 bytes/4 hexadecimal digits.
IP Address Values	Specifies the Option IP addresses.

- After you configure values for the DHCP address pool, click **Submit** to create the pool and apply the changes to the system.
- To delete a pool, select the pool from the **Pool Name** drop-down menu and click **Delete**.

Pool Options

Use the Pool Options page to configure DHCP options that the DHCP server can pass to the client. For more information about DHCP options, see RFC 2132.

To access the Pool Options page, click **LAN > Administration > DHCP Server > Pool Options** in the navigation menu.

If no DHCP pools exist, the Pool Options page does not display the fields shown in [Figure 59](#).



Figure 59: Pool Options

If any DHCP pools are configured on the system, the Pool Options page contains the following fields:

Table 49: Pool Options Fields

Field	Description
Pool Name	Select the DHCP pool to with the options you want to view or configure.
Option Code	Displays the DHCP option code configured for the selected Pool.
Option Type	Specifies the type of option associated with the option code configured for the selected pool. The possible values are as follows: <ul style="list-style-type: none"> • Ascii: The option type is a text string. • Hex: The option type is a hexadecimal number. • IP Address: The option type is an IP address.
Option Value	Shows the option to be passed to from the DHCP server to the client.
Delete Option Code	To delete an option code for the selected Pool, enter the option code in the folder and click Delete . This button is not visible to a user with read-only permission.

Reset Configuration

Use the Reset Configuration page to clear IP address bindings between that the DHCP server assigned to the client.

To access the Reset Configuration page, click **LAN > Administration > DHCP Server > Reset Configuration** in the navigation tree.

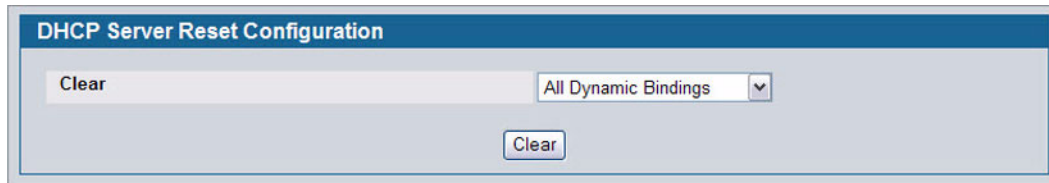


Figure 60: Reset Configuration

Table 50: Reset Configuration Fields

Field	Description
Clear	Specifies what to clear from the DHCP server database: <ul style="list-style-type: none"> • All Dynamic Bindings: Deletes all dynamic bindings from all address pools. • Specific Dynamic Binding: Deletes the specified binding. • All Address Conflicts: Deletes all address conflicts from the DHCP server database. • Specific Address Conflict: Deletes a specified conflicting address from the database.
Clear IP Address	If you select Specific Dynamic Bindings or Specific Address Conflicts from the Clear field, the screen refreshes and the Clear IP Address field appears. Enter the specific IP address to clear from the DHCP server.

- After you select the bindings or conflicts to clear and, if necessary, enter the specific IP address, click **Clear** to remove the binding from the DHCP server.

DHCP Server Summary

Bindings Information

Use the **DHCP Server Bindings Information** page to view information about the IP address bindings in the DHCP server database.

To access the **DHCP Server Bindings Information** page, click **LAN > Monitoring > DHCP Server Summary > Binding Information** in the navigation tree.

Figure 61: Bindings Information

Table 51: Bindings Information Fields

Field	Description
DHCP Binding	Select the bindings to display: <ul style="list-style-type: none"> • All Bindings: Show all bindings. • Specific Binding: Show a specific binding. When you select this option, the screen refreshes, and the Binding IP Address field appears.
Binding IP Address	Specify the IP address for which you want to view binding information. This field is only available if you select Specific Binding from the DHCP Binding field.
IP Address	Displays the client IP address.
Hardware Address	Displays the client MAC address.
Lease Time Left	Shows the remaining time left in the lease in Days, Hours and Minutes dd:hh:mm format.
Pool Allocation Type	Shows the type of binding, which is dynamic or manual.

- If you change any settings, click **Submit** to apply the changes to the system.

Server Statistics

Use the **DHCP Server Statistics** page to view information about the DHCP server bindings and messages.

To access the Server Statistics page, click **LAN > Monitoring > DHCP Server Summary > Server Statistics** in the navigation menu.

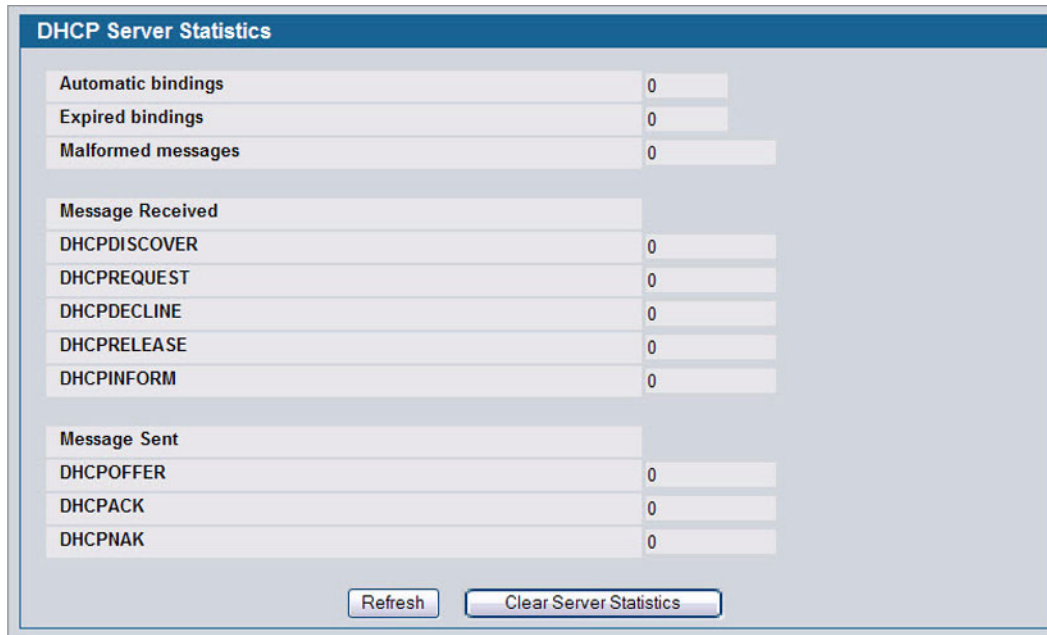


Figure 62: Server Statistics

Table 52: Server Statistics Fields

<i>Field</i>	<i>Description</i>
Automatic Bindings	Shows the number of automatic bindings on the DHCP server.
Expired Bindings	Shows the number of expired bindings on the DHCP server.
Malformed Messages	Shows the number of the malformed messages.
Message Received	
DHCPDISCOVER	Shows the number of DHCPDISCOVER messages received by the DHCP server.
DHCPREQUEST	Shows the number of DHCPREQUEST messages received by the DHCP server.
DHCPDECLINE	Shows the number of DHCPDECLINE messages received by the DHCP server.
DHCPRELEASE	Shows the number of DHCPRELEASE messages received by the DHCP server.
DHCPINFORM	Shows the number of DHCPINFORM messages received by the DHCP server.
DHCPOFFER	Shows the number of DHCPOFFER messages sent by the DHCP server.
DHCPACK	Shows the number of DHCPACK messages sent by the DHCP server.
DHCPNAK	Shows the number of DHCPNAK messages sent by the DHCP server.

- Click **Refresh** to update the information on the screen.
- Click **Clear Server Statistics** to reset all counters to zero.

Conflicts Information

Use the Conflicts Information page to view information on hosts that have address conflicts; i.e., when the same IP address is assigned to two or more devices on the network.

To access the Conflicts Information page, click **LAN > Monitoring > DHCP Server Summary > Conflicts Information** in the navigation tree.

Figure 63: Conflicts Information

Table 53: Conflicts Information Fields

Field	Description
DHCP Conflicts	Select the DHCP conflicts to display: <ul style="list-style-type: none"> • All Conflicts: Show all conflicts. • Specific Conflict: Show a specific conflict. When you select this option, the screen refreshes, and the Conflict IP Address field appears.
Conflict IP Address	Specify the IP address for which you want to view conflict information. This field is only available if you select Specific Conflicts from the DHCP Conflict field.
IP Address	Displays the client IP address.
Detection Method	Specifies the manner in which the IP address of the hosts were found on the DHCP server.
Detection Time	Specifies the time when the conflict was detected in N days NNh:NNm:NNs format with respect to the system up time.

Configuring Time Ranges

Use these pages to configure time ranges to use in time-based access control list (ACL) rules. Time-based ACLs allow one or more rules within an ACL to be based on a periodic or absolute time. Each ACL rule within an ACL except for the implicit *deny all* rule can be configured to be active and operational only during a specific time period. The time range pages allow you to define specific times of the day and week in order to implement time-based ACLs. For example, you can create a time-based MAC ACL that prevents clients with specific MAC addresses from accessing network resources on weekends. The time range is identified by a name and can then be referenced by an ACL rule defined within an ACL.

You must configure a named time range before you can reference it from an ACL. In other words, for the ACL to reference a time range, the time range must already exist. For more information about configuring ACLs, see [Section 7: “Configuring Access Control Lists,” on page 351](#).

Time Range Configuration

Use this page to create a named time range. Each time range can consist of one absolute time entry and/or one or more periodic time entries.

To access this page, click **LAN > Administration > Time Range > Configuration**.

Table	Current Number / Maximum Number
Time Ranges	0 / 100

Figure 64: Time Range Configuration

Table 54: Time Range Configuration

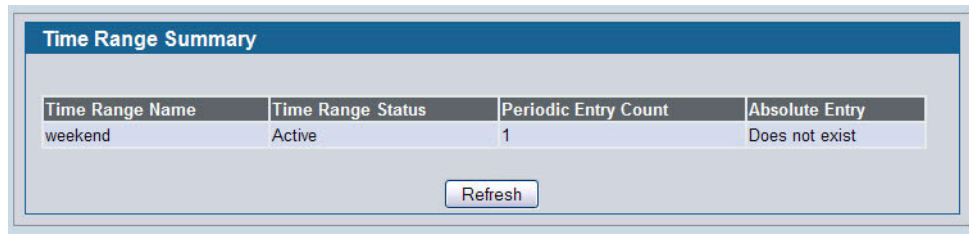
Field	Description
Time Range	To create a new time range, select Create New Time Range from the menu and specify the name in the following field. To delete an existing time range, select its name and click Delete .
Time Range Name	When creating a new time range, specify the name, which may include alphabetic, numeric, dash, underscore or space characters only. The name must start with an alphabetic character and can contain up to 31 characters.
Current Number/ Maximum Number	Displays the current number of time ranges configured on the switch and the maximum number of time ranges that can be configured.

- Use **Submit** to add a new time range.
- Use **Delete** to remove an existing time range.

Time Range Summary

Use this page to view summary information about configured time ranges.

To access this page, click **LAN > Administration > Time Range > Summary**.



Time Range Summary			
Time Range Name	Time Range Status	Periodic Entry Count	Absolute Entry
weekend	Active	1	Does not exist

Figure 65: Time Range Summary

Table 55: Time Range Summary

Field	Description
Time Range Name	Identifies the user-configured name of the time range.
Time Range Status	Shows whether the time range is active or inactive. A time range is inactive if the current day and time does not fall within the time entry specified in the time range.
Periodic Entry Count	Shows the number of periodic entries configured for the time range.
Absolute Entry	Shows whether an absolute entry is configured for the time range.

Time Range Entry Configuration

Use this page to configure periodic and absolute time range entries and add them to named time ranges.



Note: The time range entries use the system time for the time periods in which they take effect. Make sure you configure the SNTP server settings so that the SNTP client on the switch can obtain the correct date and time from the server.

To access this page, click **LAN > Administration > Time Range > Time Range Entry Configuration**.

Figure 66: Time Range Entry Configuration

Table 56: Time Range Entry Configuration

Field	Description
Time Range Name	Select the name of the time range to which you want to add a time range entry.
Time Range Entry	Select Create New Time Range Entry to add a new entry to a time range. To view or delete an existing time range entry, select its ID from the menu.
Time Range Entry ID	When creating a new time range entry, assign a unique ID number from 1–10. This field does not appear if the entry has already been configured.
Time Range Entry Type.	Specifies whether the entry is periodic or absolute. A periodic entry occurs at the same time every day or on one or more days of the week. An absolute entry does not repeat.

Table 56: Time Range Entry Configuration

Field	Description
Periodic Time Range Entry	
Applicable Days	Specify the day(s) when the time entry occurs: <ul style="list-style-type: none"> • Daily — Has the same start and end time every day • Weekdays — Has the same start and end time Monday through Friday • Weekends — Has the same start and end time on Saturday and Sunday • Days of the Week — Select the day of the week when the entry starts and stops. You do not need to use the same day of the week for the start and end time.
Start Day	(Periodic Days of Week only) Select the day the time range entry starts. To select multiple days, hold the CTRL key and click the days.
Start Time	Specify the time when the entry begins. The time is based on a 24-hour clock. For example, 6:00 PM is 18:00.
End Day	(Periodic Days of Week only) Select the day the time range entry ends.
End Time	Specify the time when the entry ends. The time is based on a 24-hour clock. For example, 6:00 PM is 18:00.
Absolute Time Range Entry	
Absolute Start Date and Time	Select the check box to configure the date and time when the time range entry begins.
Start Month	Select the month when the time entry begins.
Start Date	Select the day of the month when the time entry begins.
Start Year	Select the year when the time entry begins.
Start Time	Specify the time when the entry begins. The time is based on a 24-hour clock. For example, 6:00 PM is 18:00.
Absolute End Date and Time	Select the check box to configure the date and time when the time range entry ends.
End Month	Select the month when the time entry ends.
End Date	Select the day of the month when the time entry ends.
End Year	Select the year when the time entry ends.
End Time	Specify the time when the entry ends. The time is based on a 24-hour clock. For example, 6:00 PM is 18:00.

Click **Submit** to create the time range entry. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

Configuring DNS

You can use these pages to configure information about DNS servers the network uses and how the switch/router operates as a DNS client.

Global Configuration

Use this page to configure global DNS settings and to view DNS client status information.

To access this page, click **LAN > Administration > DNS Client > Global Configuration**.

Figure 67: DNS Global Configuration

Table 57: DNS Global Configuration Fields

Field	Description
Admin Mode	Select Enable or Disable from the pulldown menu to set the administrative status of DNS Client. The default is Disable.
Default Domain Name	Enter the default domain name for DNS client messages. The name should be no longer than 255 characters. When the system is performing a lookup on an unqualified hostname, this field is provided as the domain name (e.g., if default domain name is <i>.com</i> and the user enters <i>hotmail</i> , then hotmail is changed to <i>hotmail.com</i> to resolve the name). By default, no default domain name is configured in the system.
Retry Number	Enter the number of times to retry sending DNS queries. The valid values are from 0 to 100. The default value is 2.
Response Timeout	Enter the number of seconds to allow a DNS server to respond to a request before issuing a retry. Valid values are 0 to 3600. The default value is 3.
Domain List	Enter a domain list to define the domain to use when performing a lookup on an unqualified hostname. Each name must be no more than 256 characters. Multiple default domain names can be configured using the default domain-name list. If there is no domain list, the default domain name configured is used.

- If you change any settings, click **Submit** to send the information to the router.

- To create a new list of domain names, click **Create**. Then enter a name of the list and click submit. Repeat this step to add multiple domains to the default domain list.
- To remove a domain from the default list select the **Remove** option next to the item you want to remove and click **Submit**.

Server Configuration

Use this page to configure information about DNS servers that the router will use. The order in which you create them determines their precedence; i.e., DNS requests will go to the higher precedence server first. If that server is unavailable or does not respond in the configured response time, then the request goes to the server with the next highest precedence.

To access this page, click **LAN > Administration > DNS Client > Server Configuration**.

The screenshot shows the 'DNS Server Configuration' page. At the top, there is a blue header with the title 'DNS Server Configuration'. Below the header, there is a text input field labeled 'DNS Server Address'. Underneath that is a table titled 'DNS Server List'. The table has three columns: 'DNS Server Address', 'Precedence', and 'Remove'. The first row contains the IP address '10.27.138.20', the precedence value '0', and a checkbox. At the bottom of the form, there are two buttons: 'Submit' and 'Refresh'.

Figure 68: DNS Server Configuration

Table 58: DNS Server Configuration Fields

<i>Field</i>	<i>Description</i>
DNS Server Address	To add a new DNS server to the list, enter the DNS server IPv4 or IPv6 address in numeric notation.
Precedence	Shows the precedence value of the server that determines which server is contacted first; a lower number indicates has higher precedence.

- To create a new DNS server, enter an IP address in standard IPv4 or IPv6 dot notation in the **DNS Server Address** and click **Submit**. The server appears in the list below. The precedence is set in the order created.
- To change precedence, you must remove the server(s) by clicking the **Remove** box and then **Submit**, and add the server(s) in the preferred order.

DNS Host Name IP Mapping Configuration

Use this page to configure DNS host names for hosts on the network. The host names are associated with IPv4 or IPv6 addresses on the network, which are statically assigned to particular hosts.

To access this page, click **LAN > Administration > DNS Client > HostName IP Mapping** in the navigation tree, then click the **Add Static Entry** button.

Figure 69: DNS Host Name Mapping Configuration

Table 59: DNS Host Name Mapping Configuration Fields

<i>Field</i>	<i>Description</i>
Host Name	Enter the host name to assign to the static entry.
Inet Address	Enter the IP4 or IPv6 address associated with the host name.

- Click **Submit** to apply the new configuration and cause the change to take effect immediately. These changes will not be retained across a power cycle unless a Save is performed.
- Click **Back** to cancel and display the hostname IP mapping page to see the configured hostname-IP mapping entries.

DNS Host Name IP Mapping Summary

Use this page to configure static and dynamic DNS host names for hosts on the network. The host names are associated with IPv4 or IPv6 addresses on the network, which are assigned to particular hosts.

To access this page, click **LAN > Monitoring > DNS Server > Host Name IP Mapping Summary** in the navigation tree.

Figure 70: DNS Host Name IP Mapping Summary

Table 60: DNS Host Name IP Mapping Summary Fields

Field	Description
DNS Static Entries	
Host Name	The host name of the static entry.
Inet Address	The IP4 or IPv6 address of the static entry.
Remove	Select to remove a Host Name IP Mapping entry from the Host Name IP Mapping list.
DNS Dynamic Entries	
Host Name	The host name of the dynamic entry.
Total	The total time of the dynamic entry.
Elapsed	The elapsed time of the dynamic entry.
Type	The type of the dynamic entry.
Addresses	The IP4 or IPv6 address of the dynamic entry.
Remove	Select to remove a Host Name IP Mapping entry from the Host Name IP Mapping list.

- Click **Add Static Entry** to load the Host Name IP Mapping Configuration page in order to configure the Host Name IP Mapping entries.
- Click **Submit** to apply the new configuration and cause the change to take effect immediately. These changes will not be retained across a power cycle unless a Save is performed.
- Click **Clear Dynamic Entries** to remove all Host Name IP Mapping entries. A confirmation prompt will be displayed. Click the button to confirm removal and the Host Name IP Mapping dynamic entries are cleared.
- Click **Refresh** to refresh the page with the most current data from the switch.

Configuring and Viewing ISDP Information

The Industry Standard Discovery Protocol (ISDP) is a proprietary Layer 2 network protocol which inter-operates with Cisco® devices running the Cisco Discovery Protocol (CDP). ISDP is used to share information between neighboring devices. D-Link DWS-4000 Series switches participate in the CDP protocol and are able to both discover and be discovered by other CDP supporting devices.

Global Configuration

From the **ISDP Global Configuration** page, you can configure the ISDP settings for the switch, such as the administrative mode. To display the **ISDP Global Configuration** page, click **LAN > Administration > ISDP > Global Configuration** in the navigation tree.

Figure 71: ISDP Global Configuration

The following table describes the fields available on the ISDP **Global Configuration** page.

Table 61: ISDP Global Configuration

Field	Description
ISDP Mode	Use this field to enable or disable the Industry Standard Discovery Protocol on the switch.
ISDP V2 Mode	Use this field to enable or disable the Industry Standard Discovery Protocol v2 on the switch.
Message Interval	Specifies the ISDP transmit interval. The range is (5–254). Default value is 30 seconds.
Holdtime Interval	The receiving device holds ISDP message during this time period. The range is (10–255). Default value is 180 seconds.
Device ID	The Device ID advertised by this device. The format of this Device ID is characterized by the value of Device ID Format object.

Table 61: ISDP Global Configuration

Field	Description
Device ID Format Capability	<p>Indicates the Device ID format capability of the device.</p> <ul style="list-style-type: none"> serialNumber—Indicates that the device uses serial number as the format for its Device ID. macAddress—Indicates that the device uses layer 2 MAC address as the format for its Device ID. other—Indicates that the device uses its platform specific format as the format for its Device ID.
Device ID Format	<p>Indicates the Device ID format of the device.</p> <ul style="list-style-type: none"> serialNumber—Indicates that the value is in the form of an ASCII string containing the device serial number. macAddress—Indicates that the value is in the form of Layer 2 MAC address. other—Indicates that the value is in the form of a platform specific ASCII string containing info that identifies the device. For example: ASCII string contains serialNumber appended/prepended with system name.

Cache Table

From the **ISDP Cache Table** page, you can view information about other devices the switch has discovered through the ISDP. To access the **ISDP Cache Table** page, click **LAN > Monitoring > ISDP > Cache Table** in the navigation menu.

ISDP Cache Table									
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP, r - Repeater									
Device ID	Interface	IP Address	Version	Holdtime (secs)	Capability	Platform	Port ID	Protocol Version	Last Time Changed
SEP002584A31E4B	0/15	10.27.254.211	SCCP45.8-5-2S	176	H	Cisco IP Phone 7945	Port 2	2	17 Days 1h:15m:53s

Clear Refresh

Figure 72: ISDP Cache Table

The following table describes the fields available on the **ISDP Cache Table** page.

Table 62: ISDP Cache Table

Field	Description
Device ID	Displays the string with Device ID which is reported in the most recent ISDP message.
Interface	Displays the interface that this neighbor is attached to.
IP Address	The (first) network-layer address that is reported in the Address TLV of the most recently received ISDP message.
Version	Displays the Version string for the neighbor.

Table 62: ISDP Cache Table (Cont.)

Field	Description
Holdtime	Displays the ISDP holdtime for the neighbor.
Capability	Displays the ISDP Functional Capabilities for the neighbor.
Platform	Displays the ISDP Hardware Platform for the neighbor.
Port ID	Displays the ISDP port ID string for the neighbor.
Protocol Version	Displays the ISDP Protocol Version for the neighbor.
Last Time Changed	Displays when entry was last modified.

Interface Configuration

From the ISDP **Interface Configuration** page, you can configure the ISDP settings for each interface. To display the **ISDP Cache Table** page, click **LAN > Administration > ISDP > Interface Configuration** in the navigation tree.



Note: If ISDP is enabled on an interface, it must also be enabled globally in order for the interface to transmit ISDP packets. If the ISDP mode on the ISDP Global Configuration page is disabled, the interface will not transmit ISDP packets, regardless of the mode configured on the interface.

Figure 73: ISDP Interface Configuration

The following table describes the fields available on the ISDP **Interface Configuration** page.

Table 63: ISDP Interface Configuration

Field	Description
Slot/Port	Select the interface with the ISDP mode status to configure or view.
ISDP Mode	Use this field to enable or disable the Industry Standard Discovery Protocol on the selected interface.

Statistics

From the ISDP **Statistics** page, you can view information about the ISDP packets sent and received by the switch. To display the **ISDP Statistics** page, click **LAN > Monitoring > ISDP > Statistics** in the navigation tree.



ISDP Statistics	
Packets Received	26273
Packets Transmitted	131307
ISDPv1 Packets Received	1714
ISDPv1 Packets Transmitted	34649
ISDPv2 Packets Received	24559
ISDPv2 Packets Transmitted	96658
Bad Header	0
Checksum Error	0
Transmission Failure	0
Invalid Format Packets Received	0
Table Full	0
ISDP IP Address Table Full	0

Figure 74: ISDP Statistics

The following table describes the fields available on the ISDP **Statistics** page.

Table 64: ISDP Statistics

Field	Description
ISDP Packets Received	Displays the number of all ISDP protocol data units (PDUs) received.
ISDP Packets Transmitted	Displays the number of all ISDP PDUs transmitted.
ISDPv1 Packets Received	Displays the number of v1 ISDP PDUs received.
ISDPv1 Packets Transmitted	Displays the number of v1 ISDP PDUs transmitted.
ISDPv2 Packets Received	Displays the number of v2 ISDP PDUs received.
ISDPv2 Packets Transmitted	Displays the number of v2 ISDP PDUs transmitted.
ISDP Bad Header	Displays the number of ISDP PDUs that were received with bad headers.
ISDP Checksum Error	Displays the number of ISDP PDUs that were received with checksum errors.
ISDP Transmission Failure	Displays the number of ISDP PDUs transmission failures.
Invalid Format ISDP Packets Received	Displays the number of ISDP PDUs that were received with an invalid format.
Table Full	Displays the number of times the system tried to add an entry to the ISDP table but was unsuccessful because the table was full.
ISDP IP Address Table Full	Displays the number of times the system tried to add an entry to the ISDP IP Address table but was unsuccessful because the table was full.

Configuring sFlow

sFlow® is the standard for monitoring high-speed switched and routed networks. sFlow technology is built into network equipment and gives complete visibility into network activity, enabling effective management and control of network resources.

The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router or in a standalone probe) and a central sFlow Collector. The sFlow Agent uses sampling technology to capture traffic statistics from the device it is monitoring. sFlow datagrams are used to immediately forward the sampled traffic statistics to an sFlow Collector for analysis.

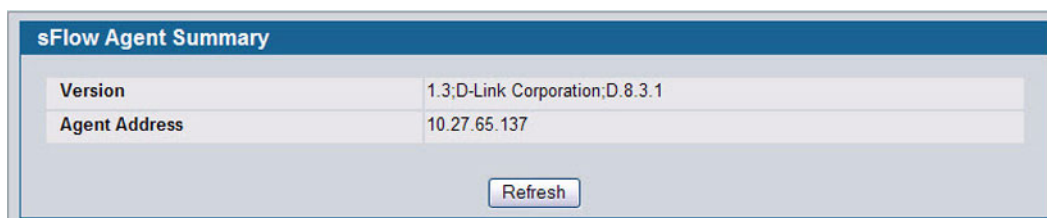
The sFlow Agent uses two forms of sampling: statistical packet-based sampling of switched or routed Packet Flows, and time-based sampling of counters.

sFlow Agent Summary

Packet Flow Sampling and Counter Sampling are performed by sFlow Instances associated with individual Data Sources within the sFlow Agent. Packet Flow Sampling and Counter Sampling are designed as part of an integrated system. Both types of samples are combined in sFlow datagrams. Packet Flow Sampling will cause a steady, but random, stream of sFlow datagrams to be sent to the sFlow Collector. Counter samples may be taken opportunistically in order to fill these datagrams.

In order to perform Packet Flow Sampling, an sFlow Sampler Instance is configured with a Sampling Rate. The Packet Flow sampling process results in the generation of Packet Flow Records. In order to perform Counter Sampling, the sFlow Poller Instance is configured with a Polling Interval, The Counter Sampling process results in the generation of Counter Records. The sFlow Agent collects Counter Records and Packet Flow Records and sends them in the form of sFlow datagrams to sFlow Collectors.

To access the sFlow Agent Summary page, click **LAN > Monitoring > sFlow > Agent Summary** in the navigation tree.



sFlow Agent Summary	
Version	1.3;D-Link Corporation;D.8.3.1
Agent Address	10.27.65.137

Figure 75: sFlow Agent Summary

Table 65: sFlow Agent Summary

Field	Description
Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version;Organization;Software Revision where: <ul style="list-style-type: none"> • MIB Version: '1.3', the version of this MIB. • Organization: D-Link Corporation • Revision: 1.0
Agent Address	The IP address associated with this agent.

- Use the **Refresh** button to refresh the page with the most current data from the switch.

sFlow Receiver Configuration

Use the sFlow Receiver Configuration page to configure the sFlow Receiver.

To access the sFlow Receiver Configuration page, click **LAN > Administration > sFlow > Receiver Configuration** in the navigation tree.

sFlow Receiver Configuration

Receiver Index 1 ▾

Receiver Owner String

Receiver Timeout (0 to 4294967295 secs)

Receiver Maximum Datagram Size (200 to 9116)

Receiver Address

Receiver Port (1 to 65535)

Receiver Datagram Version

Receiver Index	Receiver Owner	Timeout	Maximum Datagram Size	Address	Port	Datagram Version
1		0	1400	0.0.0.0	6343	5
2		0	1400	0.0.0.0	6343	5
3		0	1400	0.0.0.0	6343	5
4		0	1400	0.0.0.0	6343	5
5		0	1400	0.0.0.0	6343	5
6		0	1400	0.0.0.0	6343	5
7		0	1400	0.0.0.0	6343	5
8		0	1400	0.0.0.0	6343	5

Figure 76: sFlow Receiver Configuration

Table 66: sFlow Receiver Configuration

Field	Description
Receiver Index	Selects the receiver for which data is to be displayed or configured. The allowed range is 1 to 8.
Receiver Owner String	The entity making use of this sFlowRcvrTable entry. The empty string indicates that the entry is currently unclaimed and the receiver configuration is reset to the default values. An entity wishing to claim an sFlowRcvrTable entry must ensure that the entry is unclaimed before trying to claim it. The entry is claimed by setting the owner string. The entry must be claimed before any changes can be made to other sampler objects.
sFlow Receiver Timeout	The time (in seconds) remaining before the sampler is released and stops sampling. A management entity wanting to maintain control of the sampler is responsible for setting a new value before the old one expires. The allowed range is 0 to 4294967295 seconds. A value of zero sets the selected receiver configuration to its default values.
sFlow Receiver Maximum Datagram Size	The maximum number of data bytes that can be sent in a single sample datagram. The manager should set this value to avoid fragmentation of the sFlow datagrams. The default value is 1400. The allowed range is 200 to 9116.)
sFlow Receiver Address	The IP address of the sFlow collector. If set to 0.0.0.0 no sFlow datagrams will be sent.
sFlow Receiver Port	The destination port for sFlow datagrams. The allowed range is 1 to 65535).
Receiver Datagram Version	The version of sFlow datagrams that should be sent.

- Use the **Submit** button to sent updated data to the switch and cause the changes to take effect on the switch.
- Use the **Refresh** button to refresh the page with the most current data from the switch.

sFlow Poller Configuration

The sFlow agent collects time-based sampling of network interface statistics and sends them to the configured sFlow receivers. A data source configured to collect counter samples is called a poller.

Counter Sampling

The primary objective of Counter Sampling is to efficiently, periodically export counters associated with Data Sources. A maximum Sampling Interval is assigned to each sFlow instance associated with a Data Source.

Counter Sampling is accomplished as follows:

- The sFlow Agent keeps a list of counter sources being sampled. When a Packet Flow Sample is generated, the sFlow Agent examines the list and adds counters to the sample datagram, least recently sampled first. Counters are only added to the datagram if the sources are within a short period, i.e. five seconds, of failing to meet the required Sampling Interval. Periodically, i.e. every second, the sFlow Agent examines the list of counter sources and sends any counters that need to be sent to meet the sampling interval requirement.

To access the sFlow Poller Configuration page, click **LAN > Administration > sFlow > Poller Configuration** in the navigation tree.

Figure 77: sFlow Poller Configuration

Table 67: sFlow Poller Configuration

Field	Description
Poller DataSource	The sFlow Sampler Datasource for this flow sampler. This Agent will support Physical ports only.
Receiver Index	The sFlowReceiver for this sFlow Counter Poller. If set to zero, the poller configuration is set to the default and the poller is deleted. Only active receivers can be set. If a receiver expires, then all pollers associated with the receiver will also expire. The allowed range is 1 to 8.
Poller Interval	The maximum number of seconds between successive samples of the counters associated with this data source

- Click **Refresh** to refresh the page with the most current data from the switch.

sFlow Sampler Configuration

The sFlow Agent collects a statistical packet-based sampling of the switched flows and sends them to the configured receivers. A data source configured to collect flow samples is called a sampler.

Packet Flow Sampling

The Packet Flow Sampling mechanism carried out by each sFlow instance ensures that any packet observed at a Data Source has an equal chance of being sampled, irrespective of the Packet Flow(s) to which it belongs.

Packet Flow Sampling is accomplished as follows:

- When a packet arrives on an interface, the Network Device makes a filtering decision to determine whether the packet should be dropped.
- If the packet is not filtered (dropped), a destination interface is assigned by the switching/routing function.
- At this point, a decision is made on whether or not to sample the packet. The mechanism involves a counter that is decremented with each packet. When the counter reaches zero, a sample is taken. When a sample is taken, the counter that indicates how many packets to skip before taking the next sample is reset. The value of the counter is set to a random integer where the sequence of random integers used over time is the Sampling Rate.

To access the sFlow Sampler Configuration page, click **LAN > Administration > sFlow > Sampler Configuration** in the navigation tree.

Figure 78: sFlow Sampler Configuration

Table 68: sFlow Sampler Configuration

Field	Description
Sampler Datasource	The sFlow Datasource for this sFlow sampler. This Agent will support Physical ports only.
Receiver Index	The sFlow Receiver for this sFlow sampler. If set to zero, no packets will be sampled. Only active receivers can be set. If a receiver expires, then all samplers associated with the receiver will also expire. The allowed range is 1 to 8.
Sampling Rate	The statistical sampling rate for packet sampling from this source. A sampling rate of one (1) counts all packets. A sampling rate of zero (0) disables sampling. The allowed range is 1024 to 65536.
Maximum Header Size	The maximum number of bytes that should be copied from a sampled packet. The allowed range is 20 to 256.

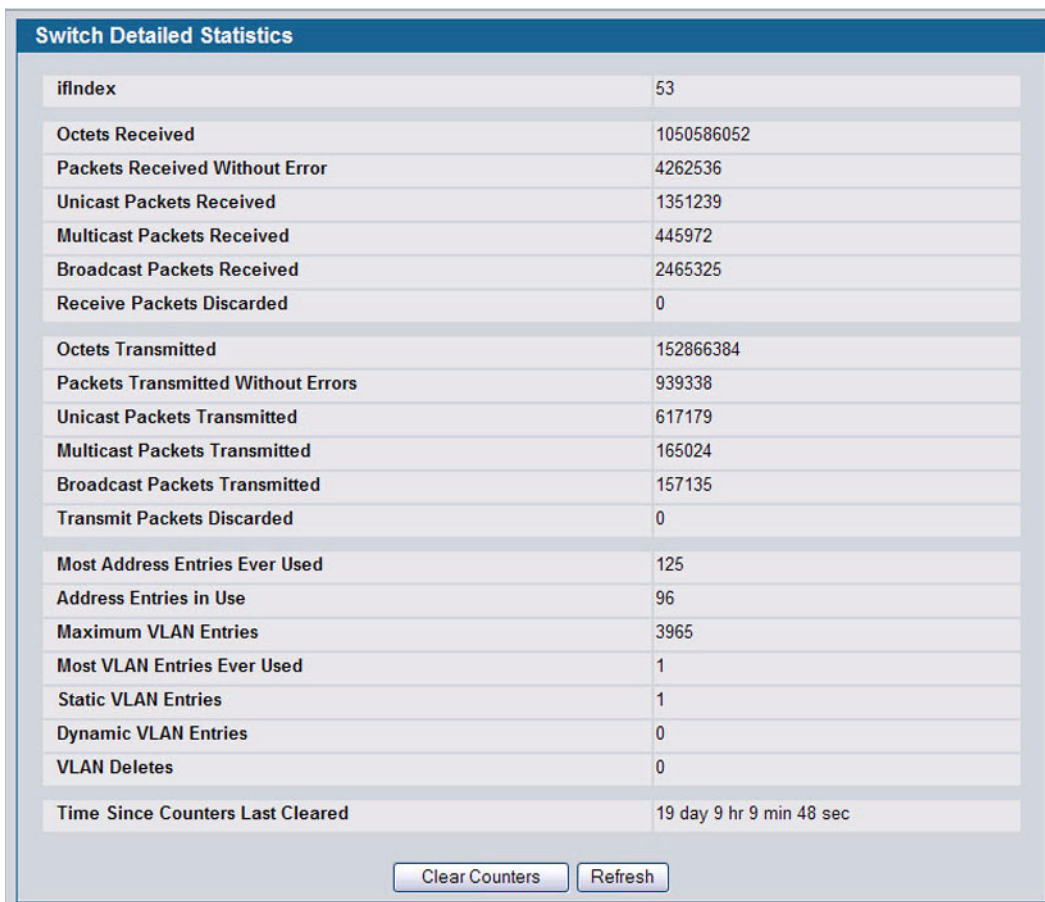
Viewing System Statistics

The pages in the Statistics folder contain a variety of information about the number and type of traffic transmitted from and received on the switch.

Switch Detailed

The Switch Detailed page shows detailed statistical information about the traffic the switch handles.

To access the Switch Detailed page, click **LAN > Monitoring > System Statistics > Switch Detail** in the navigation menu.



Switch Detailed Statistics	
ifIndex	53
Octets Received	1050586052
Packets Received Without Error	4262536
Unicast Packets Received	1351239
Multicast Packets Received	445972
Broadcast Packets Received	2465325
Receive Packets Discarded	0
Octets Transmitted	152866384
Packets Transmitted Without Errors	939338
Unicast Packets Transmitted	617179
Multicast Packets Transmitted	165024
Broadcast Packets Transmitted	157135
Transmit Packets Discarded	0
Most Address Entries Ever Used	125
Address Entries in Use	96
Maximum VLAN Entries	3965
Most VLAN Entries Ever Used	1
Static VLAN Entries	1
Dynamic VLAN Entries	0
VLAN Deletes	0
Time Since Counters Last Cleared	19 day 9 hr 9 min 48 sec

Clear Counters Refresh

Figure 79: Switch Detailed

Table 69: Switch Detailed Statistics Fields

Field	Description
Index	This object indicates the ifIndex of the interface table entry associated with the processor of this switch.
Octets Received	The total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Octets Transmitted	The total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.
Most Address Entries Ever Used	The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.
Address Entries in Use	The number of Learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	The maximum number of Virtual LANs (VLANs) allowed on this switch.
Most VLAN Entries Ever Used	The largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	The number of presently active VLAN entries on this switch that have been created statically.
Dynamic VLAN Entries	The number of presently active VLAN entries on this switch that have been created by GVRP registration.

Table 69: Switch Detailed Statistics Fields (Cont.)

Field	Description
VLAN Deletes	The number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

- Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.
- Click **Clear Counters** to clear all the statistics counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.

Switch Summary

Use the Switch Summary page to view a summary of statistics for traffic on the switch.

To access the Switch Summary page, click **LAN > Monitoring > System Statistics > Switch Summary** in the navigation tree.

Switch Summary Statistics	
ifIndex	53
Total Packets Received Without Errors	4263730
Broadcast Packets Received	2465894
Packets Received With Error	0
Packets Transmitted Without Errors	939602
Broadcast Packets Transmitted	157170
Transmit Packet Errors	0
Address Entries Currently in Use	91
VLAN Entries Currently in Use	1
Time Since Counters Last Cleared	19 day 9 hr 15 min 43 sec

Figure 80: Switch Summary**Table 70: Switch Summary Fields**

Field	Description
ifIndex	This object indicates the ifIndex of the interface table entry associated with the Processor of this switch.
Total Packets Received Without Errors	The total number of packets, including multicast packets, that were directed to the broadcast address.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Table 70: Switch Summary Fields (Cont.)

Field	Description
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently in Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently in Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

- Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.
- Click **Clear Counters** to clear all the statistics counters, resetting all summary and detailed statistics for this switch to default values. The discarded packets count cannot be cleared.
- Click **Clear All Counters** to clear counters for the switch.

Port Detailed

The Port Detailed page displays a variety of per-port traffic statistics.

To access the Port Detailed page, click **LAN > Monitoring > System Statistics > Port Detailed** in the navigation tree.

Figure 81 shows some, but not all, of the fields on the Port Detailed page.

Port Detailed Statistics	
Slot/Port	0/1
ifIndex	1
Media Type	1000Base-T
ARP Type	ARPA
Packets RX and TX 64 Octets	5409789
Packets RX and TX 65-127 Octets	4087381
Packets RX and TX 128-255 Octets	855586
Packets RX and TX 256-511 Octets	2677181
Packets RX and TX 512-1023 Octets	93294
Packets RX and TX 1024-1518 Octets	14210
Packets RX and TX 1519-1522 Octets	0
Packets RX and TX 1523-2047 Octets	0
Packets RX and TX 2048-4095 Octets	0
Packets RX and TX 4096-9216 Octets	0
Octets Received	1729650882
Packets Received 64 Octets	5102693
Packets Received 65-127 Octets	3964205
Packets Received 128-255 Octets	844451
Packets Received 256-511 Octets	2466109
Packets Received 512-1023 Octets	87790
Packets Received 1024-1518 Octets	1038
Packets Received > 1522 Octets	0
Total Packets Received Without Errors	12466286
Unicast Packets Received	760152
Multicast Packets Received	3939163

Figure 81: Port Detailed

Table 71: Detailed Port Statistics Fields

Field	Description
Slot/Port	Use the drop-down menu to select the interface for which data is to be displayed or configured.
ifIndex	This field indicates the ifIndex of the interface table entry associated with this port on an adapter.
Media Type	The type of physical medium for the Ethernet. The possible values are 10Base-T, 100Base-TX, 100Base-FX, 1000Base-X, 1000Base-T and 10GBase-X.
ARP Type	Encapsulation type for the network address. The value is always ARPA.
Packets RX and TX 64 Octets	The total number of packets (including bad packets) received or transmitted that were 64 octets in length (excluding framing bits but including FCS octets).

Table 71: Detailed Port Statistics Fields (Cont.)

Field	Description
Packets RX and TX 65-127 Octets	The total number of packets (including bad packets) received or transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 128-255 Octets	The total number of packets (including bad packets) received or transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 256-511 Octets	The total number of packets (including bad packets) received or transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 512-1023 Octets	The total number of packets (including bad packets) received or transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1024-1518 Octets	The total number of packets (including bad packets) received or transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1519-1522 Octets	The total number of packets (including bad packets) received or transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 1523-2047 Octets	The total number of packets (including bad packets) received or transmitted that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 2048-4095 Octets	The total number of packets (including bad packets) received or transmitted that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 4096-9216 Octets	The total number of packets (including bad packets) received or transmitted that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
Octets Received	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Received 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Received 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Table 71: Detailed Port Statistics Fields (Cont.)

Field	Description
Packets Received 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Received > 1522 Octets	The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Packets Received Successfully	
Total Packets Received Without Errors	The total number of packets received that were without errors.
Unicast Packets Received	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Received with MAC Errors	
Total Packets Received with MAC Errors	The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.
Fragments Received	The total number of packets received that were less than 64 octets in length with ERROR CRC (excluding framing bits but including FCS octets).
Undersize Received	The total number of packets received that were less than 64 octets in length with GOOD CRC (excluding framing bits but including FCS octets).
Alignment Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.
Rx FCS Errors	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Overruns	The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.
Total Ignored Frames	The total number of dropped packets including those that were aborted.
Total Deferred Frames	The total number of frames that could not be transmitted after multiple attempts because they encountered collisions.

Table 71: Detailed Port Statistics Fields (Cont.)

Field	Description
Received Packets Not Forwarded	
Total Received Packets Not Forwarded	A count of valid frames received which were discarded (i.e., filtered) by the forwarding process.
Local Traffic Frames	The total number of frames dropped in the forwarding process because the destination address was located off of this port.
802.3x Pause Frames Received	A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
Unacceptable Frame Type	The number of frames discarded from this port due to being an unacceptable frame type.
Multicast Tree Viable Discards	The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.
Reserved Address Discards	The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.
Broadcast Storm Recovery	The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.
CFI Discards	The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.
Upstream Threshold	The number of frames discarded due to lack of cell descriptors available for that packet's priority level.
Packets Transmitted Octets	
Total Packets Transmitted (Octets)	The total number of octets of data (including those in bad packets) transmitted on the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval.
Packets Transmitted 64 Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
Packets Transmitted 65-127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 128-255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 256-511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 512-1023 Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 1024-1518 Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Table 71: Detailed Port Statistics Fields (Cont.)

Field	Description
Maximum Frame Size	The maximum ethernet frame size the interface supports or is configured, including ethernet header, CRC, and payload. (1518 to 9216). The default maximum frame size is 1518.
Packets Transmitted Successfully	
Total Packets Transmitted Successfully	The number of frames that have been transmitted by this port to its segment.
Unicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Errors	
Total Transmit Errors	The sum of Single, Multiple, and Excessive Collisions.
Tx FCS Errors	The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets
Tx Oversized	The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per second at 10 Mb/s.
Underrun Errors	The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.
Transmit Discards	
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Total Output Packets Drops	The total number of Aged packets.
Single Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
Multiple Collision Frames	A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Late Collision Frames	Total number of collisions that occur after 512 bit collision window has passed.
Port Membership Discards	The number of frames discarded on egress for this port due to egress filtering being enabled.
Lost/No Carrier Frames	Loss of the carrier detection occurs when the carrier signal of the hardware is undetectable. It could be because the carrier signal was not present or was present but could not be detected. Each such event causes this counter to increase.

Table 71: Detailed Port Statistics Fields (Cont.)

Field	Description
Protocol Statistics	
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.
802.3x Pause Frames Transmitted	A count of MAC Control frames transmitted on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.
GVRP PDUs Received	The count of GVRP PDUs received in the GARP layer.
GVRP PDUs Transmitted	The count of GVRP PDUs transmitted from the GARP layer.
GVRP Failed Registrations	The number of times attempted GVRP registrations could not be completed.
GMRP PDUs Received	The count of GMRP PDUs received from the GARP layer.
GMRP PDUs Transmitted	The count of GMRP PDUs transmitted from the GARP layer.
GMRP Failed Registrations	The number of times attempted GMRP registrations could not be completed.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

- Click **Clear Counters** to clear all the counters. This resets all statistics for this port to the default values.
- Click **Clear All Counters** to clear all the counters for all ports on the switch. The button resets all statistics for all ports to default values.
- Click **Refresh** to refresh the data on the screen and display the most current statistics.

Port Summary Statistics

The **Port Summary Statistics** page shows a summary of per-port traffic statistics on the switch. To access the **Port Summary Statistics** page, click **LAN > Monitoring > System Statistics > Port Summary**.

Port Summary Statistics	
Slot/Port	0/1
ifIndex	1
Total Packets Received Without Errors	12473001
Packets Received With Error	0
Broadcast Packets Received	7770648
Packets Transmitted Without Errors	672603
Transmit Packet Errors	0
Collision Frames	0
Time Since Counters Last Cleared	20 day 2 hr 33 min 15 sec

Figure 82: Port Summary

Table 72: Port Summary Statistics Fields

Field	Description
Slot/Port	Use the drop-down menu to select the interface for which data is to be displayed or configured.
ifIndex	This field indicates the ifIndex of the interface table entry associated with this port on an adapter.
Total Packets Received Without Errors	The total number of packets received that were without errors.
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Packets Transmitted Without Errors	The number of frames that have been transmitted by this port to its segment.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Collision Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

- Click **Clear Counters** to clear all the counters. This resets all statistics for this port to the default values.
- Click **Clear All Counters** to clear all the counters for all ports on the switch. The button resets all statistics for all ports to default values.
- Click **Refresh** to refresh the data on the screen and display the most current statistics.

Section 3: Using System Tools

The Tools menu contains links to the following Web pages that help you perform switch maintenance:

- [“Reset Configuration to Defaults”](#)
- [“Reset Passwords to Defaults”](#)
- [“System Reset”](#)
- [“Save All Applied Changes”](#)
- [“Download File To Switch \(TFTP\)”](#)
- [“HTTP File Download”](#)
- [“Upload File From Switch \(TFTP\)”](#)
- [“Multiple Image Service”](#)
- [“Erase Startup-config File”](#)
- [“AutoInstall”](#)

Reset Configuration to Defaults

Use the Reset Configuration to Defaults page to reset the system configuration to the factory default values.



Note: By default, the switch IP address is 10.90.90.90 and the DHCP client is disabled. When you reset the system to its default values, the network IP address resets to 10.90.90.90. For information about configuring network information, see [“Connecting the Switch to the Network”](#) on page 43.

To access the Reset Configuration to Defaults page, click **Tool > Reset Configuration** in the navigation tree.

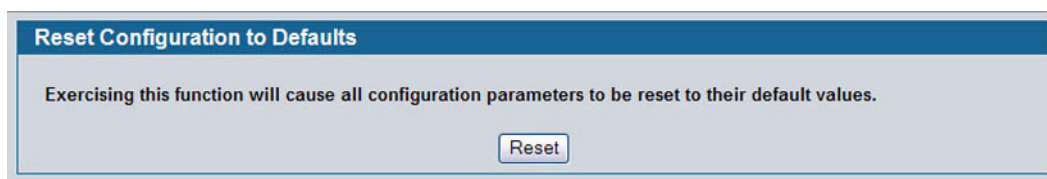


Figure 83: Reset Configuration to Defaults

- Click **Reset** to restore the factory default settings. The screen refreshes and asks you to confirm the reset. Click **Reset** again to complete the action.

Reset Passwords to Defaults

Use the Reset Passwords to Defaults page to reset the passwords for the default read/write (admin) and read-only (guest) users on the system. By default, the passwords are blank. If you have configured additional read-only users on your system, their passwords are not affected.

To access the Reset Passwords to Defaults page, click **Tool > Reset Password** in the navigation tree.

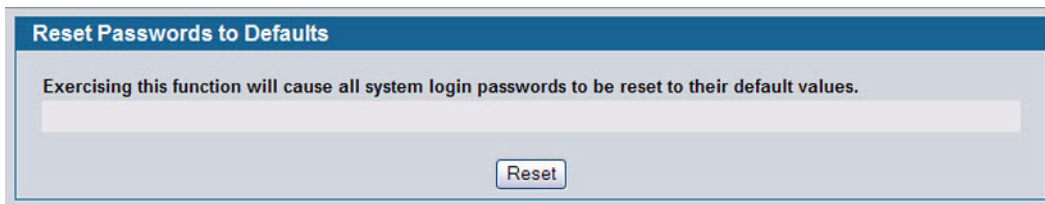


Figure 84: Reset Passwords to Defaults

- Click **Reset** to restore the passwords for the default users to the factory defaults.



Note: When the password for the read/write user (admin) changes, you must re-authenticate with the username and default password.

System Reset

Use the System Reset page to reboot the system.

To access the System Reset page, click **Tool > Reboot System** in the navigation tree.

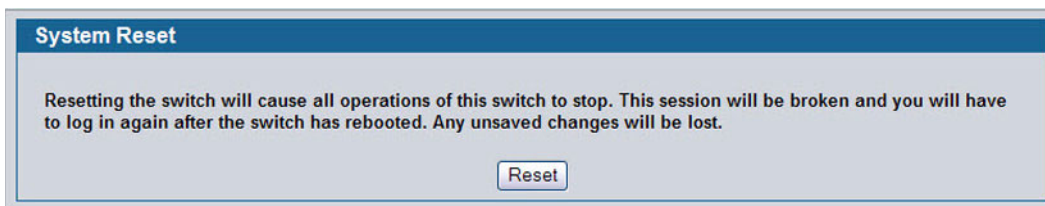


Figure 85: System Reset

- Click **Reset** to initiate the system reset. If you have not saved the changes that you submitted since the last system reset, the changes will not be applied to the system after the reset.

Save All Applied Changes

When you click Submit, the changes are applied to the system and saved in the running configuration file. However, these changes are not saved to non-volatile memory and will be lost if the system resets. Use the Save All Applied Changes page to make the changes you submit persist across a system reset.

To access the Save All Applied Changes page, click **Tool > Save Changes** in the navigation tree.

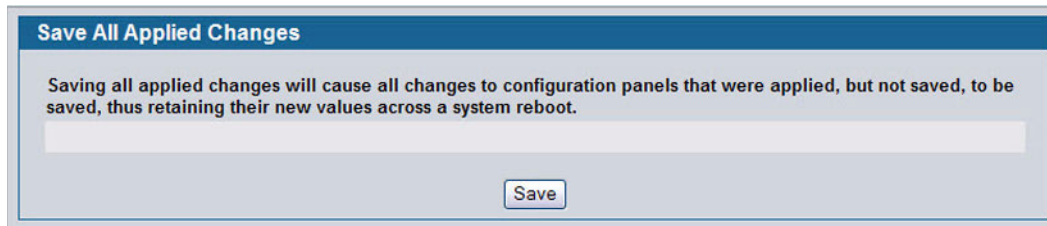


Figure 86: Save All Applied Changes

Click **Save** to save all changes applied to the system to NVRAM so that they are retained if the system reboots.

Download File To Switch (TFTP)

Use the Download File to Switch page to download the image file, the configuration files, CLI banner file, and SSH or SSL files from a TFTP server to the switch.

You can also download files via HTTP. See [“HTTP File Download” on page 170](#) for more information.

To access the Download File to Switch page, click **Tool > Download File** in the navigation tree.

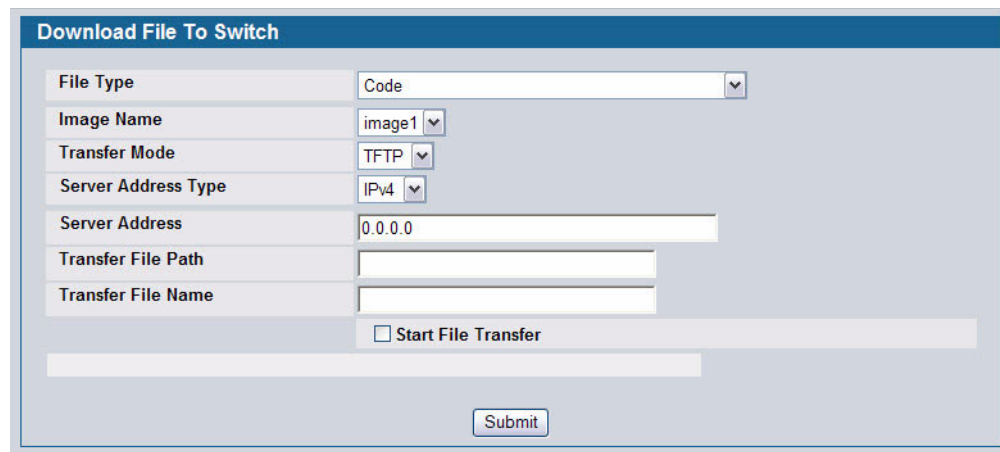


Figure 87: Download File to Switch

Table 73: Download File to Switch Fields

Field	Description
File Type	<p>Specify what type of file you want to download to the switch:</p> <ul style="list-style-type: none"> • CLI Banner: The CLI banner is the text that displays in the command-line interface before the login prompt. The CLI banner to download is a text file and displays when a user connects to the switch by using telnet, SSH, or a serial connection. • Code: The code is the system software image, which is saved in one of two flash sectors called images (image1 and image2). The active image stores the active copy; while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process. • Configuration: If you have a copy of a valid binary configuration file (fastpath.cfg) on a TFTP server, you can download it to the switch. • Text Configuration: A text-based configuration file enables you to edit a configured text file (startup-config) offline as needed without having to translate the contents for the D-Link software to understand. The most common usage of text-based configuration is to upload a working configuration from a device, edit it offline to personalize it for another similar device (i.e., change the device name, serial number, IP address, etc.), and download it to that device. • SSH-1 RSA Key File: SSH-1 Rivest-Shamir-Adleman (RSA) Key File. To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions. • SSH-2 RSA Key PEM File: SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded). To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions. • SSH-2 DSA Key PEM File: SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded). To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions. • SSL Trusted Root Certificate PEM File: SSL Trusted Root Certificate File (PEM Encoded). • SSL Server Certificate PEM File: SSL Server Certificate File (PEM Encoded). • SSL DH Weak Encryption Parameter PEM File: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded). • SSL DH Strong Encryption Parameter PEM File: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
Image Name	Specify the code image you want to download, either image1 or image2. This field is only visible when Code is selected as the File Type. The factory default is image1.
Transfer Mode	Specifies the protocol to be used for the transfer: TFTP, SFTP, or SCP.
TFTP Server Address Type	Specify either IPv4, IPv6, or DNS address to indicate the format of the TFTP Server Address field. The factory default is IPv4.
TFTP Server Address	Enter the IP address of the TFTP server in accordance with the format indicated by the TFTP Server Address Type. The factory default is the IPv4 address 0.0.0.0.
TFTP File Path	Enter the path on the TFTP server where the selected file is located. You may enter up to 32 characters. The factory default is blank.

Table 73: Download File to Switch Fields (Cont.)

Field	Description
TFTP File Name	Enter the name of the file you want to download from the TFTP server. You may enter up to 32 characters. The factory default is blank.
Start File Transfer	To initiate the download, check this box before clicking Submit .

Downloading a File to the Switch

Before you download a switch to the file, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.

Use the following procedures to download a file from a TFTP server to the switch.

1. From the **File Type** field, select the type of file to download.
2. If you are downloading a D-Link DWS-4000 Series image (Code), select the image on the switch to overwrite. If you are downloading another type of file, the **Image Name** field is not available.



Note: It is recommended that you not overwrite the active image.

3. Verify the IP address of the TFTP server and ensure that the software image or other file to be downloaded is available on the TFTP server.
4. Complete the **TFTP Server IP Address** and **TFTP File Name** (full path without TFTP server IP address) fields.
5. Click the Start File Transfer check box, and then click **Submit**.

After you click Submit, the screen refreshes and a “File transfer operation started” message appears. After the software is downloaded to the device, a message appears indicating that the file transfer operation completed successfully.

To activate a software image that you download to the switch, see [“Multiple Image Service” on page 172](#).

HTTP File Download

Use the HTTP File Download page to download files of various types to the switch using an HTTP session (i.e., via your web browser).

To display this page, click **Tool > HTTP File Download** in the navigation menu.

Figure 88: HTTP File Download

Table 74: HTTP File Download Fields

Field	Description
File Type	<p>Specify the type of file you want to download:</p> <ul style="list-style-type: none"> • Code: Choose this option to upgrade the operational software in flash (default). • Configuration: Choose this option to update the switch's configuration. If the file has errors the update will be stopped. • SSH-1 RSA Key File: SSH-1 Rivest-Shamir-Adleman (RSA) Key File • SSH-2 RSA Key PEM File: SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded) • SSH-2 DSA Key PEM File: SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded) • SSL Trusted Root Certificate PEM File: SSL Trusted Root Certificate File (PEM Encoded) • SSL Server Certificate PEM File: SSL Server Certificate File (PEM Encoded) • SSL DH Weak Encryption Parameter PEM File: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded) • SSL DH Strong Encryption Parameter PEM File: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded) • CLI Banner: Choose this option to download a banner file to be displayed before the login prompt appears. <p>Note: To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.</p>
Image Name	Specify the code image you want to download, either image1 (the default) or image2. This field is only visible when Code is selected as the File Type.
Select File	Enter the path and filename or browse for the file you want to download. You may enter up to 80 characters.

- Click the **Start File Transfer** button to initiate the file download.

Upload File From Switch (TFTP)

Use the Upload File from Switch page to upload configuration (ASCII) and image (binary) files from the switch to the TFTP server.

To display the Upload File from Switch page, click **Tool > Upload File** in the navigation tree.

The screenshot shows a web form titled "Upload File from Switch". It contains the following fields and controls:

- File Type:** A dropdown menu with "Error Log" selected.
- Transfer Mode:** A dropdown menu with "TFTP" selected.
- Server Address Type:** A dropdown menu with "IPv4" selected.
- Server Address:** A text input field containing "0.0.0.0".
- Transfer File Path:** An empty text input field.
- Transfer File Name:** An empty text input field.
- Start File Transfer:** A checkbox that is currently unchecked.
- Submit:** A button at the bottom right of the form.

Figure 89: Upload File from Switch

Table 75: Upload File from Switch Fields

Field	Description
File Type	Specify what type of file you want to upload: <ul style="list-style-type: none"> • CLI Banner: Retrieves the CLI banner file. • Code: Retrieves a stored code image. • Configuration: Retrieve the stored startup configuration (.cfg) and copy it to a TFTP server. • Text Configuration: Retrieves the text configuration file startup-config. • Error Log: Retrieves the system error (persistent) log, sometimes referred to as the event log. • Buffered Log: Retrieves the system buffered (in-memory) log. • Trap Log: Retrieves the system trap records.
Image Name	Specify the code image to upload, either image1 or image2. This field is only visible when Code is selected as the File Type. The factory default is image1.
TFTP Server Address Type	Specify either IPv4 or IPv6 address to indicate the format of the TFTP Server Address field. The factory default is IPv4.
TFTP Server Address	Enter the IP address of the TFTP server in accordance with the format indicated by the TFTP Server Address Type. The factory default is the IPv4 address 0.0.0.0.
TFTP File Path	Enter the path on the TFTP server where you want to put the file. You may enter up to 32 characters. The factory default is blank.

Table 75: Upload File from Switch Fields (Cont.)

Field	Description
TFTP File Name	Enter a destination file name for the file to upload. You may enter up to 32 characters. The factory default is blank.
Start File Transfer	To initiate the file upload, check this box before clicking Submit .

Uploading Files

Use the following procedures to upload a file from a TFTP server to the switch.

1. From the **File Type** field, select the type of file to copy from the switch to the TFTP server.
2. If you are uploading a D-Link DWS-4000 Series image (Code), select the image on the switch to upload. If you are uploading another type of file, the **Image Name** field is not available.
3. Complete the **TFTP Server Address Type**, **TFTP Server IP Address**, and **TFTP File Name** (full path without TFTP server IP address) fields.
4. Click the **Start File Transfer** check box, and then click **Submit**.
After you click **Submit**, the screen refreshes and a "File transfer operation started" message appears. After the software is downloaded to the device, a message appears indicating that the file transfer operation completed successfully.

Multiple Image Service

The system maintains two versions of the D-Link DWS-4000 Series software in permanent storage. One image is the active image, and the second image is the backup image. The active image is loaded during subsequent switch restarts. This feature reduces switch down time when upgrading/downgrading the D-Link DWS-4000 Series software.

The system running an older software version will ignore (not load) a configuration file created by the newer software version. When a configuration file created by the newer software version is discovered by the system running an older version of the software, the system will display an appropriate warning to the user.

Use the Multiple Image Service page to set the boot image.

To display the **Multiple Image Service** page, click **Tool > Multiple Image Service** in the navigation menu.

Figure 90: Multiple Image Service

The Active Image page contains the following fields:

Table 76: Multiple Image Service Fields

Field	Description
Image Name	Select Image1 or Image2 from the menu to activate on the next reload or to be deleted.
Current-active	Displays name of current active image.
Next-active	Displays the name of the image that is set to be active the next time the switch reloads.
Image Description	If desired, enter a descriptive name for the respective Image1 or Image2 software images.

- Click **Activate** to make the image that is selected in the **Image Name** field the next active image for subsequent reboots.



Note: After activating an image, you must perform a system reset of the switch in order to run the new code.

- Click **Delete** to remove the selected image from permanent storage on the switch. You cannot delete the active image.
- Click **Change** to update the image description on the switch.
- If the file you uploaded contains the boot loader code only, click **Update Bootcode**.

Viewing the Dual Image Status

The Dual Image feature allows the switch to have two D-Link DWS-4000 Series software images in the permanent storage. One image is the active image, and the second image is the backup. This feature reduces the system down-time during upgrades and downgrades. You can use the Dual Image Status page to view information about the system images on the device.

To display the Dual Image Status page, click **LAN > Monitoring > Dual Image Status** in the navigation menu.

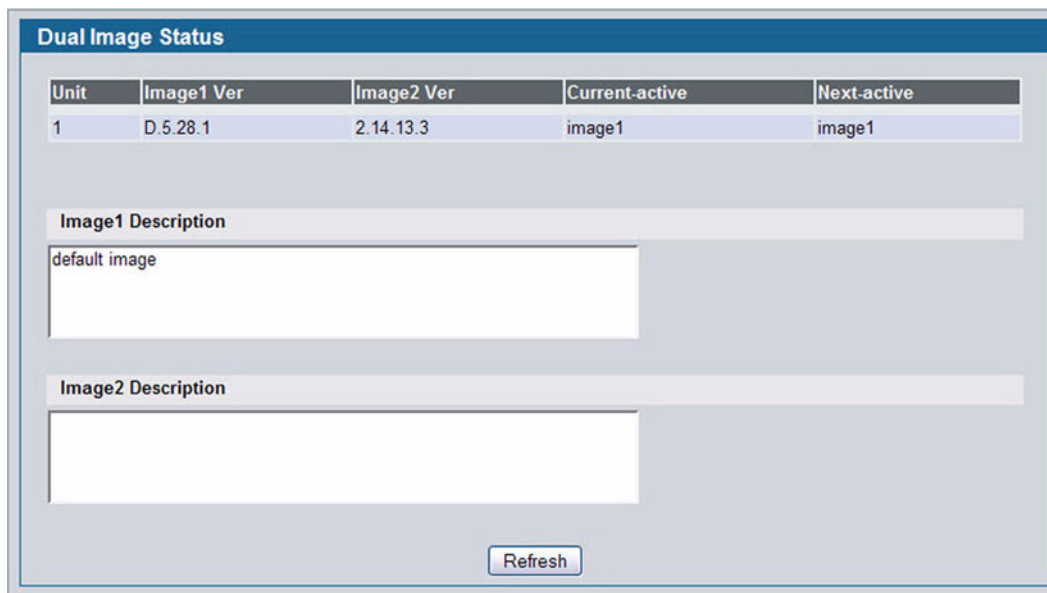


Figure 91: Dual Image Status

Table 77: Dual Image Status Fields

Field	Description
Unit	Displays the unit ID of the switch.
Image1 Ver	Displays the version of the image1 code file.
Image2 Ver	Displays the version of the image2 code file.
Current-active	Displays the currently active image on this unit.
Next-active	Displays the image to be used on the next restart of this unit.
Image1 Description	Displays the description associated with the image1 code file.
Image2 Description	Displays the description associated with the image2 code file.

- Click **Refresh** to display the latest information from the router.

Erase Startup-config File

Use the Erase Startup-config File to erase the startup-configuration file.

To display this page, click **Tool > Erase Startup-config File** in the navigation menu.

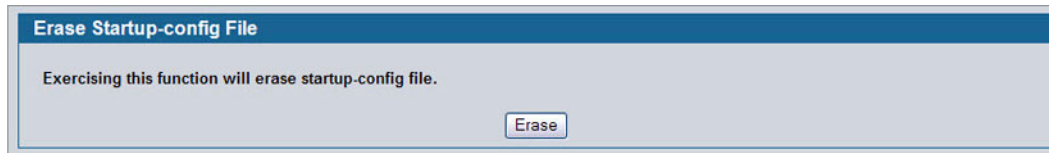


Figure 92: Erase Startup-config File

AutoInstall

The AutoInstall feature enables the configuration of a switch automatically when the device is turned on and, during the boot process, no configuration file is found in device storage. By communicating with a DHCP server, AutoInstall obtains an IP address for the switch and an IP address for a TFTP server. AutoInstall attempts to download a configuration file from the TFTP server and install it on the switch.

After obtaining IP addresses for both the switch and the TFTP server, the AutoInstall feature attempts to download a host-specific configuration file using the boot file name specified by the DHCP server. If the switch fails to obtain the file, it will retry indefinitely.

To display this page, click **Tool > AutoInstall** in the navigation menu.

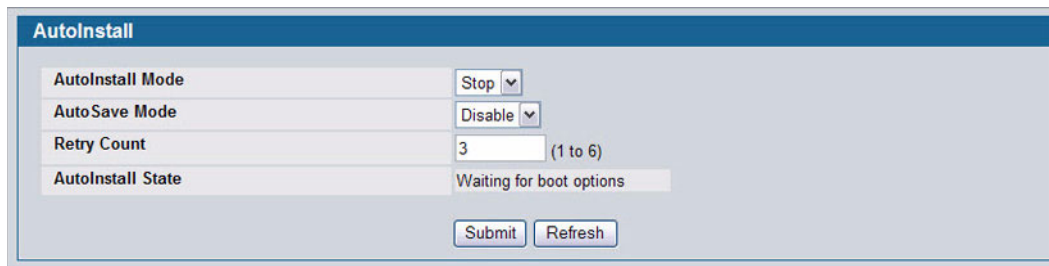


Figure 93: AutoInstall

Table 78: AutoInstall Fields

Field	Description
AutoInstall Mode	<ul style="list-style-type: none">• Select Start to initiate sending a request to a DHCP server to obtain an IP address of a server and the configuration file name. If it obtains the server address, AutoInstall proceeds to search for and download a configuration file from the server. If successful, it applies the configuration file to the switch. After starting the AutoInstall process, you can monitor the status of the process by the messages in the AutoInstall State and Retry Count fields.• Click Stop to end the process.
AutoSave Mode	Enable or Disable saving the network configuration to non-volatile memory. When enabled, the configuration is saved after downloading from the TFTP server without operator intervention. When disabled, the operator must explicitly save the configuration, if needed.
Retry Count	The number of times the switch has attempted to contact the TFTP server during the current AutoInstall session.
AutoInstall State	The status of the current or most recently completed AutoInstall session.

Click **Submit** to update the switch with the values on the window. Click Refresh to update the information on the window.

Section 4: Configuring L2 Features

Use the pages in the L2 Features navigation tree folder to configure the Layer 2 switching features available on the D-Link DWS-4000 Series switch. The **L2 Features** folder contains links to the following features:

- [“Configuring and Searching the Forwarding Database”](#)
- [“Managing VLANs”](#)
- [“Configuring Protected Ports”](#)
- [“Creating MAC Filters”](#)
- [“Configuring GARP”](#)
- [“Creating Port Channels \(Trunking\)”](#)
- [“Configuring IGMP Snooping”](#)
- [“Configuring IGMP Snooping Queriers”](#)
- [“Configuring MLD Snooping”](#)
- [“Configuring MLD Snooping Queriers”](#)
- [“Viewing Multicast Forwarding Database Information”](#)
- [“Configuring Spanning Tree Protocol”](#)
- [“Configuring DHCP Snooping”](#)
- [“Managing LLDP”](#)
- [“Configuring Dynamic ARP Inspection”](#)

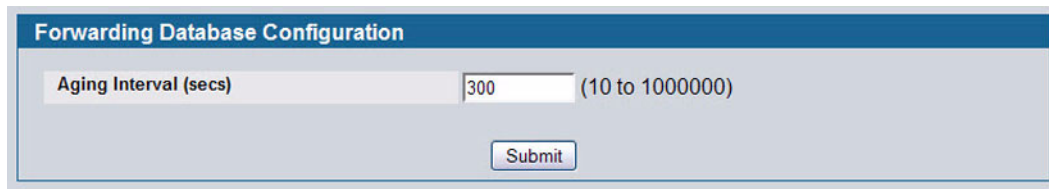
Configuring and Searching the Forwarding Database

The forwarding database maintains a list of MAC addresses after having received a packet from this MAC address. The transparent bridging function uses the forwarding database entries to determine how to forward a received frame.

Configuration

Use the Configuration page to set the amount of time to keep a learned MAC address entry in the forwarding database. The forwarding database contains static entries, which are never aged out, and dynamically learned entries, which are removed if they are not updated within a given time.

To access the Configuration page, click **LAN > L2 Features > Forwarding DB Configuration** in the navigation tree.



The screenshot shows a web interface titled "Forwarding Database Configuration". It features a text input field labeled "Aging Interval (secs)" with the value "300" entered. To the right of the input field, the range "(10 to 1000000)" is displayed. Below the input field is a "Submit" button.

Figure 94: Forwarding Database Age-Out Interval



Note: IEEE 802.1D recommends a default of 300 seconds, which is the factory default.

- Click **Submit** to apply the changes to the system. You must perform a save to make the changes persist across a reboot.

MAC Address Table

Use the MAC Address Table page to display information about entries in the forwarding database.

To access the page, click **LAN > Monitoring > MAC Address Table** in the navigation tree.

MAC address	Source Slot/Port(s)	ifIndex	Status
00:01:00:02:BC:00:17:D0	0/1	1	Learned
00:01:00:02:E3:4B:4F:6A	0/1	1	Learned
00:01:00:06:1B:D4:02:2D	0/1	1	Learned
00:01:00:06:29:32:81:40	0/1	1	Learned
00:01:00:06:29:56:65:80	0/1	1	Learned

Figure 95: Forwarding Database Search

Table 79: Forwarding Database Search Fields

Field	Description
Filter	Specify the type of entries to display. When you select a filter from the menu, the screen refreshes and displays the entries based on the filter you select, which can be one of the following: <ul style="list-style-type: none"> • Learned: If you select Learned, only MAC addresses that have been learned are displayed. • All: If you select All, the entire table is displayed.
MAC Address Search	This field allows you to search for an individual MAC address in the forwarding database table.
MAC Address	A unicast MAC address for which the switch has forwarding and/or filtering information. The format is a two byte hexadecimal VLAN ID number followed by a six byte MAC address with each byte separated by colons. For example: 01:23:45:67:89:AB:CD:EF, where 01:23 is the VLAN ID and 45:67:89:AB:CD:EF is the MAC address.
Source Slot/Port(s)	The port where this address was learned. In other words, this field shows the port through which the MAC address can be reached.
ifIndex	The ifIndex of the MIB interface table entry associated with the source port.
Status	The status of this entry. The possible values are: <ul style="list-style-type: none"> • Static: The entry was added when a static MAC filter was defined. • Learned: The entry was learned by observing the source MAC addresses of incoming traffic, and is currently in use. • Management: The system MAC address, which is identified with interface 0.1. • Self: The MAC address of one of the switch's physical interfaces.

Searching the Forwarding Database

Use the following procedures to search the forwarding database.

1. Enter the two-byte hexadecimal VLAN ID followed by the six byte hexadecimal MAC address in two-digit groups separated by colons.

For example, 01:23:45:67:89:AB:CD:EF where 01:23 is the VLAN ID and 45:67:89:AB:CD:EF is the MAC address.

2. Click **Search**.

If the address exists, that entry is displayed as the first entry in the table after the screen refreshes. The entry is followed by the remaining (greater) MAC addresses. An exact match is required. If you click **Refresh**, the MAC addresses with lower values are displayed again. fake

Managing VLANs

Adding Virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast, and like a router, it partitions the network into logical segments, which provides better administration, security and management of multicast traffic.

A VLAN is a set of end stations and the switch ports that connect them. You may have many reasons for the logical division, such as department or project membership. The only physical requirement is that the end station and the port to which it is connected both belong to the same VLAN.

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station may omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet may either reject it or insert a tag using its default VLAN ID. A given port may handle traffic for more than one VLAN, but it can only support one default VLAN ID.

VLAN Configuration

Use the VLAN Configuration page to define VLAN groups stored in the VLAN membership table. Your switch supports up to 3965 VLANs. VLAN 1 is the default VLAN of which all ports are members.

To display the VLAN Configuration page, click **LAN > L2 Features > VLAN > Configuration** in the navigation tree.

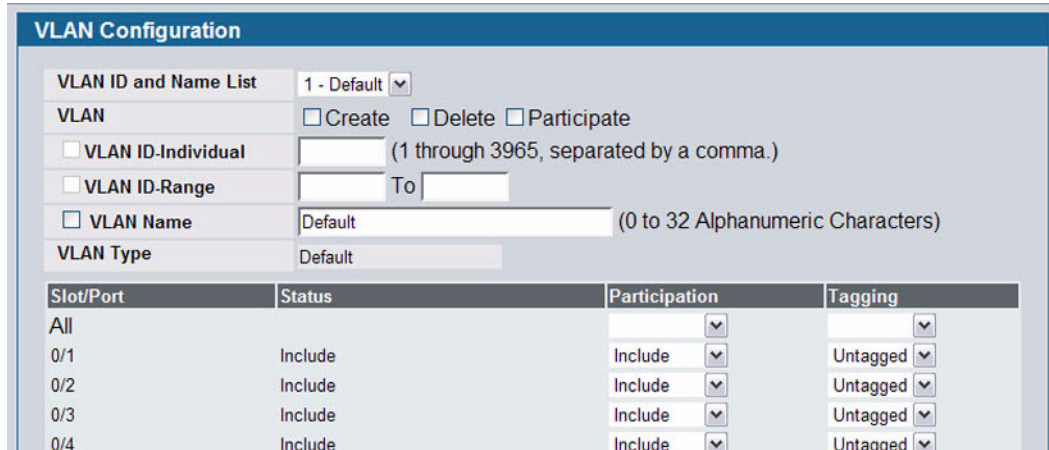


Figure 96: VLAN Configuration

Table 80: VLAN Configuration Fields

Field	Description
VLAN ID and Name	You can use this screen to reconfigure an existing VLAN, or to create a new one. Use this pulldown menu to select one of the existing VLANs, or select Create to add a new one.
VLAN ID-Individual	Specify the VLAN Identifier for the new VLAN. (You can only enter data in this field when you are creating a new VLAN.) The range of the VLAN ID is (1 to 3965).
VLAN ID-Range	Specify the range of VLAN Identifiers for the new VLANs to be created.
VLAN Name	Use this optional field to specify a name for the VLAN. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 is always named "Default."
VLAN Type	This field identifies the type of the VLAN you are configuring. You cannot change the type of the default VLAN (VLAN ID = 1): it is always type "Default." When you create a VLAN, using this screen, its type will always be "Static." A VLAN that is created by GVRP registration initially has a type of "Dynamic." You can use this pulldown menu to change its type to "Static."
Slot/Port	Indicates which port is associated with the fields on this line.
Status	Indicates the current value of the participation parameter for the port.
Participation	Use this field to specify whether a port will participate in this VLAN. The factory default is "Autodetect." The possible values are: <ul style="list-style-type: none"> • Include: This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • Exclude: This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • Autodetect: Specifies that port may be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless it receives a GVRP request. This is equivalent to registration normal in the IEEE 802.1Q standard.

Table 80: VLAN Configuration Fields (Cont.)

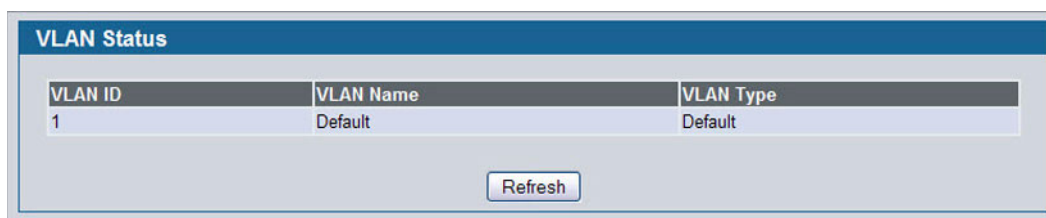
Field	Description
Tagging	Select the tagging behavior for this port in this VLAN. The factory default is "Untagged." The possible values are: <ul style="list-style-type: none"> • Tagged: all frames transmitted for this VLAN will be tagged. • Untagged: all frames transmitted for this VLAN will be untagged.

- If you make any changes to the page, click **Submit** to apply the changes to the system. To delete a VLAN, select the VLAN from the **VLAN ID and Name** field, and then click **Delete**. You cannot delete the default VLAN.

VLAN Status

Use the VLAN Status page to view information about the VLANs configured on your system.

To access the VLAN Status page, click **LAN > Monitoring > VLAN Summary > VLAN Status** in the navigation tree.

**Figure 97: VLAN Status****Table 81: VLAN Status Fields**

Field	Description
VLAN ID	The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 3965.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named Default.
VLAN Type	The VLAN type, which can be one of the following: <ul style="list-style-type: none"> • Default: (VLAN ID = 1) -- always present • Static: A VLAN you have configured • Dynamic: A VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore remove

- Click **Refresh** to display the latest information from the router.

VLAN Port Configuration

Use the VLAN Port Configuration page to configure a virtual LAN on a port.

To access the VLAN Port Configuration page, click **LAN > L2 Features > VLAN > Port Configuration** in the navigation tree.

Figure 98: VLAN Port Configuration

Table 82: VLAN Port Configuration Fields

Field	Description
Slot/Port	Select the physical interface for which you want to display or configure data. Select All to set the parameters for all ports to same values.
Port VLAN ID	Specify the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The factory default is 1.
Acceptable Frame Types	Specify how you want the port to handle untagged and priority tagged frames. Whichever you select, VLAN tagged frames will be forwarded in accordance with the IEEE 802.1Q VLAN standard. The factory default is Admit All. <ul style="list-style-type: none"> • VLAN Only: The port will discard any untagged or priority tagged frames it receives. • Admit All: Untagged and priority tagged frames received on the port will be accepted and assigned the value of the Port VLAN ID for this port.
Ingress Filtering	Specify how you want the port to handle tagged frames: <ul style="list-style-type: none"> • Enable: A tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. • Disable: All tagged frames will be accepted. The factory default is disable.
Port Priority	Specify the default 802.1p priority assigned to untagged packets arriving at the port.

- If you change any information on the page, click **Submit** to apply the changes to the system.

VLAN Port Summary

Use the VLAN Port Summary page to view VLAN configuration information for all the ports on the system.

To access the VLAN Port Summary page, click **LAN > Monitoring > VLAN Summary > VLAN Port Summary** in the navigation menu.



VLAN Port Summary						
Listing of all Ports on the Switch						
Slot/Port	Port VLAN ID Configured	Port VLAN ID Current	Acceptable Frame Types	Ingress Filtering Configured	Ingress Filtering Current	Port Priority
0/1	1	1	Admit All	Disabled	Disabled	0
0/2	1	1	Admit All	Disabled	Disabled	0
0/3	1	1	Admit All	Disabled	Disabled	0
0/4	1	1	Admit All	Disabled	Disabled	0
0/5	1	1	Admit All	Disabled	Disabled	0

Figure 99: VLAN Port Summary

Table 83: VLAN Port Summary Fields

Field	Description
Slot/Port	Identifies the physical interface associated with the rest of the data in the row.
Port VLAN ID Configured	Identifies the VLAN ID assigned to untagged or priority-tagged frames received on this port. The factory default is 1.
Port VLAN ID Current	Displays the actual VLAN ID in use for the port. If the port was acquired by another module, the actual value may differ from the configured VLAN ID. For example, if the port is a member of a port channel and the port channel has a different port VLAN ID setting than the configured value, then the two may differ.
Acceptable Frame Types	Indicates how the port handles untagged and priority tagged frames. <ul style="list-style-type: none"> VLAN Only: The port discards any untagged or priority tagged frames it receives. Admit All: Untagged and priority tagged frames received on the port are accepted and assigned the value of the Port VLAN ID for this port.
Ingress Filtering	Shows how the port handles tagged frames. <ul style="list-style-type: none"> Enable: A tagged frame is discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. Disable: All tagged frames are accepted, which is the factory default.
Port Priority	Identifies the default 802.1p priority assigned to untagged packets arriving at the port.

- Click **Refresh** to reload the page and view the most current information.

Managing Protocol-Based VLANs

In a protocol-based VLAN, traffic is bridged through specified ports based on the protocol associated with the VLAN. User-defined packet filters determine whether a particular packet belongs to a particular VLAN. Protocol-based VLANs are most often used in situations where network segments contain hosts running multiple protocols.

You can use a protocol-based VLAN to define filtering criteria for untagged packets. By default, if you do not configure any port-based (IEEE 802.1Q) or protocol-based VLANs, untagged packets are assigned to VLAN 1. You can override this behavior by defining either port-based VLANs, protocol-based VLANs, or both. Tagged packets are always handled according to the IEEE 802.1Q standard and are not included in protocol-based VLANs.

If you assign a port to a protocol-based VLAN for a specific protocol, untagged frames received on that port for that protocol will be assigned the protocol-based VLAN ID. Untagged frames received on the port for other protocols will be assigned the Port VLAN ID (PVID), which is either the default PVID (1) or a PVID you have specifically assigned to the port using the Port VLAN Configuration screen.

Use the Protocol-based VLAN Configuration page to configure which protocols go to which VLANs, and then enable certain ports to use these settings.

You define a protocol-based VLAN by creating a group. Each group has a one-to-one relationship with a VLAN ID, can include one or more protocol definitions, and can include multiple ports.

To display the Protocol-Based VLAN Configuration page, click **LAN > L2 Features > VLAN > Protocol-based VLAN > Configuration** in the navigation tree.

Figure 100: Create Protocol Group

Table 84: Protocol Group Fields (No Groups)

<i>Field</i>	<i>Description</i>
Group	When no protocol-based VLAN groups exist, only the Create New Group option is available.
Group ID	Specify a number to identify the group to create.

To create and configure a protocol group, enter a group ID and click **Submit**. The page refreshes and additional fields appear.

The screenshot shows a web-based configuration window titled "Protocol-based VLAN Configuration". It contains several input fields and a list of interfaces. The "Group ID" field is a dropdown menu currently showing "1" with a note "(Max 128 groups)". Below it, another "Group ID" field shows the value "1". The "Group Name (Optional)" field is empty with a note "(1 to 16 alphanumeric characters including -, _ ' ")". The "VLAN" field is empty with a note "(1 to 4093) Enter 0 to unconfigure". The "Protocol-list" field is empty with a note "0x0600(1536) to 0xFFFF(65535)". The "Interface(s)" field is a list box containing "0/1", "0/2", "0/3", "0/4", "0/5", "0/6", "0/7", and "0/8". At the bottom of the form are two buttons: "Submit" and "Delete".

Figure 101: Protocol Group

Table 85: Protocol Group Fields

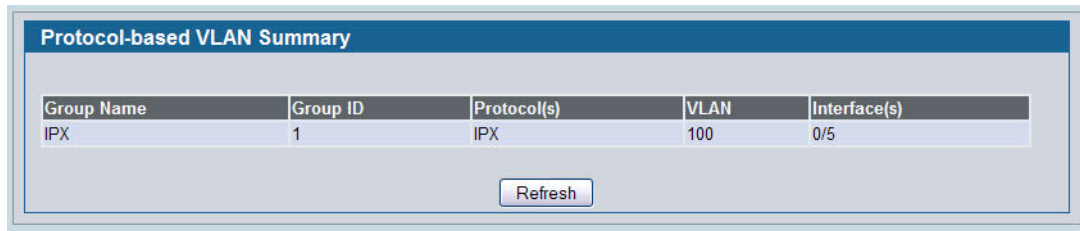
Field	Description
Group ID	Use the drop-down menu to create a new group or to configure the selected protocol group. You can create up to 128 groups.
Group ID	Identifies the group to configure.
Group Name	Optionally enter a name to associate with protocol group ID. You can modify the name of an existing group. You can enter up to 16 characters.
VLAN	Specify the VLAN ID to associate with this group. The range is 1-3965.
Protocol-list	Specify one or more protocols to associate with this group. The protocol list can be any valid comma(,) separated string with standard <i>arp</i> , <i>ip</i> , <i>ipx</i> keywords, hexadecimal or decimal values in the range of 0x0600(1536) to 0xFFFF(65535).
Interfaces	Selects the interface(s) to add or remove from this group. CTRL + click to select multiple ports.

- To create or modify a protocol-based VLAN group, edit the fields, and then click **Submit**.
- To delete an existing protocol-based VLAN group, select the group from the **Group ID** field, and then click **Delete Group**.

Protocol-Based VLAN Summary

Use the Protocol-based VLAN Summary page to view information about protocol-based VLAN groups configured on the system.

To access the Protocol-based VLAN Summary page, click **LAN > Monitoring > VLAN Summary > Protocol-based VLAN Port Summary** in the navigation tree.



Protocol-based VLAN Summary				
Group Name	Group ID	Protocol(s)	VLAN	Interface(s)
IPX	1	IPX	100	0/5

Figure 102: Protocol-based VLAN Summary

Table 86: Protocol-based VLAN Summary Fields

<i>Field</i>	<i>Description</i>
Group Name	Shows the user-defined name associated with protocol group.
Group ID	Shows the number that identifies the group you create. Group IDs are automatically assigned when you create a group.
Protocols	Shows the protocol keyword or protocol value (hex or decimal numbers) to associate with this group, which can be one or more of the following:
VLAN	Specifies the VLAN ID associated with this group.
Interface	Shows the interfaces participating in this group.

- Click **Refresh** to reload the page and display the most current information.

Managing IP Subnet-Based VLANs

If a packet is untagged or priority- tagged, the device associates the packet with any matching IP subnet classification. If no IP subnet classification can be made, then the packet is subjected to the normal VLAN classification rules of the device. An IP subnet-to-VLAN mapping is defined by configuring an entry in the IP subnet-to-VLAN table. An entry is specified by a source IP address, network mask, and the desired VLAN ID. The IP subnet-to-VLAN configurations are shared across all ports of the switch.

Use the IP Subnet-based VLAN Configuration page to assign an IP Subnet to a VLAN.

To display the IP Subnet-based VLAN Configuration page, click **LAN > L2 Features > VLAN > IP Subnet-based VLAN > Configuration** in the navigation menu.

Figure 103: IP Subnet-based VLAN Configuration

Table 87: IP Subnet-based VLAN Configuration Fields

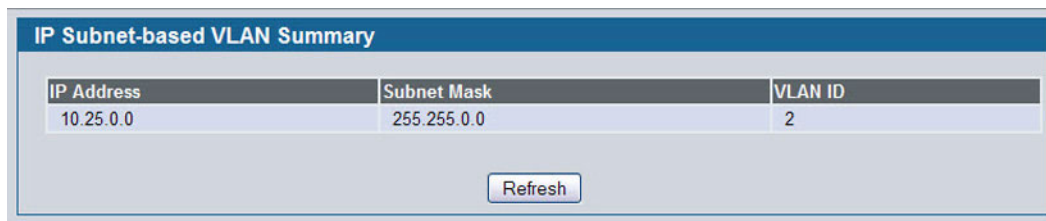
<i>Field</i>	<i>Description</i>
IP Address	Select the IP address of the IP-to-VLAN binding to view or delete, or select Add to create a new binding.
IP Address	Specifies packet source IP address. This field is configurable only when you create a new IP Subnet-based VLAN. Enter the IP address in dotted decimal notation.
Subnet Mask	Specifies packet source IP subnet mask address. This field is configurable only when you create a new IP Subnet-based VLAN. Enter the subnet mask in dotted decimal notation.
VLAN ID	Specifies the VLAN to which the IP address is assigned. The valid range is 1-3965.

- If you make any changes on this page, click **Submit** to apply the changes to the system.
- To delete an existing binding, select the source IP address from the **IP Address** drop-down menu, and then click **Delete**.

IP Subnet-based VLAN Summary

Use the IP Subnet-based VLAN Summary page to view information about IP subnet to VLAN mappings configured on your system. If no mappings are configured, the screen displays a “No IP Subnet-based VLAN Configured” message.

To access the IP Subnet-based VLAN Summary page, click **LAN > Monitoring > VLAN Summary > IP Subnet-based VLAN Summary** in the navigation tree.



IP Subnet-based VLAN Summary		
IP Address	Subnet Mask	VLAN ID
10.25.0.0	255.255.0.0	2

Figure 104: IP Subnet-based VLAN Summary

Table 88: IP Subnet-based VLAN Summary Fields

<i>Field</i>	<i>Description</i>
IP Address	Shows the packet source IP address.
Subnet Mask	Shows packet source IP subnet mask address.
VLAN ID	Shows the VLAN to which the IP address is assigned.

- Click **Refresh** to reload the page and display the most current information.

MAC-based VLAN Configuration

If a packet is untagged or priority tagged, the device shall associate it with the VLAN which corresponds to the source MAC address in its MAC-based VLAN tables. If there is no matching entry in the table, then the packet is subject to normal VLAN classification rules of the device.

Use the MAC-based VLAN Configuration page to map a MAC entry to the VLAN table. After the source MAC address and the VLAN ID are specified, the MAC-to-VLAN configurations are shared across all ports of the switch.

To display the MAC-based VLAN Configuration page, click **LAN > L2 Features > VLAN > MAC-based VLAN > Configuration** in the navigation menu.

Figure 105: MAC-based VLAN Configuration

Table 89: MAC-based VLAN Configuration Fields

<i>Field</i>	<i>Description</i>
MAC Address	Specifies the source MAC address to map to a VLAN.
VLAN ID	Specifies the VLAN to which the source MAC address is to be bound.

- If you make any changes, click **Submit** to apply the changes to the system.

MAC-based VLAN Summary

Use the MAC-based VLAN Summary page to view information about the MAC-to-VLAN mappings configured on your system.

To display the MAC-based VLAN Summary page, click **Monitoring > VLAN Summary > MAC-based VLAN Summary** in the navigation menu.

Figure 106: MAC-based VLAN Summary

Table 90: MAC-based VLAN Summary Fields

<i>Field</i>	<i>Description</i>
MAC Address	Specifies the MAC address to map to a VLAN.
VLAN ID	Specifies the VLAN to which the MAC is to be bound.

- Click **Refresh** to reload the page and display the most current information.

Double VLAN Tunneling

Double VLAN Tunneling allows the use of a second tag on network traffic. The additional tag helps differentiate between customers in the Metropolitan Area Networks (MAN) while preserving individual customer's VLAN identification when they enter their own 802.1Q domain.

With the introduction of this second tag, you do not need to divide the 4k VLAN ID space to send traffic on an Ethernet-based MAN.

With Double VLAN Tunneling enabled, every frame that is transmitted from an interface has a DVlan Tag attached while every packet that is received from an interface has a tag removed (if one or more tags are present).

Use the Double VLAN Tunneling page to configure Double VLAN frame tagging on one or more ports.

To access the Double VLAN Tunneling page, click **LAN > L2 Features > VLAN > Double VLAN** in the navigation tree.

Figure 107: Double VLAN Tunneling

Table 91: Double VLAN Tunneling Fields

Field	Description
Interface	Select the physical interface for which you want to display or configure data. Select All to set the parameters for all ports to same values.
Interface Mode	This specifies the administrative mode for Double VLAN Tagging: <ul style="list-style-type: none"> • Enable: Double VLAN Tagging is enabled for the specified port (or All ports). • Disable: Double VLAN Tagging is disabled for the specified port (or All ports), which is the default value.

- If you make any changes to the page, click **Submit** to apply the changes to the system.

Double VLAN Tunneling Summary

The Double VLAN Tunneling Summary page shows the double VLAN tunneling configuration status for all ports on the system.

To access the Double VLAN Tunneling Summary page, click **LAN > Monitoring > VLAN Summary > Double VLAN Status** in the navigation tree.

Slot/Port	Interface Mode	Interface EtherType
0/1	Disable	dVlan-tunnel ethertype 802.1Q
0/2	Disable	dVlan-tunnel ethertype 802.1Q
0/3	Disable	dVlan-tunnel ethertype 802.1Q
0/4	Disable	dVlan-tunnel ethertype 802.1Q
0/5	Disable	dVlan-tunnel ethertype 802.1Q
0/6	Disable	dVlan-tunnel ethertype 802.1Q
0/7	Disable	dVlan-tunnel ethertype 802.1Q
0/8	Disable	dVlan-tunnel ethertype 802.1Q
0/9	Disable	dVlan-tunnel ethertype 802.1Q
0/10	Disable	dVlan-tunnel ethertype 802.1Q

Figure 108: Double VLAN Tunneling Summary

Table 92: Double VLAN Tunneling Summary Fields

Field	Description
Interface	Select the physical interface for which you want to display or configure data.
Interface Mode	This specifies the administrative mode for Double VLAN Tagging: <ul style="list-style-type: none"> • Enable: Double VLAN Tagging is enabled for the specified port (or All ports). • Disable: Double VLAN Tagging is disabled for the specified port (or All ports), which is the default value.
EtherType	The two-byte hex EtherType to be used as the first 16 bits of the Double VLAN tag: <ul style="list-style-type: none"> • 802.1Q Tag: Commonly used tag representing 0x8100 • vMAN Tag: Commonly used tag representing 0x88A8 • Custom Tag: Indicates that a custom tag has been configured and displays its value.

- Click **Refresh** to display the most current information from the router.

Voice VLAN Configuration

The voice VLAN feature enables switch ports to carry voice traffic with defined settings so that voice and data traffic are separated when coming onto the port. A voice VLAN ensures that the sound quality of an IP phone is safeguarded from deterioration when data traffic on the port is high.

The inherent isolation provided by VLANs ensures that inter-VLAN traffic is under management control and that network-attached clients cannot initiate a direct attack on voice components. A QoS protocol based on the IEEE 802.1P class-of-service (CoS) protocol uses classification and scheduling to send network traffic from the switch in a predictable manner. The system uses the source MAC of the traffic traveling through the port to identify the IP phone data flow.

Voice VLAN is enabled per-port basis. A port can participate only in one voice VLAN at a time. The Voice VLAN feature is disabled by default.

To display the Voice VLAN Configuration page, click **LAN > L2 Features > VLAN > Voice VLAN > Voice VLAN Configuration**.

Voice VLAN Configuration	
Voice VLAN Admin Mode	Disable
Interface	0/1
CoS Override Mode	Disable
Voice VLAN Interface Mode	Disable
Operational State	Disable
<input type="button" value="Submit"/> <input type="button" value="Refresh"/>	

Figure 109: Voice VLAN Configuration

Table 93: Voice VLAN Configuration Fields

Field	Description
Voice VLAN Admin Mode	Click Enable or Disable to administratively turn the Voice VLAN feature on or off for all ports.
Interface	Select the slot and port to configure this service on.
CoS Override Mode	Overrides the 802.1p class-of-service (CoS) value for all data (non-voice) packets arriving at the port. Thus any rogue client that is also connected to the voice VLAN port cannot deteriorate the voice traffic.

Table 93: Voice VLAN Configuration Fields (Cont.)

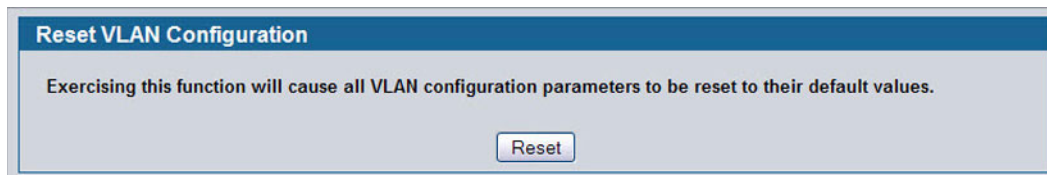
Field	Description
Voice VLAN Interface Mode	<p>Select one of the following interface modes:</p> <ul style="list-style-type: none"> • Disable: The voice VLAN service is disabled on this interface. Note that the Admin mode field takes precedence; i.e., if a particular interface is enabled, but the Admin Mode field is set to Disabled, then the service will not be operational. • VLAN ID: The voice VLAN packets are uniquely identified by a number you assign. All voice traffic carries this VLAN ID to distinguish it from other data traffic which is assigned the port's default VLAN ID. However, voice traffic is not prioritized differently than other traffic. • Dot1p: This parameter is set by the VoIP device for all voice traffic to distinguish voice data from other traffic. All other traffic is assigned the port's default priority. • None: The voice VLAN service is disabled on this interface; however, unlike Disable mode, the CoS override feature is still operational on the port. • Untagged: The VoIP device sends untagged voice traffic.
Operational State	Indicates whether the voice VLAN is operational.

- If you make any changes, click **Submit** to apply the change to the system.
- Click **Refresh** to display the latest information from the router.

Reset VLAN Configuration

Use the Reset Configuration page to return all VLAN parameters for all interfaces to the factory default values.

To access the Reset Configuration page, click **LAN > L2 Features > VLAN > Reset Configuration** in the navigation tree.

**Figure 110: Reset VLAN Configuration**

When you click **Reset**, the screen refreshes, and you are asked to confirm the reset. Click **Reset** again to restore all default VLAN settings for the ports on the system.

Configuring Protected Ports

The Protected Ports feature assists in Layer 2 security. Ports that are configured to be protected cannot forward traffic to other protected ports in the same group, regardless of having the same VLAN membership. However, protected ports can forward traffic to ports which are unprotected as well as ports in other protected groups. Unprotected ports can forward traffic to both protected and unprotected ports.

Protected Port Configuration

Use the Protected Ports Configuration page to create up to three protected port groups and to assign physical ports to a group.

To display the Protected Port Configuration page, click **LAN > L2 Features > Protected Ports > Configuration** in the navigation tree.

Figure 111: Protected Port Configuration

Table 94: Protected Port Configuration Fields

Field	Description
Group ID	The protected ports can be combined into a logical group. Traffic can flow between protected ports belonging to different groups, but not within the same group. The selection box lists all the possible protected port Group IDs supported for the current platform. The valid range is platform-dependent.
Group Name	Assign an optional name to associate with the protected ports group. The name is for identification purposes and can be up to 32 alphanumeric characters long, including blanks. The default is blank.
Protected Port(s)	Specifies the Slot/Port for which port parameters are defined.

Assigning Ports to a Group

1. Select a group ID from the **Group ID** field.
2. From the **Protected Port(s)** field, click one port to add a single port to the group, or hold the CTRL key and click multiple ports to add more than one port to the group.
3. Click **Submit** to apply the changes to the system.

Protected Ports Summary

Use the Protected Ports Summary page to view information about protected port groups and their included ports.

To view the Protected Ports Summary page, click **LAN > Monitoring > Protected Ports > Summary** in the navigation tree.



Group ID	Group Name	Protected Port(s)
0		
1		
2		

Figure 112: Protected Ports Summary

Table 95: Protected Ports Summary Fields

Field	Description
Group ID	Identifies the protected ports group as either Group 0, 1, or 2.
Group Name	Identifies the protected ports group with a user-defined string.
Protected Port(s)	Shows the Slot/Port that are members of the protected ports group.

- Click **Refresh** to reload the page and display the most current information.

Creating MAC Filters

Use the MAC Filtering Configuration page to associate a MAC address with a VLAN and set of source ports and destination ports. Any packet with a static MAC address in a specific VLAN is admitted only if the ingress port is included in the set of source ports; otherwise the packet is dropped. If admitted, the packet is forwarded to all the ports in the destination list.

To access the MAC Filter Configuration page, click **LAN > L2 Features > Filters > MAC Filter Configuration** in the navigation tree.

Figure 113: MAC Filter Configuration

Table 96: MAC Filter Configuration Fields

Field	Description
MAC Filter	If no MAC filters are configured on the system, Create Filter is the only item in the drop-down menu. If one or more MAC filters exist, the list also contains the MAC address and associated VLAN ID of a configured filter.
MAC Address	The MAC address of the filter in the format 00:01:1A:B2:53:4D. You can only change this field when you have selected the "Create Filter" option. Note: You cannot define filters for the following MAC addresses: <ul style="list-style-type: none"> • 00:00:00:00:00:00 • 01:80:C2:00:00:00 to 01:80:C2:00:00:0F • 01:80:C2:00:00:20 to 01:80:C2:00:00:21 • FF:FF:FF:FF:FF:FF
VLAN ID	The VLAN ID used with the MAC address to fully identify packets you want filtered. You can only change this field when you have selected the "Create Filter" option.
Source Port Members	Select the ports you want included in the inbound filter. If a packet with the MAC address and VLAN ID you selected is received on a port that is not in the list, it will be dropped.
Destination Port Members	Select the ports you want to include in the outbound filter. Packets with the MAC address and VLAN ID you selected will only be transmitted out of ports that are in the list.

- Click **Submit** to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle, you must perform a save.
- Click **Delete** to remove the currently selected filter.
- Click **Delete All** to remove all configured filters.

Adding MAC Filters

1. To add a MAC filter, select **Create Filter** from the **MAC Filter** drop-down menu.
2. Enter a valid MAC address and select a VLAN ID from the drop-down menu.
The VLAN ID drop-down menu only lists VLANs currently configured on the system.
3. Select one or more ports to include in the filter. Use **CTRL** + click to select multiple ports.
4. Click **Submit** to apply the changes to the system.

Modifying MAC Filters

To change the port mask(s) for an existing filter, select the entry from the **MAC Filter** field, and then click (or CTRL + click) the port(s) to include in the filter. Only those ports that are highlighted when you click **Submit** are included in the filter.

To change the MAC address or VLAN associated with a filter, you must delete and re-create the filter.

Deleting MAC Filters

To delete a filter, select it from the **MAC Filter** drop-down menu and click **Delete**. To delete all configured filters from the forwarding database, click **Delete All**.

MAC Filter Summary

Use the MAC Filter Summary page to associate a MAC address with a VLAN and one or more source ports.

To access the MAC Filter Summary page, click **LAN > Monitoring > Filters > MAC Filter Summary** in the navigation tree.



MAC address	VLAN ID	Source Port Members	Destination Port Members
00:11:22:33:44:55	1	[0/4] [0/5] [0/6] [0/7]	

Figure 114: MAC Filter Summary

Configuring GARP

Generic Attribute Registration Protocol (GARP) is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of switches interested in a given network attribute, such as VLAN or multicast address.

The GARP VLAN Registration Protocol (GVRP) provides a mechanism that allows networking switches to dynamically register (and de-register) VLAN membership information with the networking devices attached to the same segment, and for that information to be disseminated across all networking switches in the bridged LAN that support GARP Multicast Registration Protocol (GMRP).

With the GARP Multicast Registration Protocol (GMRP), networking devices can dynamically register and de-register group membership information with the networking devices attached to the same segment. GMRP enables the group membership information to be disseminated across all networking devices in the bridged LAN that support GMRP.

The operation of GVRP and GMRP relies upon the services provided by GARP.

GARP Status

Use the GARP Status page to view GARP settings for the system and for each interface.

To access the GARP Status page, click **LAN > Monitoring > GARP Status > Status** in the navigation tree.

GARP Status					
Switch GVRP			Disabled		
Switch GMRP			Disabled		
Slot/Port	Port GVRP Mode	Port GMRP Mode	Join Timer (centisecs)	Leave Timer (centisecs)	Leave All Timer (centisecs)
0/1	Disabled	Disabled	20	60	1000
0/2	Disabled	Disabled	20	60	1000
0/3	Disabled	Disabled	20	60	1000

Figure 115: GARP Status

The GARP Status page contains the following fields:

Table 97: GARP Status Fields

Field	Description
Switch GVRP	Shows whether the switch GVRP protocol is enabled or disabled.
Switch GMRP	Shows whether the switch GMRP protocol is enabled or disabled.
Slot/Port	Identifies the system interface.
Port GVRP Mode	Shows the GARP VLAN Registration Protocol administrative mode for the port. If the mode is Disabled, the protocol will not be active and the Join Time, Leave Time and Leave All Time will have no effect.
Port GMRP Mode	Shows the GARP Multicast Registration Protocol administrative mode for the port. If the mode is Disabled, the protocol will not be active, and Join Time, Leave Time and Leave All Time have no effect.
Join Timer (centisecs)	Shows the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds.
Leave Timer (centisecs)	Displays time lapse, in centiseconds, that the switch waits before leaving its GARP state. Leave time is activated by a Leave All Time message sent/received, and cancelled by the Join message received. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service.
Leave All Timer (centisecs)	Displays time lapse, in centiseconds, that all switches wait before leaving the GARP state. The leave all time must be greater than the leave time. The Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration.

GARP Switch Configuration

Use the GARP Switch Configuration page to configure GARP settings for the system.

To access the GARP Switch Configuration page, click **LAN > L2 Features > GARP > Switch Configuration** in the navigation tree.

Figure 116: GARP Switch Configuration

Table 98: GARP Switch Configuration Fields

Field	Description
Switch GVRP Mode	Shows the GARP VLAN Registration Protocol administrative mode for the switch. The switch GVRP mode must be enabled for the ports to function in GARP protocols, even if GVRP is enabled on a port.
Switch GMRP Mode	Shows the GARP Multicast Registration Protocol administrative mode for the switch. The switch GMRP mode must be enabled for the ports to function in GARP protocols, even if GMRP is enabled on a port.

- If you make any changes to the page, click **Submit** to apply the changes to the system.

GARP Port Configuration

Use the GARP Port Configuration page to configure GARP settings for a specific interface.

To access the GARP Port Configuration page, click **LAN > L2 Features > GARP > Port Configuration** in the navigation tree.

Figure 117: GARP Port Configuration

Table 99: GARP Port Configuration Fields

Field	Description
Slot/Port	Specifies interface on which to configure the GARP settings. If you select All from the drop-down menu, the settings on the page affect all interfaces.
Port GVRP Mode	Choose the GARP VLAN Registration Protocol administrative mode for the port by selecting enable or disable from the pulldown menu. If you select disable, the protocol will not be active and the Join Time, Leave Time and Leave All Time will have no effect. The factory default is disable.
Port GMRP Mode	Choose the GARP Multicast Registration Protocol administrative mode for the port by selecting enable or disable from the pulldown menu. If you select disable, the protocol will not be active, and Join Time, Leave Time and Leave All Time have no effect. The factory default is disable.
GARP Timers	
GARP Join Timer (centiseocs)	Specify the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. Enter a number between 10 and 100 (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds). An instance of this timer exists for each GARP participant for each port.

Table 99: GARP Port Configuration Fields (Cont.)

Field	Description
GARP Leave Timer (centisecs)	Displays time lapse, in centiseconds, that the switch waits before leaving its GARP state. Leave time is activated by a Leave All Time message sent/received, and cancelled by the Join message received. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. Enter a number between 20 and 600 (0.2 to 6.0 seconds). Leave time must be greater than or equal to three times the join time. The factory default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.
GARP Leave All Timer (centisecs)	Displays time lapse, in centiseconds, that all switches wait before leaving the GARP state. The leave all time must be greater than the leave time. The possible field value is 200-6000. The default value is 1000 centisecs. The Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. The timer is specified in centiseconds. Enter a number between 200 and 6000 (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds). An instance of this timer exists for each GARP participant for each port.

- If you make any changes to the page, click **Submit** to apply the changes to the system.

Creating Port Channels (Trunking)

Port-trunks, which are also known as link aggregation groups (LAGs), allow you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. You assign the port-channel (LAG) VLAN membership after you create a port-trunk. The port channel by default becomes a member of the management VLAN.

A port-trunk (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols. A static port-trunk interface does not require a partner system to be able to aggregate its member ports.



Note: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

Static LAGs are supported. When a port is added to a LAG as a static member, it neither transmits nor receives LACPDUs.

Port Channel Configuration

Use the Port Channel Configuration page to group one or more full duplex Ethernet links to be aggregated together to form a port-channel, which is also known as a link aggregation group (LAG). The switch treats the port-channel as if it were a single link.

To access the Port Channel Configuration page, click **LAN > L2 Features > Trunking > Configuration** in the navigation tree.

Slot/Port	Port Channel Name	Link Trap	Administrative Mode	Link Status	STP Mode	Static Mode	Load Balance
		Enable	Enable		Enable	Disable	Src/Dest MAC, VLAN, EType, incoming port
Slot/Port	Participation		Membership Conflicts				
0/1	Exclude						
0/2	Exclude						
0/3	Exclude						
0/4	Exclude						
0/5	Exclude						

Figure 118: Port Channel Configuration

Table 100: Port Channel Configuration Fields

Field	Description
Port Channel Name	Select Create from the drop-down menu to configure a new port channel, or select an existing port channel, identified by the interface and name, to modify its settings. The maximum number of port channels is platform-dependent.
Slot/Port	After you create the port channel, this field identifies the Port Channel with the Slot/Port interface naming convention. This field does not appear while you initially configure a new Port Channel.
Port Channel Name	Enter the name you want assigned to the Port Channel. You may enter any string of up to 15 alphanumeric characters. You must specify a valid name in order to create the Port Channel.
Link Trap	Specify whether you want to have a trap sent when link status changes. The factory default is enable, which will cause the trap to be sent.
Administrative Mode	Select enable or disable from the pulldown menu. When the Port Channel is disabled no traffic will flow and LACPDU's will be dropped, but the links that form the Port Channel will not be released. The factory default is enable.
Link Status	Indicates whether the link is Up or Down.
STP Mode	Select the Spanning Tree Protocol (STP) Administrative Mode associated with the Port Channel: <ul style="list-style-type: none"> • Disable: Spanning tree is disabled for this Port Channel. • Enable: Spanning tree is enabled for this Port Channel.
Static Mode	Select enable or disable from the pulldown menu. The factory default is Disable. <ul style="list-style-type: none"> • Enable: The port channel is statically maintained, which means it does not transmit or process received LAGPDUs. The member ports do not transmit LAGPDUs and all the LAGPDUs it may receive are dropped. A static port-channel interface does not require a partner system to be able to aggregate its member ports. • Disable: The port channel is dynamically maintained. The interface transmits and processes LAGPDUs and requires a partner system
Load Balance	Select the hashing algorithm used to distribute the traffic load among available physical ports in the LAG. The range of possible values may vary with the type of switch. The possible values are: <ul style="list-style-type: none"> • Source MAC, VLAN, EtherType, and source port • Destination MAC, VLAN, EtherType and source port • Source/Destination MAC, VLAN, EtherType, and source port • Source IP and Source TCP/UDP Port • Destination IP and Destination TCP/UDP Port • Source/Destination IP and source/destination TCP/UDP Port
Port Channel Members	After you create one or more port channel, this field lists the members of the Port Channel in Slot/Port form. If there are no port channels on the system, this field is not present.
Slot/Port	This column lists the physical ports available on the system.

Table 100: Port Channel Configuration Fields (Cont.)

Field	Description
Participation	Select each port's membership status for the Port Channel you are configuring. There can be a maximum of 8 ports assigned to a Port Channel. <ul style="list-style-type: none"> • Include: The port participates in the port channel. • Exclude: The port does not participate in the port channel, which is the default.
Membership Conflicts	Shows ports that are already members of other Port Channels. A port may only be a member of one Port Channel at a time. If the entry is blank, the port is not currently a member of any Port Channel

- If you make any changes to this page, click **Submit** to apply the changes to the system.
- To remove a port channel, select it from the **Port Channel Name** drop-down menu and click **Delete**. All ports that were members of this Port Channel are removed from the Port Channel and included in the default VLAN. This field will not appear when a new Port Channel is being created.

Port Channel Status

Use the Port Channel Status page to group one or more full duplex Ethernet links to be aggregated together to form a port-channel, which is also known as a link aggregation group (LAG). The switch can treat the port-channel as if it were a single link.

To access the Port Channel Status page, click **LAN > Monitoring > Trunking > Status** in the navigation tree.

Port Channel	Port Channel Name	Port Channel Type	Admin Mode	Link State	STP Mode	Static Mode	Link Trap	Configured Ports	Active Ports	Load Balance
3/1	LAG1	Dynamic	Enable	Link Down	Enable	Disable	Enable	0/1		Src/Dest MAC, VLAN, EType, incoming port
3/2	LAG2	Dynamic	Enable	Link Down	Enable	Disable	Enable	0/2		Src/Dest MAC, VLAN, EType, incoming port

Refresh

Figure 119: Port Channel Status**Table 101: Port Channel Status Fields**

Field	Description
Port Channel	Identifies the port channel with the Slot/Port interface naming convention.
Port Channel Name	Identifies the user-configured text name of the port channel.
Port Channel Type	The type of this Port Channel, which is one of the following: <ul style="list-style-type: none"> • Static: The port channel is statically maintained. • Dynamic: The port channel is dynamically maintained.

Table 101: Port Channel Status Fields (Cont.)

Field	Description
Admin Mode	Select enable or disable from the pulldown menu. When the Port Channel is disabled no traffic will flow and LACPDU's will be dropped, but the links that form the Port Channel will not be released. The factory default is enable.
Link State	Indicates whether the link is Up or Down.
STP Mode	Shows whether the Spanning Tree Protocol (STP) Administrative Mode is enabled or disabled on the port channel
Static Mode	Shows whether static mode is enabled for this port channel.
Link Trap	Shows whether to send traps when link status changes. If the status is Enabled, traps are sent.
Configured Ports	Lists the ports that are members of the Port Channel, in Slot/Port notation. There can be a maximum of 8 ports assigned to a Port Channel.
Active Ports	Lists the ports that are actively participating members of this Port Channel, in Slot/Port notation.
Load Balance	Shows the hashing algorithm used to distribute the traffic load among available physical ports in the LAG. The range of possible values may vary with the type of switch. The possible values are: <ul style="list-style-type: none"> • Source MAC, VLAN, EtherType, and source port • Destination MAC, VLAN, EtherType and source port • Source/Destination MAC, VLAN, EtherType, and source port • Source IP and Source TCP/UDP Port • Destination IP and Destination TCP/UDP Port • Source/Destination IP and source/destination TCP/UDP Port

Configuring IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping is a feature that allows a switch to forward multicast traffic intelligently on the switch. Multicast IP traffic is traffic that is destined to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request the multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly affecting network performance.

A traditional Ethernet network may be separated into different network segments to prevent placing too many devices onto the same shared media. Bridges and switches connect these segments. When a packet with a broadcast or multicast destination address is received, the switch will forward a copy into each of the remaining network segments in accordance with the IEEE MAC Bridge standard. Eventually, the packet is made accessible to all nodes connected to the network.

This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets will be flooded into network segments where no node has any interest in receiving the packet. While nodes will rarely incur any processing overhead to filter packets addressed to un-requested group addresses, they are unable to transmit new packets onto the shared media for the period of time that the multicast packet is flooded. The problem of wasting bandwidth is even worse when the LAN segment is not shared, for example in Full Duplex links.

Allowing switches to snoop IGMP packets is a creative effort to solve this problem. The switch uses the information in the IGMP packets as they are being forwarded throughout the network to determine which segments should receive packets directed to the group address.

Global Configuration and Status

Use the IGMP Snooping Global Configuration and Status page to enable IGMP snooping on the switch and view information about the current IGMP configuration.

To access the IGMP Snooping Configuration and Status page, click **LAN > L2 Features > IGMP Snooping > Configuration and Status** in the navigation tree.

IGMP Snooping Global Configuration and Status	
Admin Mode	Disable ▾
Multicast Control Frame Count	0
Interfaces Enabled for IGMP Snooping	[None]
Data Frames Forwarded by the CPU	0
VLAN Ids Enabled for IGMP Snooping	

Figure 120: IGMP Snooping Global Configuration and Status

Table 102: IGMP Snooping Global Configuration and Status Fields

<i>Field</i>	<i>Description</i>
Admin Mode	Select the administrative mode for IGMP Snooping for the switch from the pulldown menu. The default is disable.
Multicast Control Frame Count	Shows the number of multicast control frames that have been processed by the CPU.
Interfaces Enabled for IGMP Snooping	Lists the interfaces currently enabled for IGMP Snooping. To enable interfaces for IGMP snooping, see “Interface Configuration” on page 210 .
Data Frames Forwarded by the CPU	Shows the number of data frames forwarded by the CPU.
VLAN Ids Enabled For IGMP Snooping	Displays VLAN Ids enabled for IGMP snooping. To enable VLANs for IGMP snooping, see “Multicast Router Status” on page 214 .

- Select **Enable** or **Disable** the **Admin Mode** field and click **Submit** to turn the feature on or off. Perform a save if you want the changes to remain in effect over a power cycle.

Interface Configuration

Use the IGMP Snooping Interface Configuration page to configure IGMP snooping settings on specific interfaces.

To access the IGMP Snooping Interface Configuration page, click **LAN > L2 Features > IGMP Snooping > Interface Configuration** in the navigation tree.

IGMP Snooping Interface Configuration	
Slot/Port	0/1
Admin Mode	Disable
Group Membership Interval	260 ((Max Response Time + 1) to 3600 secs)
Max Response Time(Less Than Group Membership Interval)	10 (1 to 25 secs)
Multicast Router Present Expiration Time	0 (0 to 3600 secs)
Fast Leave Admin Mode	Disable

Figure 121: IGMP Snooping Interface Configuration

Table 103: IGMP Snooping Interface Configuration Fields

<i>Field</i>	<i>Description</i>
Slot/Port	Select the physical or LAG interfaces to configure.
Admin Mode	Select the interface mode for the selected interface for IGMP Snooping for the switch from the pulldown menu. The default is disable.
Group Membership Interval	Specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group. The valid range is from (2 to 3600) seconds. The default is 260 seconds.
Max Response Time	Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds. The default is 10 seconds. The configured value must be less than the Group Membership Interval.
Multicast Router Present Expiration Time	Specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite timeout; i.e., no expiration.
Fast Leave Admin Mode	Select the Fast Leave mode for the a particular interface from the pulldown menu. The default is Disable . Enabling Fast Leave mode allows the switch to immediately remove the Layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface.

- If you make any changes on the page, click **Submit** to apply the new settings to the switch.

VLAN Configuration

Use the IGMP Snooping VLAN Configuration page to configure IGMP snooping settings for VLANs on the system.

To access the IGMP Snooping VLAN Configuration page, click **LAN > L2 Features > IGMP Snooping > VLAN Configuration** in the navigation tree.

IGMP Snooping VLAN Configuration	
VLAN ID	1
Admin Mode	Enable
Fast Leave Admin Mode	Enable
Group Membership Interval	260 ((Max Response Time + 1) to 3600 secs)
Maximum Response Time	10 (1 to 25 secs)
Multicast Router Expiry Time	0 (0 to 3600 secs)
<input type="button" value="Submit"/> <input type="button" value="Delete"/>	

Figure 122: IGMP Snooping VLAN Configuration

Table 104: IGMP Snooping VLAN Configuration Fields

Field	Description
VLAN ID	From the drop-down menu, select the VLAN ID of the VLAN to modify, or select New Entry to configure settings for a VLAN that does not have IGMP Snooping enabled.
Admin Mode	Enable is the only available option from the drop-down menu. To disable the IGMP snooping admin mode on the VLAN, select the VLAN from the VLAN ID field and click Delete .
Fast Leave Admin Mode	Enabling fast-leave allows the switch to immediately remove the layer 2 LAN interface from its forwarding table entry upon receiving an IGMP leave message for that multicast group without first sending out MAC-based general queries to the interface. You should enable fast-leave admin mode only on VLANs where only one host is connected to each layer 2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer 2 LAN port but were still interested in receiving multicast traffic directed to that group. Also, fast-leave processing is supported only with IGMP version 2 hosts.
Group Membership Interval	The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response time value. The range is 2 to 3600 seconds.
Maximum Response Time	Enter the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the Group Membership Interval time value. The range is 1 to 25 seconds.

Table 104: IGMP Snooping VLAN Configuration Fields (Cont.)

Field	Description
Operational Maximum Response Time	This read-only field displays the value for maximum response time of IGMP Snooping for the specified VLAN ID. Its value is learned dynamically from the IGMPv2 or IGMPv3 queries received on this VLAN. For the multicast traffic not to get disturbed, you should configure group membership interval to be greater than this value.
Multicast Router Expiry Time	Enter the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out; i.e., no expiration.

- If you make any changes to the page, click **Submit** to apply the new settings to the system.

VLAN Status

Use the IGMP Snooping VLAN Status page to view information about the VLANs on the system that are configured for IGMP snooping.

To access the IGMP Snooping VLAN Status page, click **LAN > Monitoring > IGMP Snooping Status > VLAN Status** in the navigation tree.

IGMP Snooping VLAN Status					
VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval (secs)	Max Response Time (secs)	Multicast Router Expiry Time (secs)
1	Enable	Enable	260	10	0

Figure 123: IGMP Snooping VLAN Status**Table 105: IGMP Snooping VLAN Status Fields**

Field	Description
VLAN ID	Displays the VLAN IDs for which the IGMP Snooping mode is Enabled.
Admin Mode	Shows the IGMP Snooping Mode for the VLAN ID.
Fast Leave Admin Mode	Indicates whether IGMP Snooping Fast-leave is active on the VLAN.
Group Membership Interval	Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry.
Max Response Time	Shows the amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. This value may be configured.

Table 105: IGMP Snooping VLAN Status Fields (Cont.)

Field	Description
Operational Maximum Response Time	Displays the value for maximum response time of IGMP Snooping for the specified VLAN ID. Its value is learned dynamically from the IGMPv2 or IGMPv3 queries received on this VLAN.
Multicast Router Expiry Time	Shows the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received.

- Click **Refresh** to re-display the page with the latest information from the router.

Multicast Router Configuration

If a multicast router is attached to the switch, its existence can be learned dynamically. You can also statically configure a switch port as a multicast router interface. Use the Multicast Router Configuration page to manually configure an interface as a static multicast router interface.

To access the IGMP Snooping Multicast Router Configuration page, click **LAN > L2 Features > IGMP Snooping > Multicast Router Configuration** in the navigation tree.

Figure 124: Multicast Router Configuration**Table 106: Multicast Router Configuration Fields**

Field	Description
Slot/Port	Select the physical or LAG interface to display.
Multicast Router	Set the multicast router status: <ul style="list-style-type: none"> • Enabled: The port is a multicast router interface. • Disabled: The port does not have a multicast router configured.

If you enable or disable multicast router configuration on an interface, click **Submit** to apply the new settings to the switch.

Multicast Router Status

Use the IGMP Snooping Multicast Router Status page to see whether a particular interface is configured as a multicast router interface.

To access the IGMP Snooping Multicast Router Statistics page, click **Monitoring > IGMP Snooping Status > Multicast Router Status** in the navigation tree.

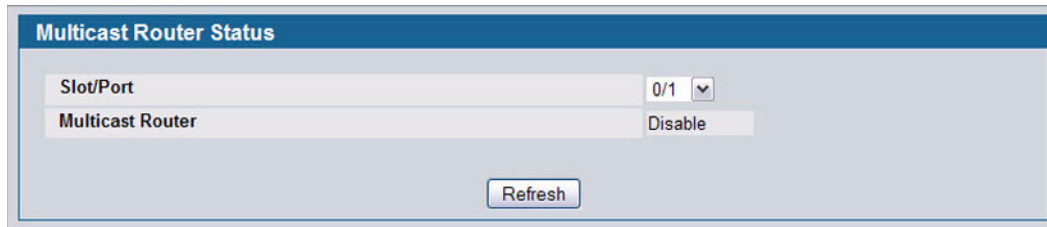


Figure 125: Multicast Router Status

Table 107: Multicast Router Status Fields

Field	Description
Slot/Port	Select the physical or LAG interface to display.
Multicast Router	Shows whether the specified interface is configured as a multicast router interface.

- Click **Refresh** to re-display the page with the latest information from the router.

Multicast Router VLAN Configuration

Use the IGMP Snooping Multicast Router VLAN Configuration page to configure multicast router settings for VLANs on an interface.

To access the IGMP Snooping Multicast Router VLAN Configuration page, click **LAN > L2 Features > IGMP Snooping > Multicast Router VLAN Configuration** in the navigation tree.

Figure 126: Multicast Router VLAN Configuration

Table 108: Multicast Router VLAN Configuration Fields

Field	Description
Slot/Port	Select the physical or LAG interface to display.
VLAN ID	Enter the VLAN ID to configure as enabled or disabled for multicast routing.
Multicast Router	Select Enable or Disable from the drop-down menu to change the multicast router mode of the VLAN associated with this interface.

- If you enable or disable multicast router configuration for VLANs on an interface, click **Submit** to apply the new settings to the switch.

Multicast Router VLAN Status

Use the IGMP Snooping Multicast Router VLAN Status page to view multicast router settings for VLANs on a specific interface.

To access the IGMP Snooping Multicast Router VLAN Status page, click **Monitoring > IGMP Snooping Status > Multicast Router VLAN Status** in the navigation tree.

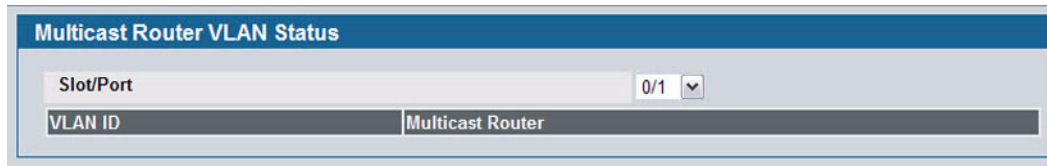


Figure 127: Multicast Router VLAN Status

The IGMP Snooping Multicast Router VLAN Status page contains the following fields:

Table 109: Multicast Router VLAN Status Fields

	<i>Description</i>
Slot/Port	Select the physical or LAG interface to display.
VLAN ID	If a VLAN is enabled for multicast routing on the interface, this field displays its ID.
Multicast Router	Indicates that the multicast router is enabled for the VLAN on this interface.

- Click **Refresh** to re-display the page with the latest information from the router.

Configuring IGMP Snooping Queriers

IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the 'IGMP querier'. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicast to the port where the end device is located.

These pages enable you to configure and display information on IGMP snooping queriers on the network and, separately, on VLANs.

IGMP Snooping Querier Configuration

Use this page to enable or disable the IGMP Snooping Querier feature, specify the IP address of the router to perform the querying, and configure related parameters. Users must have Read/Write access privileges to change the data on this page.

To access this page, click **LAN > L2 Features > IGMP Snooping Querier > IGMP Snooping Querier Configuration** in the navigation tree.

IGMP Snooping Querier Configuration	
Snooping Querier Admin Mode	Disable ▾
Snooping Querier Address	0.0.0.0
IGMP Version	2 (1 to 2)
Query Interval(secs)	60 (1 to 1800)
Querier Expiry Interval(secs)	60 (60 to 300)
<input type="button" value="Submit"/> <input type="button" value="Refresh"/>	

Figure 128: IGMP Snooping Querier Configuration

Table 110: IGMP Snooping Querier Configuration Fields

Field	Description
Snooping Querier Admin Mode	Select the administrative mode for IGMP Snooping for the switch from the pulldown menu. The default is Disable .
Snooping Querier Address	Specify the Snooping Querier Address to be used as source IP address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.
IGMP Version	Specify the IGMP protocol version used in periodic IGMP queries.
Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800 seconds. The default value is 60 seconds.

Table 110: IGMP Snooping Querier Configuration Fields (Cont.)

Field	Description
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60 seconds.

- If you configure an IGMP snooping querier, click **Submit** to apply the new settings to the switch.
- Click **Refresh** to re-display the page with the latest information from the switch.

IGMP Snooping Querier VLAN Configuration

Use this page to configure IGMP queriers for use with VLANs on the network.

To access this page, click **LAN > L2 Features > IGMP Snooping Querier > IGMP Snooping Querier VLAN Configuration** in the navigation tree.

Figure 129: IGMP Snooping Querier VLAN Configuration**Table 111: IGMP Snooping Querier VLAN Configuration Fields**

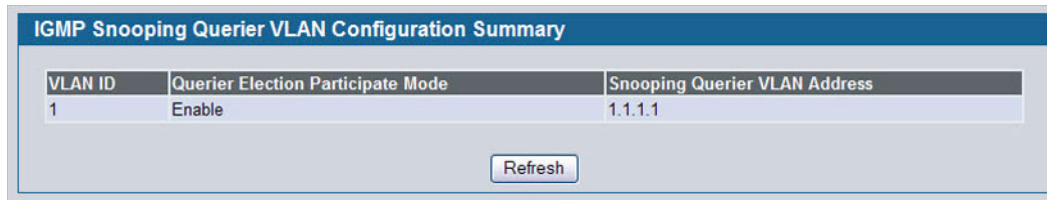
Field	Description
VLAN ID	Specifies VLAN ID for which the IGMP Snooping Querier is to be enabled. Select New Entry to create a new VLAN ID for IGMP Snooping.
Querier Election Participate Mode	Enables or disables Querier Participate Mode. When this mode is disabled, upon seeing another querier of same version in the VLAN, the snooping querier moves to non-querier state. When enabled, the snooping querier participates in querier election, in which the least IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
Snooping Querier VLAN Address	Specifies the Snooping Querier Address to be used as source IP address in periodic IGMP queries sent on the specified VLAN.

- If you configure a snooping querier for a VLAN, click **Submit** to apply the new settings.
- Click **Refresh** to re-display the page with the latest information from the switch.

IGMP Snooping Querier VLAN Configuration Summary

Use this page to view summary information for IGMP snooping queriers for on VLANs in the network.

To access this page, click **LAN > L2 Features > IGMP Snooping Querier > IGMP Snooping Querier VLAN Configuration Summary** in the navigation tree.



VLAN ID	Querier Election Participate Mode	Snooping Querier VLAN Address
1	Enable	1.1.1.1

Figure 130: IGMP Snooping Querier VLAN Configuration Summary

Table 112: IGMP Snooping Querier VLAN Configuration Summary Fields

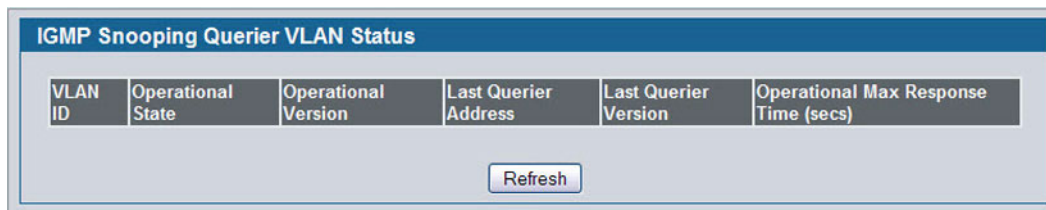
<i>Field</i>	<i>Description</i>
VLAN ID	Specifies the VLAN ID on which IGMP Snooping Querier is administratively enabled.
Querier Election Participate Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, upon seeing a query of the same version in the VLAN, the snooping querier moves to non-querier state. When this mode is enabled, the snooping querier participates in querier election, in which the lowest IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
Snooping Querier VLAN Address	Displays the Snooping Querier Address to be used as source address in periodic IGMP queries sent on the specified VLAN.

- Click **Refresh** to re-display the page with the latest information from the router.

IGMP Snooping Querier VLAN Status

Use this page to view the operational state and other information for IGMP snooping queriers for VLANs on the network.

To access this page, click **Monitoring > Querier VLAN Status** in the navigation tree.



VLAN ID	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time (secs)
Refresh					

Figure 131: IGMP Snooping Querier VLAN Status

Table 113: IGMP Snooping Querier VLAN Status Fields

Field	Description
VLANID	Specifies the VLAN ID on which the IGMP Snooping Querier is administratively enabled and for which VLAN exists in the VLAN database.
Operational State	Specifies the operational state of the IGMP Snooping Querier on a VLAN: <ul style="list-style-type: none"> • Querier: The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier (numerically lower) in the VLAN, it moves to non-querier mode. • Non-Querier: The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. • Disabled: The snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when IGMP snooping is not operational on the VLAN, when the querier address is not configured, or the network management address is not configured.
Operational Version	Displays the IGMP protocol version of the operational querier.
Last Querier Address	Displays the IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	Displays the IGMP protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	Displays the maximum response time to be used in the queries that are sent by the snooping querier.

- Click **Refresh** to re-display the page with the latest information from the switch.

Configuring MLD Snooping

In IPv4, Layer 2 switches can use IGMP snooping to limit the flooding of multicast traffic by dynamically configuring Layer-2 interfaces so that multicast traffic is forwarded to only those interfaces associated with an IP multicast address. In IPv6, Multicast Listener Discovery (MLD) snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly-attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) is equivalent to IGMPv2 and MLD version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages.

The switch can snoop on both MLDv1 and MLDv2 protocol packets and bridge IPv6 multicast data based on destination IPv6 multicast MAC addresses. The switch can be configured to perform MLD snooping and IGMP snooping simultaneously.

Configuration and Status

Use the MLD Snooping Global Configuration and Status page to enable MLD snooping on the switch and view information about the current MLD snooping configuration.

To access this page, click **LAN > L2 Features > MLD Snooping > Configuration and Status** in the navigation tree.

MLD Snooping Global Configuration and Status	
Admin Mode	Disable ▾
Multicast Control Frame Count	0
Interfaces Enabled for MLD Snooping	[None]
Data Frames Forwarded by the CPU	0
VLAN Ids Enabled for MLD Snooping	

Figure 132: MLD Snooping Global Configuration and Status

Table 114: MLD Snooping Global Configuration and Status Fields

<i>Field</i>	<i>Description</i>
Admin Mode	Select the administrative mode for MLD Snooping for the switch from the pulldown menu. The default is disable.
Multicast Control Frame Count	Shows the number of multicast control frames that have been processed by the CPU.
Interfaces Enabled for MLD Snooping	Lists the interfaces currently enabled for MLD Snooping. To enable interfaces for MLD snooping, see “Interface Configuration” on page 222 .

Table 114: MLD Snooping Global Configuration and Status Fields (Cont.)

Field	Description
Data Frames Forwarded by the CPU	Shows the number of data frames forwarded by the CPU.
VLAN Ids Enabled For MLD Snooping	Displays VLAN Ids enabled for MLD snooping. To enable interfaces for MLD snooping, see “VLAN Configuration” on page 224 .

- Select **Enable** or **Disable** the **Admin Mode** field and click **Submit** to turn the feature on or off. Perform a save if you want the changes to remain in effect over a power cycle.

Interface Configuration

Use the MLD Snooping Interface Configuration page to configure snooping settings on specific interfaces.

To access the MLD Snooping Interface Configuration page, click **LAN > L2 Features > MLD Snooping > Interface Configuration** in the navigation tree.

Figure 133: MLD Snooping Interface Configuration**Table 115: MLD Snooping Interface Configuration Fields**

Field	Description
Slot/Port	Select the physical or LAG interfaces to configure.
Admin Mode	Select the interface mode for the selected interface for MLD Snooping for the switch from the pulldown menu. The default is Disable .
Group Membership Interval	Specify the amount of time you want the switch to wait for a report for a particular group on a particular interface before it deletes that interface from the group. The valid range is from (2 to 3600) seconds. The default is 260 seconds.
Max Response Time	Specify the amount of time you want the switch to wait after sending a query on an interface because it did not receive a report for a particular group on that interface. Enter a value greater or equal to 1 and less than the Group Membership Interval in seconds. The default is 10 seconds. The configured value must be less than the Group Membership Interval.

Table 115: MLD Snooping Interface Configuration Fields (Cont.)

Field	Description
Multicast Router Present Expiration Time	Specify the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite timeout; i.e., no expiration.
Fast Leave Admin Mode	Select the Fast Leave mode for the a particular interface from the pulldown menu. The default is Disable .

- If you make any changes on the page, click **Submit** to apply the new settings to the switch.

VLAN Status

Use the MLD Snooping VLAN Status page to view information about the VLANs on the system that are configured for MLD snooping.

To access the MLD Snooping VLAN Status page, click **Monitoring > MLD Snooping > VLAN Status** in the navigation tree.

MLD Snooping VLAN Status					
VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval (secs)	Max Response Time (secs)	Multicast Router Expiry Time (secs)
1	Enable	Disable	260	10	0

Figure 134: MLD Snooping VLAN Status**Table 116: MLD Snooping VLAN Status Fields**

Field	Description
VLAN ID	Displays the VLAN IDs for which the MLD Snooping mode is Enabled.
Admin Mode	Shows the MLD Snooping Mode for the VLAN ID.
Fast Leave Admin Mode	Indicates whether MLD Snooping Fast-leave is active on the VLAN.
Group Membership Interval	Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. The valid range is 2 to 3600.
Maximum Response Time	Shows the amount of time the switch waits after it sends a query on an interface, participating in the VLAN, because it did not receive a report for a particular group on that interface. The valid range is 1 to 3599. Its value should be greater than group membership interval value.
Multicast Router Expiry Time	Shows the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. The valid range is 0 to 3600.

- Click **Refresh** to re-display the page with the latest information from the router.

VLAN Configuration

Use the MLD Snooping VLAN Configuration page to configure MLD Snooping settings for VLANs on the system.

To access the MLD Snooping VLAN Configuration page, click **LAN > L2 Features > MLD Snooping > VLAN Configuration** in the navigation tree.

Figure 135: MLD Snooping VLAN Configuration

Table 117: MLD Snooping VLAN Configuration Fields

<i>Field</i>	<i>Description</i>
VLAN ID	Specifies list of VLAN IDs for which MLD Snooping is enabled. If no entries exist, New Entry displays. Enter the VLAN ID of the VLAN on which to enable and configure MLD Snooping.
Admin Mode	Enable is the only available option from the drop-down menu. To disable the MLD Snooping admin mode on the VLAN, select the VLAN from the VLAN ID field and click Delete .
Fast Leave Admin Mode	Enabling fast-leave allows the switch to immediately remove the layer-2 LAN interface from its forwarding table entry upon receiving an MLD leave message for that multicast group without first sending out MAC-based general queries to the interface. Enable fast-leave admin mode only on VLANs where only one host is connected to each layer-2 LAN port. This prevents the inadvertent dropping of the other hosts that were connected to the same layer-2 LAN port but were still interested in receiving multicast traffic directed to that group.
Group Membership Interval	The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the Maximum Response time value. The range is 2 to 3600 seconds.
Maximum Response Time	Enter the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the Group Membership Interval value. The range is 1 to 65 seconds.

Table 117: MLD Snooping VLAN Configuration Fields (Cont.)

Field	Description
Multicast Router Expiry Time	Enter the amount of time in seconds that a switch waits for a query to be received on an interface before the interface is removed from the list of interfaces with multicast routers attached. The range is 0 to 3600 seconds. A value of 0 indicates an infinite time-out; i.e., no expiration.

- If you make any changes to the page, click **Submit** to apply the new settings to the system.
- To disable the MLD Snooping admin mode on a VLAN, select the VLAN from the VLAN ID field and click **Delete**.

Multicast Router Configuration

The switch can dynamically learn of an attached multicast router, or you can configure a switch port as a multicast router interface. Use the MLD Snooping Multicast Router Configuration page to configure an interface as a static multicast router interface.

To access the MLD Snooping Multicast Router Configuration page, click **LAN > L2 Features > MLD Snooping > Multicast Router Configuration** in the navigation tree.

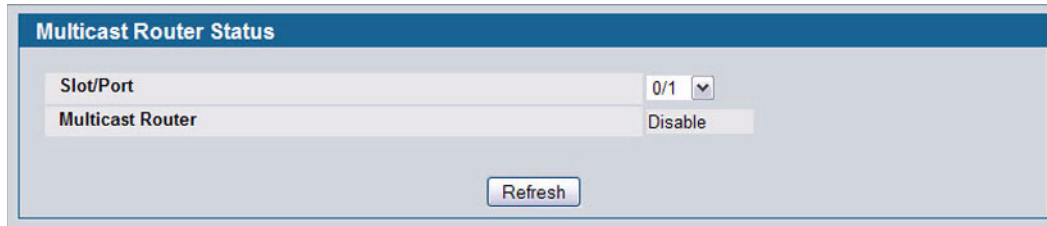
Figure 136: MLD Snooping Multicast Router Configuration**Table 118: MLD Snooping Multicast Router Configuration Fields**

Field	Description
Slot/Port	Select the physical or LAG interface to display.
Multicast Router	Set the multicast router status: <ul style="list-style-type: none"> • Enabled: The port is a multicast router interface. • Disabled: The port does not have multicast router configured.

- If you enable or disable multicast router configuration on an interface, click **Submit** to apply the new settings to the switch.

Multicast Router Status

Use the MLD Snooping Multicast Router Status page to view multicast router functionality on selected ports. To access this page, click **Monitoring > MLD Snooping > Multicast Router Status** in the navigation tree.



The screenshot shows a web interface for configuring Multicast Router Status. It features a blue header with the title "Multicast Router Status". Below the header, there are two input fields: "Slot/Port" with a dropdown menu showing "0/1" and "Multicast Router" with a dropdown menu showing "Disable". At the bottom center, there is a "Refresh" button.

Figure 137: MLD Snooping Multicast Router Status

Table 119: MLD Snooping Multicast Router Status Fields

Field	Description
Slot/Port	Select the slot and port number with the information to view.
Multicast Router	Indicates whether the specified interface is configured to perform multicast routing.

- Click **Refresh** to re-display the page with the latest information from the router.

Multicast Router VLAN Configuration

Use the MLD Snooping Multicast Router VLAN Configuration page to configure multicast router settings for VLANs on an interface.

To access the MLD Snooping Multicast Router VLAN Configuration page, click **LAN > L2 Features > MLD Snooping > Multicast Router VLAN Configuration** in the navigation tree.

Figure 138: Multicast Router VLAN Configuration

Table 120: Multicast Router VLAN Configuration Fields

Field	Description
Slot/Port	Select the physical, VLAN, or LAG interface to display.
VLAN ID	Enter the VLAN ID to configure as enabled or disabled for multicast routing.
Multicast Router	Select Enable or Disable from the drop-down menu to change the multicast router mode of the VLAN associated with this interface.

- If you enable or disable multicast router configuration for VLANs on an interface, click **Submit** to apply the new settings to the switch.

Multicast Router VLAN Status

Use the MLD Snooping Multicast Router VLAN Status page to view multicast router settings for VLANs on a specific interface.

To access the MLD Snooping Multicast Router VLAN Statistics page, click **Monitoring > MLD Snooping > Multicast Router VLAN Status** in the navigation tree.

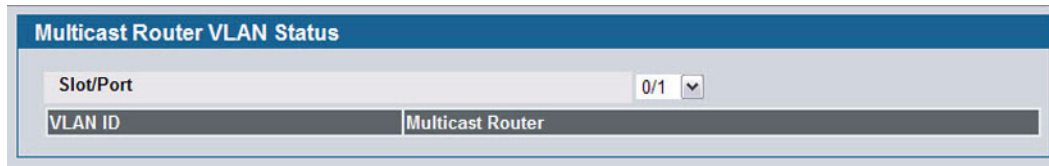


Figure 139: MLD Snooping Multicast Router VLAN Status

The MLD Snooping Multicast Router VLAN Statistics page contains the following fields:

Table 121: MLD Snooping Multicast Router VLAN Status Fields

<i>Description</i>	
Slot/Port	Select the physical or LAG interface to display.
VLAN ID	If a VLAN is enabled for multicast routing on the interface, this field displays its ID.
Multicast Router	Indicates that the multicast router is enabled for the VLAN on this interface.

- Click **Refresh** to re-display the page with the latest information from the router.

Configuring MLD Snooping Queriers

In an IPv6 environment, MLD Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the 'MLD querier'. The MLD query responses, known as MLD reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicast to the port where the end device is located.

These pages enable you to configure and display information on MLD Snooping queriers on the network and, separately, on VLANs.

MLD Snooping Querier Configuration

Use this page to enable or disable the MLD Snooping Querier feature, specify the IP address of the router to perform the querying, and configure related parameters. Users must have Read/Write access privileges to change the data on this page.

To access this page, click **LAN > L2 Features > MLD Snooping Querier > MLD Snooping Querier Configuration** in the navigation tree.

MLD Snooping Querier Configuration	
Snooping Querier Admin Mode	Disable
Snooping Querier Address	:: Supported Formats
MLD Version	1
Query Interval(secs)	60 (1 to 1800)
Querier Expiry Interval(secs)	60 (60 to 300)
<input type="button" value="Submit"/> <input type="button" value="Refresh"/>	

Figure 140: MLD Snooping Querier Configuration

Table 122: MLD Snooping Querier Configuration Fields

Field	Description
Snooping Querier Admin Mode	Select the administrative mode for MLD Snooping for the switch from the pulldown menu. The default is Disable.
Snooping Querier Address	Specify the Snooping Querier Address to be used as source IPv6 address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.
MLD Version	Specify the MLD protocol version used in periodic MLD queries.
Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.

Table 122: MLD Snooping Querier Configuration Fields (Cont.)

Field	Description
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 60.

- If you configure an MLD Snooping querier, click **Submit** to apply the new settings to the switch.
- Click **Refresh** to display the page with the latest information from the switch.

MLD Snooping Querier VLAN Configuration

Use this page to configure MLD queriers for use with VLANs on the network.

To access this page, click **LAN > L2 Features > MLD Snooping Querier > MLD Snooping Querier VLAN Configuration** in the navigation tree.

Figure 141: MLD Snooping Querier VLAN Configuration**Table 123: MLD Snooping Querier VLAN Configuration Fields**

Field	Description
VLAN ID	Specifies VLAN ID for which MLD Snooping Querier is to be enabled. You can select New Entry to create a new VLAN ID for the MLD Snooping feature.
Querier Election Participate Mode	Enables or disables Querier Participate Mode. When this mode is disabled, upon seeing another querier of same version in the VLAN, the snooping querier moves to non-querier state. When enabled, the snooping querier participates in querier election, in which the least IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
Snooping Querier VLAN Address	Specifies the Snooping Querier Address to be used as source IPv6 address in periodic IGMP queries sent on the specified VLAN.

- If you configure or modify the participate mode of a snooping querier for a VLAN, click **Submit** to apply the new settings.
- Click **Refresh** to display the page with the latest information from the switch.
- To remove a querier from the network, select its VLAN ID and click **Delete**.

MLD Snooping Querier VLAN Configuration Summary

Use this page to view summary information for MLD Snooping queriers for on VLANs in the network.

To access this page, click **Monitoring > MLD Snooping Querier > Querier VLAN Configuration Summary** in the navigation tree.



Figure 142: MLD Snooping Querier VLAN Configuration Summary

Table 124: MLD Snooping Querier VLAN Configuration Summary Fields

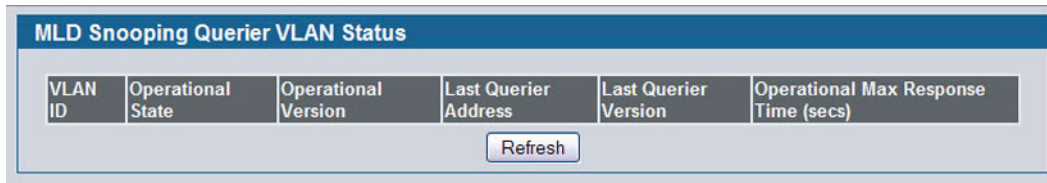
Field	Description
VLAN ID	Specifies the VLAN ID on which MLD Snooping Querier is administratively enabled.
Querier Election Participate Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the VLAN, the snooping querier moves to non-querier state. When this mode is enabled, the snooping querier participate in querier election, in which the lowest IP address operates as the querier in that VLAN. The other querier moves to non-querier state.
Snooping Querier VLAN Address	Displays the Snooping Querier Address to be used as source IPv6 address in periodic IGMP queries sent on the specified VLAN.

- Click **Refresh** to display the page with the latest information from the router.

MLD Snooping Querier VLAN Status

Use this page to view the operational state and other information for MLD Snooping queriers for VLANs on the network.

To access this page, click **LAN > Monitoring > MLD Snooping Querier > Querier VLAN Status** in the navigation tree.



VLAN ID	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time (secs)
Refresh					

Figure 143: MLD Snooping Querier VLAN Status

Table 125: MLD Snooping Querier VLAN Status Fields

Field	Description
VLAN ID	Specifies the VLAN ID on which the MLD Snooping Querier is administratively enabled and for which VLAN exists in the VLAN database.
Operational State	Specifies the operational state of the MLD Snooping Querier on a VLAN: <ul style="list-style-type: none"> • Querier: The snooping switch is the querier in the VLAN. The snooping switch will send out periodic queries with a time interval equal to the configured querier query interval. If the snooping switch sees a better querier in the VLAN (i.e., with a numerically lower value), it moves to non-querier mode. • Non-Querier: The snooping switch is in non-querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch moves into querier mode. • Disabled: The snooping querier is not operational on the VLAN. The snooping querier moves to disabled mode when MLD Snooping is not operational on the VLAN, when the querier address is not configured, or the network management address is not configured.
Operational Version	Displays the MLD protocol version of the operational querier.
Last Querier Address	Displays the IP address of the last querier from which a query was snooped on the VLAN.
Last Querier Version	Displays the MLD protocol version of the last querier from which a query was snooped on the VLAN.
Operational Max Response Time	Displays the maximum response time to be used in the queries that are sent by the snooping querier.

- Click **Refresh** to display the page with the latest information from the switch.

Viewing Multicast Forwarding Database Information

The Layer 2 Multicast Forwarding Database (MFDB) is used by the switch to make forwarding decisions for packets that arrive with a multicast destination MAC address. By limiting multicasts to only certain ports in the switch, traffic is prevented from going to parts of the network where that traffic is unnecessary.

When a packet enters the switch, the destination MAC address is combined with the VLAN ID and a search is performed in the Layer 2 Multicast Forwarding Database. If no match is found, then the packet is either flooded to all ports in the VLAN or discarded, depending on the switch configuration. If a match is found, then the packet is forwarded only to the ports that are members of that multicast group.

MFDB Table

Use the MFDB Table page to view the port membership information for all active multicast address entries. The key for an entry consists of a VLAN ID and MAC address pair. Entries may contain data for more than one protocol.

To access the MFDB Table page, click **LAN > Monitoring > Multicast Forwarding Database > MFDB Table** in the navigation tree.

The screenshot shows a web interface titled "Multicast Forwarding Database Table". At the top, there is a search bar labeled "MAC address" with a "Search" button. Below the search bar is a table with the following columns: "MAC address", "Component", "Type", "Description", "Slot/Port", and "Forwarding Slot/Port(s)". Below the table is a "Refresh" button.

Figure 144: MFDB Table

Table 126: MFDB Table Fields

Field	Description
MAC Address	Enter the VLAN ID/MAC Address pair whose MFDB table entry you want displayed. Enter eight two-digit hexadecimal numbers separated by colons, for example 00:01:23:43:45:67:89:AB. The first two 2-digit hexadecimal numbers are the VLAN ID and the remaining numbers are the MAC address. Then click on the Search button. If the address exists, that entry will be displayed. An exact match is required.
MAC Address	The multicast MAC address for which you requested data.
Component	This is the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are MLD Snooping, GMRP, IGMP Snooping, and Static Filtering.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.

Table 126: MFDB Table Fields (Cont.)

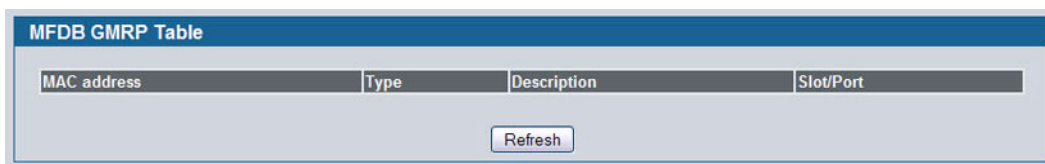
Field	Description
Slot/Port	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the selected address.
Forwarding Slot/Port(s)	The resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

- To search for a MAC address if the list is too long to scan, enter the MAC address in hex format and click **Search**.
- Click **Refresh** to update the information on the screen with the most current data.

MFDB GMRP Table

Use the GMRP Table page to view all of the entries in the Multicast Forwarding Database that were created for the GARP Multicast Registration Protocol.

To access the GMRP Table page, click **LAN > Monitoring > Multicast Forwarding Database > GMRP Table** in the navigation tree.

**Figure 145: GMRP Table****Table 127: GMRP Table Fields**

Field	Description
MAC Address	A VLAN ID/multicast MAC address pair for which the switch has forwarding and or filtering information. The format is 8 two-digit hexadecimal numbers that are separated by colons, for example 00:01:23:45:67:89:AB:CD.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
Slot/Port	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address.

- Click **Refresh** to update the information on the screen with the most current data.

MFDB IGMP Snooping Table

Use the IGMP Snooping Table page to view all of the entries in the Multicast Forwarding Database that were created for IGMP snooping.

To access the IGMP Snooping Table page, click **LAN > Monitoring > Multicast Forwarding Database > IGMP Snooping Table** in the navigation tree.

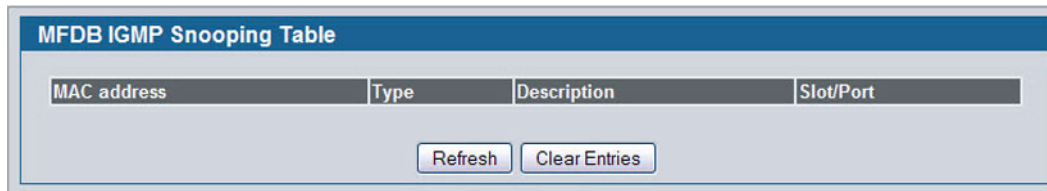


Figure 146: IGMP Snooping Table

Table 128: MFDB IGMP Snooping Table Fields

Field	Description
MAC Address	A VLAN ID/multicast MAC address pair for which the switch has forwarding and or filtering information. The format is 8 two-digit hexadecimal numbers that are separated by colons, for example, 00:01:23:45:67:89:AB:CD.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
Slot/Port	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address.

- Click **Refresh** to update the information on the screen with the most current data.
- Click **Clear Entries** to tell the IGMP Snooping component to delete all of its entries from the multicast forwarding database.

MFDB MLD Snooping Table

Use the MLD Snooping Table page to view all of the entries in the Multicast Forwarding Database that were created for MLD Snooping.

To access the MLD Snooping Table page, click **LAN > Monitoring > Multicast Forwarding Database > MLD Snooping Table** in the navigation tree.

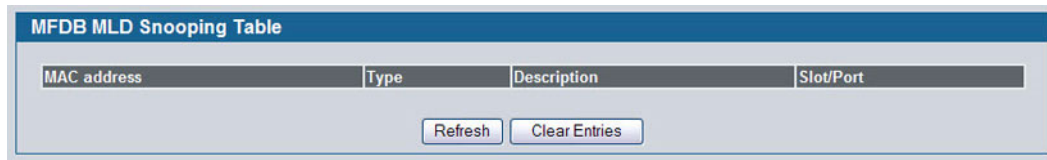


Figure 147: MFDB MLD Snooping Table

Table 129: MLD Snooping Table Fields

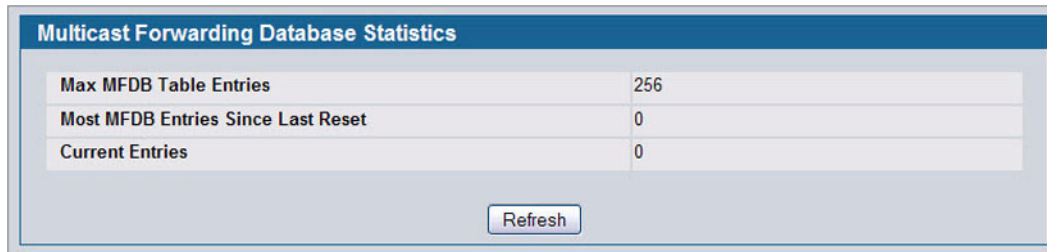
Field	Description
MAC Address	A VLAN ID/multicast MAC address pair for which the switch has forwarding and or filtering information. The format is 8 two-digit hexadecimal numbers that are separated by colons, for example, 00:01:23:45:67:89:AB:CD.
Type	This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	The text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
Slot/Port	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address.

- Click **Refresh** to update the information on the screen with the most current data.
- Click **Clear Entries** to tell the MLD Snooping component to delete all of its entries from the multicast forwarding database.

MFDB Statistics

Use the multicast forwarding database Stats page to view statistical information about the MFDB table.

To access the Stats page, click **LAN > Monitoring > Multicast Forwarding Database > Statistics** in the navigation tree.



Multicast Forwarding Database Statistics	
Max MFDB Table Entries	256
Most MFDB Entries Since Last Reset	0
Current Entries	0

Figure 148: Multicast Forwarding Database Statistics

Table 130: Multicast Forwarding Database Statistics Fields

<i>Field</i>	<i>Description</i>
Max MFDB Entries	Shows the maximum number of entries that the Multicast Forwarding Database table can hold.
Most MFDB Entries Since Last Reset	The largest number of entries that have been present in the Multicast Forwarding Database table since the system was last reset. This value is also known as the MFDB high-water mark.
Current Entries	Shows the current number of entries in the Multicast Forwarding Database table.

- Click **Refresh** to update the information on the screen with the most current data.

Configuring Spanning Tree Protocol

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops. Spanning tree versions supported include Common STP, Multiple STP, and Rapid STP.

Classic STP provides a single path between end stations, avoiding and eliminating loops. For information on configuring Common STP, see [“CST Port Configuration/Status” on page 244](#).

Multiple Spanning Tree Protocol (MSTP) supports multiple instances of Spanning Tree to efficiently channel VLAN traffic over different interfaces. Each instance of the Spanning Tree behaves in the manner specified in IEEE 802.1w, Rapid Spanning Tree (RSTP), with slight modifications in the working but not the end effect (chief among the effects, is the rapid transitioning of the port to ‘Forwarding’). The difference between the RSTP and the traditional STP (IEEE 802.1D) is the ability to configure and recognize full duplex connectivity and ports which are connected to end stations, resulting in rapid transitioning of the port to ‘Forwarding’ state and the suppression of Topology Change Notification. These features are represented by the parameters ‘pointtopoint’ and ‘edgeport’. MSTP is compatible to both RSTP and STP. It behaves appropriately to STP and RSTP bridges. A MSTP bridge can be configured to behave entirely as a RSTP bridge or a STP bridge.



Note: For two bridges to be in the same region, the force version should be 802.1s and their configuration name, digest key, and revision level should match. For more information about regions and their effect on network topology, refer to the IEEE 802.1Q standard.

Switch Configuration/Status

The Spanning Tree Switch Configuration/Status page contains fields for enabling STP on the switch.

To display the Spanning Tree Switch Configuration/Status page, click **LAN > L2 Features > Spanning Tree > Switch Configuration/Status** in the navigation tree.

MST ID	VID	FID
CST	1	1

Figure 149: Spanning Tree Switch Configuration/Status

Table 131: Spanning Tree Switch Configuration/Status Fields

Field	Description
Spanning Tree Admin Mode	Enables or disables STP on the switch.
Force Protocol Version	Specifies the Force Protocol Version parameter for the switch: <ul style="list-style-type: none"> • IEEE 802.1D: Spanning Tree Protocol (STP) • IEEE 802.1w: Rapid Spanning Tree Protocol (RSTP) • IEEE 802.1s: Multiple Spanning Tree Protocol (MSTP)
Configuration Name	Name used to identify the configuration currently being used. It may be up to 32 alphanumeric characters.
Configuration Revision Level	Number used to identify the configuration currently being used. The values allowed are between 0 and 65535. The default value is 0.
Configuration Digest Key	Number used to identify the configuration currently being used. The digest key is generated based on the association of VLANs to different instances. To ensure the digest key is same on two different switches, the mapping of VLAN-to-instance must be the same.
MST ID	Table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID	This table consists of the VLAN identifier (VID) and the corresponding filtering identifier (FID) associated with each VID.
FID	Table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Refresh** to update the information on the screen with the most current data.

CST Configuration/Status

Use the Spanning Tree CST Configuration/Status page to configure Common Spanning Tree (CST) and Internal Spanning Tree on the switch.

To display the Spanning Tree CST Configuration/Status page, click **LAN > L2 Features > Spanning Tree > CST Configuration/Status** in the navigation tree.

Spanning Tree CST Configuration/Status	
Bridge Priority	32768 (0 to 61440)
Bridge Max Age (secs)	20 (6 to 40)
Bridge Hello Time (secs)	2 (1 to 10)
Bridge Forward Delay (secs)	15 (4 to 30)
Spanning Tree Maximum Hops	20 (1 to 127)
BPDU Guard	Disable
BPDU Filter	Disable
Spanning Tree Tx Hold Count	6 (1 to 10)
Bridge Identifier	80:00:00:17:9a:95:00:60
Time Since Topology Change	0 day 5 hr 21 min 14 sec
Topology Change Count	0
Topology Change	False
Designated Root	80:00:00:17:9a:95:00:60
Root Path Cost	0
Root Port	00:00
Max Age (secs)	20
Forward Delay (secs)	15
Hold Time (secs)	6
CST Regional Root	80:00:00:17:9a:95:00:60
CST Path Cost	0

Figure 150: Spanning Tree CST Configuration/Status

Table 132: Spanning Tree CST Configuration/Status Fields

Field	Description
Bridge Priority	Specifies the bridge priority value. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. The default priority is 32768. The valid range is 0-61440.

Table 132: Spanning Tree CST Configuration/Status Fields (Cont.)

Field	Description
Bridge Max Age (secs)	Specifies the switch maximum age time, which indicates the amount of time in seconds a bridge waits before implementing a topological change. The valid range is 6-40, and the value must be less than or equal to $(2 * \text{Bridge Forward Delay}) - 1$ and greater than or equal to $2 * (\text{Bridge Hello Time} + 1)$. The default value is 20.
Bridge Hello Time (secs)	Specifies the switch Hello time, which indicates the amount of time in seconds a root bridge waits between configuration messages. The valid range is 1-10, and the default value is 2. The value must be less than or equal to $(\text{Bridge Max Age} / 2) - 1$. The default hello time value is 2.
Bridge Forward Delay (secs)	Specifies the switch forward delay time, which indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The value must be greater or equal to $(\text{Bridge Max Age} / 2) + 1$. The time range is from 4 seconds to 30 seconds. The default value is 15.
Spanning Tree Maximum Hops	Specifies the maximum number of bridge hops the information for a particular CST instance can travel before being discarded.
BPDU Guard	Enable or disable the BPDU Guard. The switches behind the edge ports that have BPDU guard enabled will not be able to influence the overall STP topology. Using the BPDU Guard feature can help enforce the STP domain borders and keep the active topology be consistent and predictable.
BPUD Filter	Enable or disable the BPDU Filter. When BPDU filtering is enabled, the port drops the BPDUs received.
Spanning Tree Tx Hold Count	Configure the maximum number of BPDUs the bridge is allowed to send within the hello time window. The default value is 6.
Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Displays the total amount of time since the last topographic change. The time is displayed in hour/minute/second format, for example, 5 hours 10 minutes and 4 seconds.
Topology Changes Counts	Displays the total amount of STP state changes that have occurred.
Topology Change	Indicates whether a topology change is in progress on any port assigned to the CST. The possible values are True or False.
Designated Root	Displays the bridge identifier of the root bridge, which is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Displays the cost of the path from this bridge to the designated root.
Root Port	Indicates the root port of the selected instance.
Max Age	Shows the path Cost to the Designated Root for the CST.
Forward Delay	Shows the derived value of the Root Port Bridge Forward Delay parameter.
Hold Time	Indicates the minimum time between transmission of Configuration BPDUs.
CST Regional Root	Shows the priority and base MAC address of the CST Regional Root.
CST Path Cost	Shows the path Cost to the CST tree Regional Root.

MST Configuration/Status

Use the Spanning Tree MST Configuration/Status page to configure Multiple Spanning Tree (MST) on the switch.

To display the Spanning Tree MST Configuration/Status page, click **LAN > L2 Features > Spanning Tree > MST Configuration/Status Identification** in the navigation tree.

If no MST instances exist, or if you select Create from the **MST** field, the MST Configuration/Status page looks like the screen in [Figure 151](#).

The screenshot shows the 'Spanning Tree MST Configuration/Status' page. At the top, there is a 'Create' dropdown menu. Below it, the 'MST ID' field is set to '1' with a range of '(1 to 4094)'. A 'Submit' button is located at the bottom right of the form.

Figure 151: Spanning Tree MST Configuration/Status

[Figure 152](#) shows an example of the page with an MST instance configured.

The screenshot shows the 'Spanning Tree MST Configuration/Status' page with a configured MST instance. The 'MST' field is set to '1'. The 'Priority' field is set to '32768' with a range of '(0 to 61440)'. The 'VLAN ID' field is set to '1'. The 'Bridge Identifier' is '80:01:00:17:9a:95:00:60'. The 'Time Since Topology Change' is '0 day 5 hr 19 min 36 sec'. The 'Topology Change Count' is '0'. The 'Topology Change' field is 'False'. The 'Designated Root' is '80:01:00:17:9a:95:00:60'. The 'Root Path Cost' is '0'. The 'Root Port' is '00:00'. At the bottom, there are 'Submit', 'Delete', and 'Refresh' buttons.

Figure 152: Spanning Tree MST Configuration/Status

Table 133: Spanning Tree MST Configuration/Status

Field	Description
MST	Use the drop-down menu to create and configure a new MST or select an existing MST to display or configure.
MST ID	This is only visible when Create is selected from the MST field drop-down menu. The ID of the MST being created. Valid values for this are between 1 and 4094.
Priority	Specifies the bridge priority value for the MST. When switches or bridges are running STP, each is assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The bridge priority is a multiple of 4096. If you specify a priority that is not a multiple of 4096, the priority is automatically set to the next lowest priority that is a multiple of 4096. For example if the priority is attempted to be set to any value between 0 and 4095, it will be set to 0. The default priority is 32768. The valid range is 0-61440.
VLAN ID	This gives a list box of all VLANs on the switch. The VLANs associated with the MST instance which is selected are highlighted on the list. These can be selected or unselected for reconfiguring the association of VLANs to MST instances.
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Displays the total amount of time since the last topographic change. The time is displayed in hour/minute/second format, for example, 5 hours 10 minutes and 4 seconds.
Topology Changes Counts	Displays the total number of MST state changes that have occurred.
Topology Change	Indicates whether a topology change is in progress on any port assigned to the CST. The possible values are True or False.
Designated Root	Displays the bridge identifier of the root bridge, which is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Displays the path cost to the Designated Root for this MST instance.
Root Port	Indicates the port to access the Designated Root for this MST instance.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Force** to force the port to send out 802.1w or 802.1D BPDUs.
- Click **Refresh** to update the screen with most recent data.

CST Port Configuration/Status

Use the Spanning Tree CST Port Configuration/Status page to configure Common Spanning Tree (CST) and Internal Spanning Tree on a specific port on the switch.

To display the Spanning Tree CST Port Configuration/Status page, click **LAN > L2 Features > Spanning Tree > CST Port Configuration/Status** in the navigation tree.

Spanning Tree CST Port Configuration/Status	
Slot/Port	0/1
Port Priority	128 (0 to 240)
Admin Edge Port	Disable
Port Path Cost	0 (0 to 200000000) 0 = Auto
Auto-calculate Port Path Cost	Enabled
Hello Timer	Not Configured (1 to 10)
External Port Path Cost	0 (0 to 200000000) 0 = Auto
Auto-calculate External Prt Path Cost	Enabled
BPDU Filter	Disable
BPDU Flood	Disable
BPDU Guard Effect	Disabled
Port ID	80:01
Port Up Time Since Counters Last Cleared	0 day 0 hr 3 min 25 sec
Port Mode	Disable
Port Forwarding State	Manual forwarding
Port Role	Disabled
Designated Root	80:00:00:17:9a:95:00:60
Designated Cost	0
Designated Bridge	80:00:00:17:9a:95:00:60
Designated Port	00:00
Topology Change Acknowledge	False
Auto Edge	Disable
Edge Port	Disabled
Point-to-point MAC	True
Root Guard	Disable
Loop Guard	Disable
TCN Guard	Disable
CST Regional Root	80:00:00:17:9a:95:00:60
CST Path Cost	0
Loop Inconsistent State	False
Transitions Into Loop Inconsistent State	0
Transitions Out Of Loop Inconsistent State	0

Figure 153: Spanning Tree CST Port Configuration/Status

Table 134: Spanning Tree CST Port Configuration/Status Fields

Field	Description
Slot/Port	Select a physical or port channel interface to configure. The port is associated with the VLAN(s) associated with the CST.
Port Priority	The priority for a particular port within the CST. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the priority is automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16.
Admin Edge Port	Determines whether the specified port is an Edge Port within the CIST. It takes a value of TRUE or FALSE, where the default value is FALSE.
Port Path Cost	Set the Path Cost to a new value for the specified port in the common and internal spanning tree. It takes a value in the range of 1 to 200000000.
Auto-calculate Port Path Cost	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
Hello Timer	Specifies the switch Hello time, which indicates the amount of time in seconds a port waits between configuration messages. The valid range is 1-10, and the default value is 2. The value must be less than or equal to $(\text{Bridge Max Age} / 2) - 1$. The default hello time value is 2.
External Port Path Cost	Set the External Path Cost to a new value for the specified port in the spanning tree. It takes a value in the range of 1 to 200000000.
Auto-calculate External Port Path Cost	Displays whether the external path cost is automatically calculated (Enabled) or not (Disabled). External Path cost will be calculated based on the link speed of the port if the configured value for External Port Path Cost is zero.
BPDU Filter	Enable or disable the BPDU Filter, which filters the BPDU traffic on this port when STP is enabled on this port.
BPDU Flood	Enable or disable the BPDU Flood, which floods the BPDU traffic arriving on this port when STP is disabled on this port.
BPDU Guard Effect	If BPDU Guard is enabled for the switch and the edge port receives a BPDU, the port will be disabled and the status of this field is Enabled.
Port ID	The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
Port Up Time Since Counters Last Cleared	Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.
Port Mode	Spanning Tree Protocol Administrative Mode associated with the port or port channel. The possible values are Enable or Disable.

Table 134: Spanning Tree CST Port Configuration/Status Fields (Cont.)

Field	Description
Port Forwarding State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are: <ul style="list-style-type: none"> • Disabled: STP is currently disabled on the port. The port forwards traffic while learning MAC addresses. • Blocking: The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. • Listening: The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses. • Learning: The port is currently in the learning mode. The port cannot forward traffic, however, it can learn new MAC addresses. • Forwarding: The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.
Port Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
Designated Root	Root Bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.
Topology Change Acknowledge	Identifies whether the next BPDU to be transmitted for this port would have the topology change acknowledgement flag set. It is either "True" or "False".
Auto Edge	Configuring the auto edge mode of a port allows the port to become an edge port if it does not see BPDUs for some duration. The possible values are Enable or Disable.
Edge Port	Indicates whether the port is enabled as an edge port.
Point-to-point MAC	Derived value of the point-to-point status.
Root Guard	Configuring the root guard mode sets a port to discard any superior information received by the port and thus protect against root of the device from changing. The port gets put into discarding state and does not forward any packets. The possible values are Enable or Disable.
Loop Guard	Configuring the loop guard mode prevents a port from erroneously transitioning from blocking state to forwarding when the port stops receiving BPDUs. The port is marked as being in loop-inconsistent state. In this state, the port does not forward packets. The possible values are Enable or Disable.
TCN Guard	Configuring the TCN guard for a port restricts the port from propagating any topology change information received through that port. The possible values are Enable or Disable.
CST Regional Root	Shows the priority and base MAC address of the CST Regional Root.
CST Path Cost	Shows the path Cost to the CST tree Regional Root.
Loop Inconsistent State	Identifies whether the port is currently in a loop inconsistent state. If the port is in a loop inconsistent state, it does not forward packets.

Table 134: Spanning Tree CST Port Configuration/Status Fields (Cont.)

Field	Description
Transitions Into Loop Inconsistent State	Shows the number of times this interface has moved into a loop inconsistent state.
Transitions Out Of Loop Inconsistent State	Shows the number of times this interface has gotten out of a loop inconsistent state.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Force** to force the port to send out 802.1w or 802.1D BPDUs.
- Click **Refresh** to update the screen with most recent data.

MST Port Configuration/Status

Use the Spanning Tree MST Port Configuration/Status page to configure Multiple Spanning Tree (MST) on a specific port on the switch.

To display the Spanning Tree MST Port Configuration/Status page, click **LAN > L2 Features > Spanning Tree > MST Port Configuration /Status** in the navigation tree.



Note: If no MST instances have been configured on the switch, the page displays a “No MSTs Available” message and does not display the fields shown in [Figure 154](#).

Spanning Tree MST Port Configuration/Status

MST ID	1	
Interface	0/1	
Port Priority	128	(0 to 240)
Port Path Cost	200000	(0 to 200000000)
Auto-calculate Port Path Cost	Enabled	
Port ID	80:01	
Port Up Time Since Counters Last Cleared	0 day 0 hr 0 min 3 sec	
Port Mode	Enabled	
Port Forwarding State	Forwarding	
Port Role	Master	
Designated Root	80:01:00:17:9A:95:4E:D0	
Designated Cost	0	
Designated Bridge	80:01:00:17:9A:95:4E:D0	
Designated Port	80:01	
Loop Inconsistent State	False	
Transitions Into Loop Inconsistent State	0	
Transitions OutOf Loop Inconsistent State	0	

Figure 154: Spanning Tree MST Port Configuration/Status

Table 135: Spanning Tree MST Port Configuration/Status Fields

Field	Description
MST ID	Select an existing MST instance from drop-down list to display or configure its values.
Interface	Select a physical or port channel interface to configure. The port is associated with the VLAN(s) associated with the MST.
Port Priority	The priority for a particular port within the MST. The port priority is set in multiples of 16. If you specify a value that is not a multiple of 16, the priority is set to the priority is automatically set to the next lowest priority that is a multiple of 16. For example, if you set a value between 0 and 15, the priority is set to 0. If you specify a number between 16 and 31, the priority is set to 16.
Port Path Cost	Set the Path Cost to a new value for the specified port in the selected MST instance. It takes a value in the range of 1 to 200000000.
Auto-calculate Port Path Cost	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost is calculated based on the link speed of the port if the configured value for Port Path Cost is zero.
Port ID	The port identifier for the specified port within the CST. It is made up from the port priority and the interface number of the port.
Port Up Time Since Counters Last Cleared	Time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.
Port Mode	Shows whether STP is enabled on the port. To enable STP on a port, use the System > Port > Configuration page.
Port Forwarding State	Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are: <ul style="list-style-type: none"> • Disabled: STP is currently disabled on the port. The port forwards traffic while learning MAC addresses. • Blocking: The port is currently blocked and cannot be used to forward traffic or learn MAC addresses. • Listening: The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses. • Learning: The port is currently in the learning mode. The port cannot forward traffic, however, it can learn new MAC addresses. • Forwarding: The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses
Port Role	Each MST Bridge Port that is enabled is assigned a Port Role for each spanning tree. The port role will be one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
Designated Root	Root Bridge for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Displays cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Port	Port Identifier on the Designated Bridge that offers the lowest cost to the LAN. It is made up from the port priority and the interface number of the port.

Table 135: Spanning Tree MST Port Configuration/Status Fields (Cont.)

Field	Description
Loop Inconsistent State	This parameter identifies whether the port is in a loop inconsistent state in the specified MST instance. If the port is in a loop inconsistent state, it does not forward packets.
Transitions Into Loop Inconsistent State	Shows the number of times this interface has gone into a loop inconsistent state.
Transitions Out Of Loop Inconsistent State	Shows the number of times this interface has gotten out of a loop inconsistent state.

- If you make any configuration changes, click **Submit** to apply the new settings to the switch.
- Click **Refresh** to update the screen with most recent data.

Statistics

Use the Spanning Tree Statistics page to view information about the number and type of bridge protocol data units (BPDUs) transmitted and received on each port.

To display the Spanning Tree Statistics page, click **LAN > Monitoring > Spanning Tree > Statistics > Statistics** in the navigation tree.

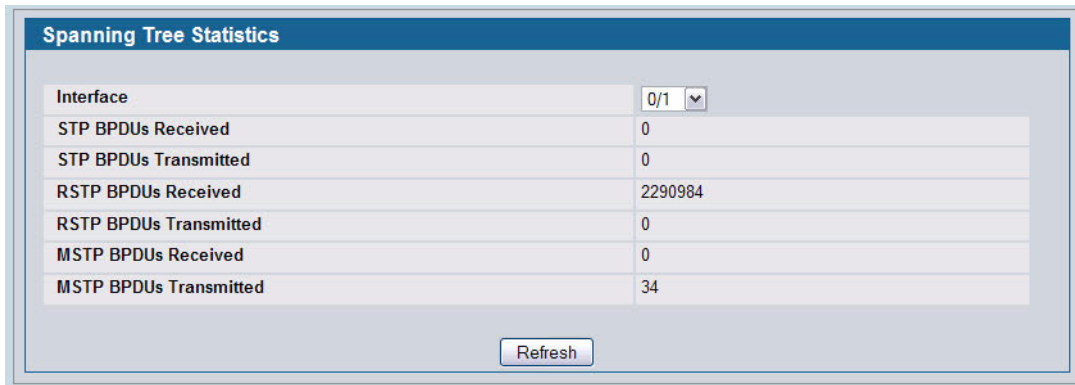


Figure 155: Spanning Tree Statistics

Table 136: Spanning Tree Statistics Fields

Field	Description
Interface	Select a physical or port channel interface to view its statistics.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Number of MSTP BPDUs transmitted from the selected port.

- Click **Refresh** to update the screen with most recent data.

Configuring DHCP Snooping

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized. You can enable DHCP snooping globally and on specific VLANs, and configure ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports. DHCP snooping enforces the following security rules:

- DHCP packets from a DHCP server (DHCP OFFER, DHCP ACK, DHCP NAK, DHCP RELEASE QUERY) are dropped if received on an untrusted port.
- DHCP RELEASE and DHCP DECLINE messages are dropped if destined for a MAC address in the snooping database, but the corresponding IP address in the snooping database is different than the interface where the message was received.
- On untrusted interfaces, the switch drops DHCP packets whose source MAC address does not match the client hardware address. This feature is a configurable option.

The hardware identifies all incoming DHCP packets on ports where DHCP snooping is enabled. DHCP snooping is enabled on a port if (a) DHCP snooping is enabled globally, and (b) the port is a member of a VLAN where DHCP snooping is enabled. On untrusted ports, the hardware traps all incoming DHCP packets to the CPU. On trusted ports, the hardware forwards client messages and copies server messages to the CPU so that DHCP snooping can learn the binding.

Global DHCP Snooping Configuration

To access the DHCP Snooping Configuration page, click **LAN > L2 Features > DHCP Snooping > Configuration** in the navigation tree.

Figure 156: DHCP Snooping Configuration

Table 137: DHCP Snooping Configuration

Field	Description
DHCP Snooping Mode	Enables or disables the DHCP Snooping feature. The default is Disable .
MAC Address Validation	Enables or disables the validation of sender MAC Address for DHCP Snooping. The default is Enable .

- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save configuration** is performed.

DHCP Snooping VLAN Configuration

The DHCP snooping application does not forward server messages because they are forwarded in hardware.

DHCP snooping forwards valid DHCP client messages received on non-routing VLANs. The message is forwarded on all trusted interfaces in the VLAN.

DHCP snooping can be configured on switching VLANs and routing VLANs. When a DHCP packet is received on a routing VLAN, the DHCP snooping application applies its filtering rules and updates the bindings database. If a client message passes filtering rules, the message is placed into the software forwarding path, where it may be processed by the DHCP relay agent, the local DHCP server, or forwarded as an IP packet.

DHCP snooping is disabled globally and on all VLANs by default. Ports are untrusted by default.

To access the DHCP Snooping VLAN Configuration page, click **LAN > L2 Features > DHCP Snooping > VLAN Configuration** in the navigation tree.

Figure 157: DHCP Snooping VLAN Configuration

Table 138: DHCP Snooping VLAN Configuration

<i>Field</i>	<i>Description</i>
VLAN ID	Select the VLAN for which information to be displayed or configured for the DHCP snooping application.
DHCP Snooping Mode	Enables or disables the DHCP snooping feature on the selected VLAN. The default is Disable .

- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save configuration** is performed.

DHCP Snooping Interface Configuration

The hardware rate limits DHCP packets sent to the CPU from untrusted interfaces to 15 packets per second. There is no hardware rate limiting on trusted interfaces.

To prevent DHCP packets from being used as a DoS attack when DHCP snooping is enabled, the snooping application enforces a rate limit for DHCP packets received on untrusted interfaces. DHCP snooping monitors the receive rate on each interface separately. If the receive rate exceeds the configuration limit, DHCP snooping brings down the interface. You must do “no shutdown” on this interface to further work with that port. You can configure both the rate and the burst interval.

The DHCP snooping application processes incoming DHCP messages. For DHCPRELEASE and DHCPDECLINE messages, the application compares the receive interface and VLAN with the client's interface and VLAN in the binding database. If the interfaces do not match, the application logs the event and drops the message. For valid client messages, DHCP snooping compares the source MAC address to the DHCP client hardware address. Where there is a mismatch, DHCP snooping logs and drops the packet. You can disable this feature using the DHCP Snooping Interface Configuration page, shown in [Figure 158](#) below, or by using the `no ip dhcp snooping verify mac-address` command. DHCP snooping forwards valid client messages on trusted members within the VLAN. If DHCP relay and/or DHCP server co-exist with the DHCP snooping, the DHCP client message will be sent to the DHCP relay and/or DHCP server to process further.

To access the DHCP Snooping Interface Configuration page, click **LAN > L2 Features > DHCP Snooping > Interface Configuration** in the navigation tree.

Figure 158: DHCP Snooping Interface Configuration

Table 139: DHCP Snooping Interface Configuration

<i>Field</i>	<i>Description</i>
Interface	Select the interface for which data is to be displayed or configured.
Trust State	If it is enabled, the DHCP snooping application considers the port as trusted. The default is Disable .
Logging Invalid Packets	If it is enabled, the DHCP snooping application logs invalid packets on this interface. The default is Disable .
Rate Limit	Specifies the rate limit value for DHCP snooping purposes. If the incoming rate of DHCP packets exceeds the value of this object for consecutively burst interval seconds, the port will be shutdown. If this value is None , there is no limit. The default is 15 packets per second (pps). The Rate Limit range is 0 to 300.
Burst Interval	Specifies the burst interval value for rate limiting purposes on this interface. If the rate limit is None , the burst interval has no meaning and displays it as "N/A". The default is 1 second . The Burst Interval range is 1 to 15.

- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a **Save configuration** is performed.

Managing LLDP

The IEEE 802.1AB defined standard, Link Layer Discovery Protocol (LLDP), allows stations residing on an 802 LAN to advertise major capabilities and physical descriptions. This information is viewed by a network manager to identify system topology and detect bad configurations on the LAN.

LLDP is a one-way protocol; there are no request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function. The transmit and receive functions can be enabled/disabled separately per port. By default, both transmit and receive are disabled on all ports. The application is responsible for starting each transmit and receive state machine appropriately, based on the configured status and operational state of the port.

D-Link DWS-4000 Series allows LLDP to have multiple LLDP neighbors per interface. The number of such neighbors is limited by the memory constraints. A product-specific constant defines the maximum number of neighbors supported by the switch. There is no restriction on the number of neighbors supported on a per LLDP port. If all the remote entries on the switch are filled up, then the new neighbors are ignored. In case of multiple VOIP devices on a single interface, the 802.1ab component sends the Voice VLAN configuration to all the VoIP devices.

Global Configuration

Use the LLDP Global Configuration page to specify LLDP parameters that are applied to the switch.

To display the LLDP Global Configuration page, click **LAN > L2 Features > LLDP > Global Configuration** in the navigation tree.

LLDP Global Configuration		
Transmit Interval	<input type="text" value="30"/>	(1 to 32768 secs)
Transmit Hold Multiplier	<input type="text" value="4"/>	(2 to 10 secs)
Re- Initialization Delay	<input type="text" value="2"/>	(1 to 10 secs)
Notification Interval	<input type="text" value="5"/>	(5 to 3600 secs)
<input type="button" value="Submit"/>		

Figure 159: LLDP Global Configuration

Table 140: LLDP Global Configuration Fields

Field	Description
Transmit Interval	Specifies the interval at which LLDP frames are transmitted. The default is 30 seconds, and the valid range is 1-32768 seconds.
Transmit Hold Multiplier	Specifies multiplier on the transmit interval to assign to TTL. The default is 4, and the range is 2-10.
Re-Initialization Delay	Specifies the delay before a re-initialization. The default is 2 seconds, and the range is 1-10 seconds.
Notification Interval	Limits the transmission of notifications. The default is 5 seconds, and the range is 5-3600 seconds.

- If you make any changes to the page, click **Submit** to apply the new settings to the system.

Interface Configuration

Use the LLDP Interface Configuration page to specify LLDP parameters that are applied to a specific interface.

To display the LLDP Interface Configuration page, click **LAN > L2 Features > LLDP > Interface Configuration** in the navigation tree.

Figure 160: LLDP Interface Configuration

Table 141: LLDP Interface Configuration Fields

Field	Description
Interface	Specifies the port to be affected by these parameters.
Transmit	Enables or disables the transmission of LLDP protocol data units (PDUs). The default is disabled.
Receive	Enables or disables the ability of the port to receive LLDP PDUs. The default is disabled.
Notify	When notifications are enabled, LLDP interacts with the Trap Manager to notify subscribers of remote data change statistics. The default is disabled.
Transmit Management Information	Select the check box to enable the transmission of management address instance. Clear the check box to disable management information transmission. The default is disabled.
Optional TLV(s)	Select each check box next to the type-length value (TLV) information to transmit. Choices include: <ul style="list-style-type: none"> • System Name. To include system name TLV in LLDP frames. To configure the System Name, see “System Description” on page 63. • System Description. To include system description TLV in LLDP frames. • System Capabilities. To include system capability TLV in LLDP frames. • Port Description. To include port description TLV in LLDP frames. To configure the Port Description, see “Port Description” on page 109

- If you make any changes to the page, click **Submit** to apply the new settings to the system.

Interface Summary

Use the LLDP Interface Summary page to view the LLDP parameters configured on each physical port on the system.

To display the LLDP Interface Summary page, click **LAN > Monitoring > LLDP Status > Interface Summary** in the navigation tree.



Interface	Link Status	Transmit	Receive	Notify	Optional TLV(s)	Transmit Management Information
0/1	Link Up	Enabled	Enabled	Enabled		No
0/2	Link Down	Disabled	Disabled	Disabled		No
0/3	Link Down	Disabled	Disabled	Disabled		No
0/4	Link Down	Disabled	Disabled	Disabled		No
0/5	Link Down	Disabled	Disabled	Disabled		No

Figure 161: LLDP Interface Summary

Table 142: LLDP Interface Summary Fields

Field	Description
Interface	Displays all the ports on which LLDP-802.1AB can be configured.
Link Status	Displays whether the link status of the ports is up or down.
Transmit	Displays the LLDP-802.1AB transmit mode of the interface.
Receive	Displays the LLDP-802.1AB receive mode of the interface.
Notify	Displays the LLDP-802.1AB notification mode of the interface.
Optional TLV(s)	Shows the LLDP-802.1AB optional type-length values (TLV) that are included. If no TVLs are sent, the entry is blank. The field can contain one or more of the following TVLs. <ul style="list-style-type: none"> • System Name • System Capabilities • System Description • Port Description.
Transmit Management Information	Shows whether the management address is transmitted in the LLDP frames.

- To update the page with the latest data, click **Refresh**.

Statistics

Use the LLDP Statistics page to view the global and interface LLDP statistics.

To display the LLDP Statistics page, click **LAN > Monitoring > LLDP Status > Statistics** in the navigation tree.

The screenshot shows the 'LLDP Statistics' page with a blue header. It contains a summary section with the following values:

- Last Update: 0 Days 00:00:00
- Total Inserts: 0
- Total Deletes: 0
- Total Drops: 0
- Total Ageouts: 0

Below this is a table with the following columns: Interface, Transmit Total, Receive Total, Discards, Errors, Ageouts, TLV Discards, TLV Unknowns, TLV MED, TLV 802.1, and TLV 802.3. The data row shows Interface 0/1 with Transmit Total 1782 and all other values at 0. At the bottom are 'Refresh' and 'Clear' buttons.

Interface	Transmit Total	Receive Total	Discards	Errors	Ageouts	TLV Discards	TLV Unknowns	TLV MED	TLV 802.1	TLV 802.3
0/1	1782	0	0	0	0	0	0	0	0	0

Figure 162: LLDP Statistics

Table 143: LLDP Statistics Fields

Field	Description
System-wide Statistics	
Last Update	Displays the time when an entry was created, modified, or deleted in the tables associated with the remote systems.
Total Inserts	Displays the number of times a complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into the tables associated with the remote systems.
Total Deletes	Displays the number of times a complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from the tables associated with the remote systems.
Total Drops	Displays the number of times a complete set of information advertised by a particular MAC Service Access Point (MSAP) could not be entered into tables associated with the remote systems because of insufficient resources.
Total Ageouts	Displays the number of times a complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with the remote systems because the information timelines interval has expired.
Port Statistics	
Interface	Displays the slot/port for the interfaces.
Transmit Total	Displays the total number of LLDP frames transmitted by the LLDP agent on the corresponding port.
Receive Total	Displays the total number of valid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Discards	Displays the number of LLDP TLVs discarded for any reason by the LLDP agent on the corresponding port.

Table 143: LLDP Statistics Fields (Cont.)

Field	Description
Errors	Displays the number of invalid LLDP frames received by the LLDP agent on the corresponding port, while the LLDP agent is enabled.
Ageouts	Displays the number of age-outs that occurred on a given port. An age-out is the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been deleted from tables associated with remote entries because the information timeliness interval had expired.
TLV Discards	Displays the number of LLDP TLVs (Type, Length, Value sets) discarded for any reason by the LLDP agent on the corresponding port.
TLV Unknowns	Displays the number of LLDP TLVs received on the local ports which were not recognized by the LLDP agent on the corresponding port.
TLV MED	Displays the total number of LLDP-MED TLVs received on the local ports.
TLV 802.1	Displays the total number of LLDP TLVs received on the local ports which are of type 802.1.
TLV 802.3	Displays the total number of LLDP TLVs received on the local ports which are of type 802.3.

- Click **Refresh** to update the page with the most current information.
- Click **Clear** to clear the LLDP statistics of all the interfaces.

Local Device Information

Use the LLDP Local Device Information page to view the data that each port advertises through LLDP.

To display the LLDP Local Device Information page, click **LAN > Monitoring > LLDP Status > Local Device Information** in the navigation tree.

LLDP Local Device Information	
Interface	0/1
Chassis ID Subtype	MAC Address
Chassis ID	00:17:9A:95:00:60
Port ID Subtype	MAC Address
Port ID	00:17:9A:95:00:62
System Name	
System Description	Broadcom FASTPATH Routing
Port Description	
System Capabilities Supported	bridge, router
System Capabilities Enabled	bridge
Management Address	10.27.64.222
Management Address Type	IPv4

Figure 163: LLDP Local Device Information

Table 144: LLDP Local Device Information Fields

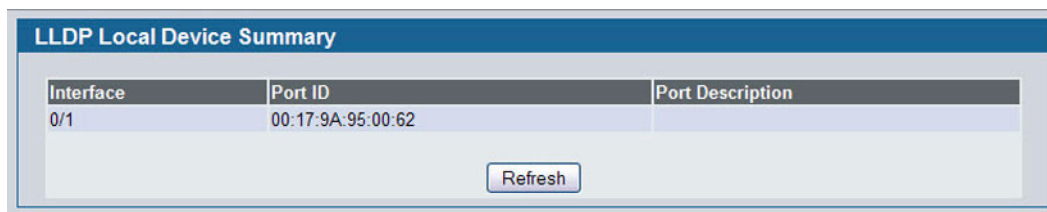
Field	Description
Interface	Select from the list of all the ports on which LLDP-802.1AB frames can be transmitted.
Chassis ID Subtype	Displays the string that describes the source of the chassis identifier.
Chassis ID	Displays the string value used to identify the chassis component associated with the local system.
Port ID Subtype	Displays the string describing the source of the port identifier.
Port ID	Identifies the physical address of the port.
System Name	Displays the system name of the local system.
System Description	Displays the description of the selected port associated with the local system.
Port Description	Displays the user-defined description of the port.
System Capabilities Supported	Displays the system capabilities of the local system.
System Capabilities Enabled	Displays the system capabilities of the local system which are supported and enabled.
Management Address	Displays the advertised management address of the local system.
Management Address Type	Specifies the type of the management address.

- Click **Refresh** to update the information on the screen with the most current data.

Local Device Summary

Use the LLDP Local Device Summary page to view information about all interfaces on the device that are enabled to transmit LLDP information.

To display the LLDP Local Device Summary page, click **LAN > Monitoring > LLDP Status > Local Device Summary** in the navigation tree.



LLDP Local Device Summary		
Interface	Port ID	Port Description
0/1	00:17:9A:95:00:62	

Figure 164: LLDP Local Device Summary

Table 145: LLDP Local Device Summary Columns

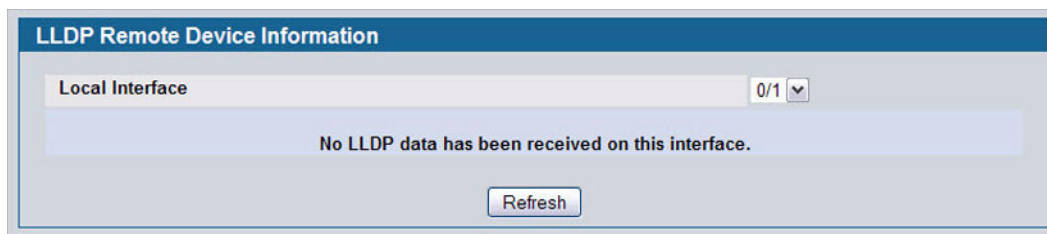
Field	Description
Interface	Displays the slot/port on which LLDP-802.1AB frames can be transmitted.
Port ID	Displays the string describing the source of the port identifier.
Port Description	Displays the description of the port associated with the local system.

- Click **Refresh** to update the information on the screen with the most current data.

Remote Device Information

Use the LLDP Remote Device Information page to view the data that a specified interface has received from other LLDP-enabled systems.

To display the LLDP Remote Device Information page, click **LAN > Monitoring > LLDP Status > Remote Device Information** in the navigation tree.

**Figure 165: LLDP Remote Device Information****Table 146: LLDP Remote Device Information Fields**

Field	Description
Local Interface	Select the slot/port on the local system to display the LLDP information it has received. Note: If no LLDP data has been received on the select interface, then a message stating so displays. If the selected interface has received LLDP information from a remote device, the following fields display:
Remote ID	Displays the remote client identifier assigned to the remote system.
Chassis ID Subtype	Identifies the type of data displayed in the Chassis ID field on the remote system.
Chassis ID	Identifies the chassis component associated with the remote system.
Port ID Subtype	Identifies the type of data displayed in the remote system's Port ID field.
Port ID	Identifies the physical address of the port on the remote system from which the data was sent.
System Name	Identifies the system name of the remote system.
System Description	Displays the description of the selected port associated with the remote system.

Table 146: LLDP Remote Device Information Fields (Cont.)

Field	Description
Port Description	Displays the user-defined description of the port.
System Capabilities Supported	Displays the system capabilities of the remote system.
System Capabilities Enabled	Displays the system capabilities of the remote system which are supported and enabled.
Time to Live	Displays the Time to Live value in seconds of the received remote entry.
Management Address	Displays the advertised management address of the remote system.
Management Address Type	Displays the type of the management address.

- Click **Refresh** to update the information on the screen with the most current data.

Remote Device Summary

Use the LLDP Remote Device Summary page to view information about all interfaces on the device that are enabled to transmit LLDP information.

To display the LLDP Remote Device Summary page, click **LAN > Monitoring > LLDP Status > Remote Device Summary** in the navigation tree.

LLDP Remote Device Summary				
Local Interface	Chassis ID	Port ID	Remote ID	System Name
0/1		0		

Figure 166: LLDP Remote Device Summary**Table 147: LLDP Remote Device Summary Columns**

Field	Description
Local Interface	Shows the slot/port on the local system that can receive LLDP frames advertised by a remote system.
Chassis ID	Identifies the chassis component associated with the remote system.
Port ID	Identifies the physical address of the port on the remote device that sent the LLDP data.
Remote ID	Shows the remote client identifier assigned to the remote system.
System Name	Shows the system name of the remote device. If the system name is not configured, the field is blank.

- Click **Refresh** to update the information on the screen with the most current data.

LLDP-MED

The Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP that features:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and DiffServ settings), enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet endpoints.
- Inventory management, enabling network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial/asset number).

LLDP-MED Global Configuration

Use this page to set global parameters for LLDP-MED operation. To display this page, click **LAN > L2 Features > LLDP > LLDP-MED > Global Configuration** in the navigation tree.

Figure 167: LLDP Global Configuration

Table 148: LLDP Global Configuration Fields

Field	Description
Fast Start Repeat Count	Specifies the number of LLDP PDUs that will be transmitted when the protocol is enabled. The range is from (1 to 10). The default value is 3.
Device Class	Specifies local device's MED Classification. The following three represent the actual endpoints: <ul style="list-style-type: none"> • Class I Generic [IP Communication Controller etc.] • Class II Media [Conference Bridge etc.] • Class III Communication [IP Telephone etc.] The fourth device is Network Connectivity Device, which is typically a LAN switch/router, IEEE 802.1 bridge, IEEE 802.11 wireless access point, etc.

- Click **Submit** to update the switch. The changes take effect but will not be retained across a power cycle unless a save is performed.

LLDP-MED Interface Configuration

Use this page to enable LLDP-MED mode on an interface and configure its properties. To display this page, click **LAN > L2 Features > LLDP > LLDP-MED > Interface Configuration** in the navigation tree.

Figure 168: LLDP-MED Interface Configure

Table 149: LLDP-MED Interface Configuration Fields

Field	Description
Interface	Selects the port that you want to configure LLDP-MED - 802.1AB on. You can select All to configure all interfaces on the DUT with the same properties. To view the summary of all interfaces, refer to the “LLDP-MED Interface Summary” on page 265 . The Interface Configuration page will not be able to display the summary of ‘All’ interfaces. The summary of individual interfaces is visible from the Interface Configuration page. The Interface Configuration page for the ‘All’ option will always display the LLDP-MED mode and notification mode as ‘disabled’ and check boxes for ‘Transmit TLVs’ will always be unchecked.
LLDP-MED Mode	Enables or disables LLDP-MED mode for the selected interface. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.
Config Notification Mode	Enables or disables LLDP-MED topology change notification mode for the selected interface.
Transmit TLVs	Specifies which optional type length values (TLVs) in the LLDP-MED will be transmitted in the LLDP PDUs frames for the selected interface: <ul style="list-style-type: none"> • MED Capabilities: Transmits the capabilities TLV in LLDP frames. • Network Policy: Transmits the network policy TLV in LLDP frames. • Location Identification: Transmits the location TLV in LLDP frames. • Extended Power via MDI - PSE: Transmits the extended PSE TLV in LLDP frames. • Extended Power via MDI - PD: Transmits the extended PD TLV in LLDP frames. • Inventory: Transmits the inventory TLV in LLDP frames.

- Click **Submit** to send the updated configuration to the switch. These changes take effect immediately but will not be retained across a power cycle unless a save is performed.

LLDP-MED Interface Summary

This page lists each switch interface and its LLDP configuration status. To display this page, click **LAN > Monitoring > LLDP Status > LLDP-MED > Interface Summary** in the navigation tree.

Interface	Link Status	MED Status	Operational Status	Notification Status	Transmit TLVs
0/1	Up	Disable	Disable	Disable	Capabilities Network Policy
0/2	Down	Disable	Disable	Disable	Capabilities Network Policy
0/3	Down	Disable	Disable	Disable	Capabilities Network Policy
0/4	Down	Disable	Disable	Disable	Capabilities Network Policy
0/5	Down	Disable	Disable	Disable	Capabilities

Figure 169: LLDP-MED Interface Summary

Table 150: LLDP-MED Interface Summary Fields

Field	Description
Interface	Specifies all the ports on which LLDP-MED can be configured.
Link Status	Specifies the link status of the ports as Up/Down.
MED Status	Specifies the transmit and/or receive LLDP-MED mode is enabled or disabled on this interface.
Operational Status	Specifies whether the interface will transmit TLVs.
Notification Status	Specifies the LLDP-MED topology notification mode of the interface.
Transmit TLVs	Specifies the LLDP-MED transmit TLV(s) that are included.

- Click **Refresh** to update the page with the latest information from the router.

LLDP Local Device Information

This page displays information on LLDP-MED information advertised on the selected local interface. To display this page, click **LAN > Monitoring > LLDP Status > LLDP-MED > Local Device Information** in the navigation tree.

Figure 170: LLDP-MED Local Device Information

Table 151: LLDP-MED Local Device Information Fields

Field	Description
Interface	Select from the list of all the ports on which LLDP-MED frames can be transmitted.
Network Policy Information	Specifies if network policy TLV is present in the LLDP frames: <ul style="list-style-type: none"> • Media Application Type: Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, vidosignalling. Each application type that is received has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been transmitted only then would this information be displayed. • Vlan Id: Specifies the VLAN id associated with a particular policy type. • Priority: Specifies the priority associated with a particular policy type. • DSCP: Specifies the DSCP associated with a particular policy type. • Unknown Bit Status: Specifies the unknown bit associated with a particular policy type. • Tagged Bit Status: Specifies the tagged bit associated with a particular policy type.

Table 151: LLDP-MED Local Device Information Fields (Cont.)

Field	Description
Inventory	Specifies the inventory TLV present in LLDP frames: <ul style="list-style-type: none">• Hardware Revisions. Specifies hardware version.• Firmware Revisions. Specifies firmware version.• Software Revisions. Specifies software version.• Serial Number. Specifies serial number.• Manufacturer Name. Specifies manufacturer's name.• Model Name. Specifies model name.• Asset ID. Specifies asset ID.
Location Information	Specifies if location TLV is present in LLDP frames: <ul style="list-style-type: none">• Sub Type: Specifies type of location information.• Location Information: Specifies the location information as a string for given type of location ID.

- Click **Refresh** to update the page with the latest information from the router.

LLDP-MED Remote Device Information

This page displays information on LLDP-MED information received from remote clients on the selected local interface. To display this page, click **LAN > Monitoring > LLDP Status > LLDP-MED > Remote Device Information** in the navigation tree.

Figure 171: LLDP Remote Device Information

Table 152: LLDP-MED Remote Device Information Fields

Field	Description
Local Interface	Specifies the list of all the ports on which LLDP-MED is enabled.
Remote ID	Specifies the remote client identifier assigned to the remote system.
Capability Information	Specifies the supported and enabled capabilities that were received in MED TLV on this port: <ul style="list-style-type: none"> • Supported Capabilities: Specifies supported capabilities that were received in MED TLV on this port. • Enabled Capabilities: Specifies enabled capabilities that were received in MED TLV on this port. • Device Class: Specifies device class as advertised by the device remotely connected to the port.

Table 152: LLDP-MED Remote Device Information Fields (Cont.)

Field	Description
Network Policy Information	<p>Specifies if network policy TLV is received in the LLDP frames on this port:</p> <ul style="list-style-type: none"> • Media Application Type: Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streamingvideo, vidoesignalling. Each application type that is received has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been received on this port, only then would this information be displayed. • Vlan ID: Specifies the VLAN ID associated with a particular policy type. • Priority: Specifies the priority associated with a particular policy type. • DSCP: Specifies the DSCP associated with a particular policy type. • Unknown Bit Status: Specifies the unknown bit associated with a particular policy type. • Tagged Bit Status: Specifies the tagged bit associated with a particular policy type.
Inventory	<p>Specifies the inventory TLV is received in LLDP frames on this port:</p> <ul style="list-style-type: none"> • Hardware Revisions. Specifies hardware version of the remote device. • Firmware Revisions. Specifies firmware version of the remote device. • Software Revisions. Specifies software version of the remote device. • Serial Number. Specifies serial number of the remote device. • Manufacturer Name. Specifies manufacturer's name of the remote device. • Model Name. Specifies model name of the remote device. • Asset ID. Specifies asset ID of the remote device.
Location Information	<p>Specifies if location TLV is received in LLDP frames on this port.</p> <ul style="list-style-type: none"> • Sub Type: Specifies type of location information. • Location Information: Specifies the location information as a string for given type of location ID.
Extended PoE	<p>Specifies if remote device is a PoE device.</p> <ul style="list-style-type: none"> • Device Type. Specifies the remote device's PoE device type connected to this port.
Extended PoE PSE	<p>Specifies if extended PSE TLV is received in LLDP frame on this port:</p> <ul style="list-style-type: none"> • Available: Specifies the remote port's power sourcing equipment's (PSE) power value in tenths of watts. • Source: Specifies the remote port's PSE power source. • Priority: Specifies the remote port's PSE power priority.
Extended PoE PD	<p>Specifies if extended PD TLV is received in LLDP frame on this port.</p> <ul style="list-style-type: none"> • Required: Specifies the remote port's power device power requirement. • Source: Specifies the remote port's PD power source. • Priority: Specifies the remote port's PD power priority.

- Click **Refresh** to update the page with the latest information from the router.

Configuring Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

DAI Configuration

Use the DAI Configuration page to configure global DAI settings.

To display the DAI Configuration page, click **LAN > L2 Features > Dynamic ARP Inspection > DAI Configuration** in the navigation tree.

Figure 172: Dynamic ARP Inspection Configuration

Table 153: Dynamic ARP Inspection Configuration

Field	Description
Validate Source MAC	Select the DAI Source MAC Validation Mode for the switch. If you select Enable , Sender MAC validation for the ARP packets will be enabled. The default is Disable .
Validate Destination MAC	Select the DAI Destination MAC Validation Mode for the switch. If you select Enable , Destination MAC validation for the ARP Response packets will be enabled. The default is Disable .
Validate IP	Select the DAI IP Validation Mode for the switch. If you select Enable , IP Address validation for the ARP packets will be enabled. The default is Disable .

- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.

DAI VLAN Configuration

Use the DAI VLAN Configuration page to select the DAI-capable VLANs for which information is to be displayed or configured.

To display the DAI Configuration page, click **LAN > L2 Features > Dynamic ARP Inspection > DAI VLAN Configuration** in the navigation tree.

Figure 173: Dynamic ARP Inspection VLAN Configuration

Table 154: Dynamic ARP Inspection VLAN Configuration

<i>Field</i>	<i>Description</i>
VLAN ID	Select the VLAN ID for which information is to be displayed or configured.
Dynamic ARP Inspection	Select whether Dynamic ARP Inspection is Enabled or Disabled on this VLAN. The default is Disable .
Logging Invalid Packets	Select whether Dynamic ARP Inspection logging is Enabled or Disabled on this VLAN. The default is Disable .
ARP ACL Name	The name of the ARP Access List. A VLAN can be configured to use this ARP ACL containing rules as the filter for ARP packet validation. The name can contain 1-31 alphanumeric characters.
Static Flag	Use this flag to determine whether the ARP packet needs validation using the DHCP snooping database, in case the ARP ACL rules do not match. If Enabled , then the ARP Packet will be validated by the ARP ACL Rules only. If Disabled , then the ARP Packet needs further validation by using the DHCP Snooping entries. The default is Disable .

- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Refresh** to refresh the page with the most current data from the switch.

DAI Interface Configuration

Use the DAI Interface Configuration page to select the DAI Interface for which information is to be displayed or configured.

To display the DAI Interface Configuration page, click **LAN > L2 Features > Dynamic ARP Inspection > DAI Interface Configuration** in the navigation tree.

Figure 174: Dynamic ARP Inspection Interface Configuration

Table 155: Dynamic ARP Inspection Interface Configuration

Field	Description
Slot/Port	Select the physical interface for which data is to be displayed or configured.
Trust State	Indicates whether the interface is trusted for Dynamic ARP Inspection. If you select Enable , the interface is trusted. ARP packets coming to this interface will be forwarded without checking. If you select Disable , the interface is not trusted. ARP packets coming to this interface will be subjected to ARP inspection. The default is Disable .
Rate Limit	Specify the rate limit value for Dynamic ARP Inspection. If the incoming rate exceeds the Rate Limit value for consecutively burst interval seconds, ARP packets will be dropped. If the value is None , there is no limit. The default is 15 packets per second (pps).
Burst Interval	Specify the burst interval for rate limiting on this interface. If the Rate Limit is None , then Burst Interval has no meaning and shows as N/A (Not Applicable). The default is 1 second.

- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Refresh** to refresh the page with the most current data from the switch.

DAI ARP ACL Configuration

Use the DAI ARP ACL Configuration page to add or remove DAI ARP ACLs.

To display the DAI ARP ACL Configuration page, click **LAN > L2 Features > Dynamic ARP Inspection > DAI ARP ACL Configuration** in the navigation tree.

Figure 175: Dynamic ARP Inspection ARP ACL Configuration

Table 156: Dynamic ARP Inspection ARP ACL Configuration

Field	Description
ARP ACL Name	Use this field to create a new ARP ACL for Dynamic ARP Inspection. The name can be 1 to 31 alphanumeric characters in length.
ARP ACL List	Displays by name a list of all the configured ARP ACLs. Use the Remove column, to select the particular ACLs you want to delete.

- Click **Add** to create a new ARP ACL.
- Click **Delete** to remove the configured ARP ACL entry you selected in the **Remove** column.
- Click **Refresh** to refresh the page with the most current data from the switch.

DAI ARP ACL Rule Configuration

Use the DAI ARP ACL Rule Configuration page to add or remove DAI ARP ACL Rules.

To display the DAI ARP ACL Rule Configuration page, click **LAN > L2 Features > Dynamic ARP Inspection > DAI ARP ACL Rule Configuration** in the navigation tree.

Figure 176: Dynamic ARP Inspection ARP ACL Rule Configuration

Table 157: Dynamic ARP Inspection ARP ACL Rule Configuration

Field	Description
ARP ACL Name	Select the ARP ACL for which information is to be displayed or configured.
Sender IP Address	To create a new rule for the selected ARP ACL, enter in this field the Sender IP Address match value for the ARP ACL.
Sender MAC Address	To create a new rule for the selected ARP ACL, enter in this field the Sender MAC Address match value for the ARP ACL.
Remove	Use the Remove column to select the particular ARP ACL Rules you want to delete.

- Click **Add** to add a new ARP ACL rule.
- Click **Submit** to delete the entries selected in the **Remove** column.
- Click **Refresh** to refresh the page with the most current data from the switch.

Dynamic ARP Inspection Statistics

Use the **Dynamic ARP Inspection (DAI) Statistics** page to display the statistics per VLAN.

To display the DAI Statistics page, click **LAN > Monitoring > Dynamic ARP Inspection Statistics** in the navigation tree.

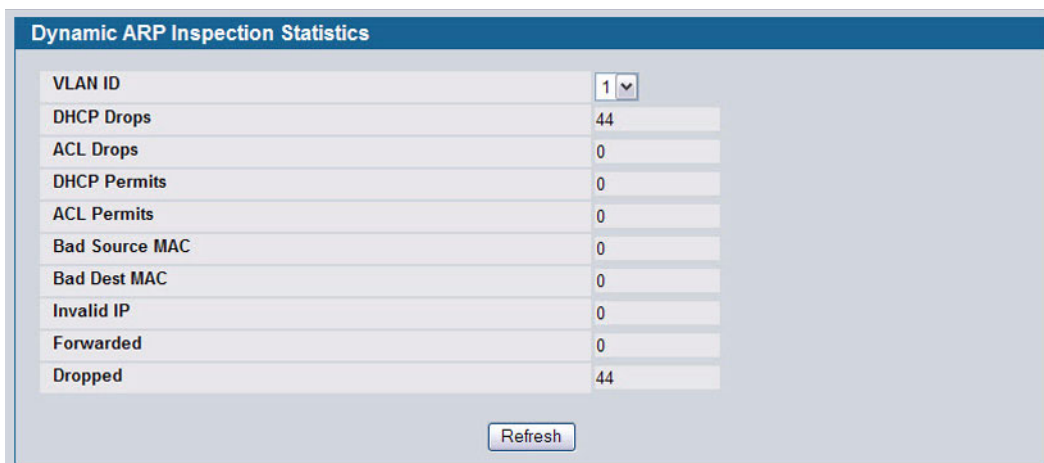


Figure 177: Dynamic ARP Inspection Statistics

Table 158: Dynamic ARP Inspection Statistics

Field	Description
VLAN ID	Select the DAI-enabled VLAN ID for which to display statistics.
DHCP Drops	The number of ARP packets that were dropped by DAI because there was no matching DHCP snooping binding entry found.
ACL Drops	The number of ARP packets that were dropped by DAI because there was no matching ARP ACL rule found for this VLAN and the static flag is set on this VLAN.
DHCP Permits	The number of ARP packets that were forwarded by DAI because there was a matching DHCP snooping binding entry found.
ACL Permits	The number of ARP packets that were permitted by DAI because there was a matching ARP ACL rule found for this VLAN.
Bad Source MAC	The number of ARP packets that were dropped by DAI because the sender MAC address in the ARP packet did not match the source MAC in the Ethernet header.
Bad Dest MAC	The number of ARP packets that were dropped by DAI because the target MAC address in the ARP reply packet did not match the destination MAC in the Ethernet header.
Invalid IP	The number of ARP packets that were dropped by DAI because the sender IP address in the ARP packet or target IP address in the ARP reply packet is not valid. Not valid addresses include 0.0.0.0, 255.255.255.255, IP multicast addresses, class E addresses (240.0.0.0/4), and loopback addresses (127.0.0.0/8).
Forwarded	The number of valid ARP packets forwarded by DAI.
Dropped	The number of not valid ARP packets dropped by DAI.

- Click **Refresh** to refresh the page with the most current data from the switch.

Section 5: Configuring L3 Features

The D-Link Unified Switch supports IP routing. Use the pages in the LAN > L3 Features navigation tree folder to manage routing on the system. This section contains the following information:

- [“Managing the BOOTP/DHCP Relay Agent”](#)
- [“Configuring the IP Helper Features”](#)
- [“Configuring ARP”](#)
- [“Configuring Global and Interface IP Settings”](#)
- [“Configuring RIP”](#)
- [“Router Discovery”](#)
- [“Router”](#)
- [“VLAN Routing”](#)
- [“Virtual Router Redundancy Protocol \(VRRP\)”](#)
- [“Configuring Quality of Service”](#)

When a packet enters the switch, the destination MAC address is checked to see if it matches any of the configured routing interfaces. If it does, then the silicon searches the host table for a matching destination IP address. If an entry is found, then the packet is routed to the host. If there is not a matching entry, then the switch performs a longest prefix match on the destination IP address. If an entry is found, then the packet is routed to the next hop. If there is no match, then the packet is routed to the next hop specified in the default route. If there is no default route configured, then the packet is passed to the CPU to be handled appropriately.

The routing table can have entries added either statically by the administrator or dynamically via a routing protocol. The host table can have entries added either statically by the administrator or dynamically via ARP.

Managing the BOOTP/DHCP Relay Agent

The BootP/DHCP Relay Agent enables BootP/DHCP clients and servers to exchange BootP/DHCP messages across different subnets. The relay agent receives the requests from the clients, and checks the valid hops and giaddr fields. If the number of hops is greater than the configured, the agent assumes the packet has looped through the agents and discards the packet. If giaddr field is zero the agent must fill in this field with the IP address of the interface on which the request was received. The agent unicasts the valid packets to the next configured destination. The server responds with a unicast BOOTREPLY addressed to the relay agent closest to the client as indicated by giaddr field. Upon reception of the BOOTREPLY from the server, the agent forwards this reply as broadcast or unicast on the interface that had received the BOOTREQUEST. This interface can be identified by giaddr field.

The DWS-4000 Series switch also supports DHCP relay agent options to identify the source circuit when customers are connected to the Internet with high-speed modem. The relay agent inserts these options when forwarding the request to the server and removes them when sending the reply to the clients.

If an interface has more than one IP address, the relay agent should use the primary IP address configured as its relay agent IP address.

BootP/DHCP Relay Agent Configuration

Use the BOOTP/DHCP Relay Agent Configuration page to configure and display a BOOTP/DHCP relay agent.

To display the page, click **LAN > L3 Features > BOOTP/DHCP Relay Agent > Configuration** in the navigation tree.



Figure 178: BOOTP/DHCP Relay Agent Configuration

Table 159: BOOTP/DHCP Relay Agent Configuration Fields

Field	Description
Maximum Hop Count	Enter the maximum number of hops a client request can take before being discarded.
Minimum Wait Time (secs)	Enter a time in seconds. This value is compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets are only forwarded when the time stamp exceeds the minimum wait time.
Circuit ID Option Mode	Select Enable or Disable from the dropdown menu. If you select Enable, the relay agent adds Option 82 header packets to the DHCP Request packets before forwarding them to the server, and strips them off while forwarding the responses to the client.

- If you make any changes to the page, click **Submit** to apply the changes to the system.

BOOTP/DHCP Relay Agent Status

Use the BOOTP/DHCP Relay Agent Status page to display the BOOTP/DHCP Relay Agent configuration and status information.

To display the page, click **LAN > Monitoring > L3 Status > BOOTP/DHCP Relay Agent Status** in the navigation tree.



BOOTP/DHCP Relay Agent Status	
Maximum Hop Count	4
Server IP Address	0.0.0.0
Admin Mode	Disable
Minimum Wait Time (secs)	0
Circuit ID Option Mode	Disable
Requests Received	0
Requests Relayed	0
Packets Discarded	0

Figure 179: BOOTP/DHCP Relay Agent Status

Table 160: BOOTP/DHCP Relay Agent Status Fields

Field	Description
Maximum Hop Count	The maximum number of Hops a client request can go without being discarded.
Server IP Address	The IP address of the BOOTP/DHCP server or the IP address of the next BOOTP/DHCP Relay Agent.
Admin Mode	The administrative mode of the relay. When you select Enable on the configuration page, BOOTP/DHCP requests are forwarded to the IP address you entered in the Server IP address field.
Minimum Wait Time (secs)	The Minimum time in seconds. This value is compared to the time stamp in the client's request packets, which should represent the time since the client was powered up. Packets are only forwarded when the time stamp exceeds the minimum wait time.
Circuit ID Option Mode	This is the Relay agent option, which can be either Enabled or Disabled. If you select Enable, the relay agent adds Option 82 header packets to the DHCP Request packets before forwarding them to the server, and strips them off while forwarding the responses to the client.
Requests Received	The total number of BOOTP/DHCP requests received from all clients since the last time the switch was reset.
Requests Relayed	The total number of BOOTP/DHCP requests forwarded to the server since the last time the switch was reset.
Packets Discarded	The total number of BOOTP/DHCP packets discarded by this Relay Agent since the last time the switch was reset.

Configuring the IP Helper Features

The IP Helper feature provides the ability for a router to forward configured UDP broadcast packets to a particular IP address. This allows applications to reach servers on non-local subnets. This is possible even when the application is designed to assume a server is always on a local subnet or when the application uses broadcast packets to reach the server (with the limited broadcast address 255.255.255.255, or a network directed broadcast address).

You can configure relay entries globally and on routing interfaces. Each relay entry maps an ingress interface and destination UDP port number to a single IPv4 address (the helper address). Multiple relay entries may be configured for the same interface and UDP port, in which case the relay agent relays matching packets to each server address. Interface configuration takes priority over global configuration. If the destination UDP port for a packet matches any entry on the ingress interface, the packet is handled according to the interface configuration. If the packet does not match any entry on the ingress interface, the packet is handled according to the global IP helper configuration.

IP Helper Global Configuration

Use the IP Helper Global Configuration page to globally enable the IP Helper admin mode and to configure global relay settings on the switch.

To display the page, click **LAN > L3 Features > IP Helper > Global Configuration** in the navigation tree.

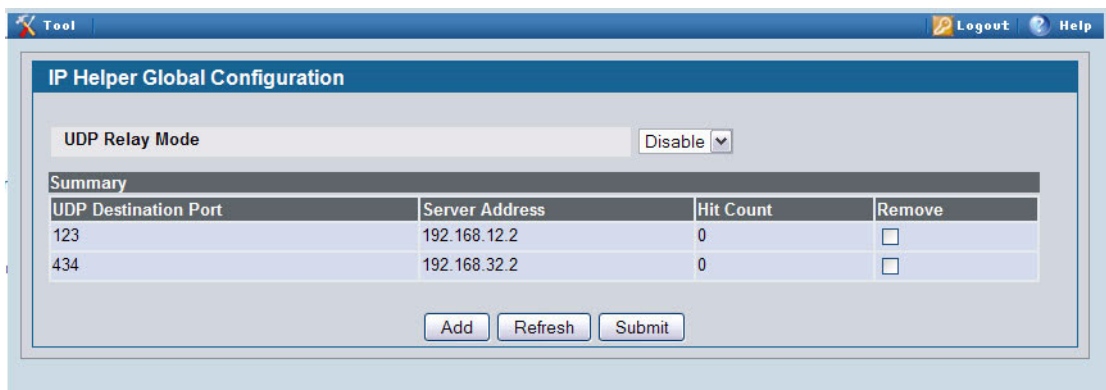


Figure 180: IP Helper Global Configuration

Table 161: IP Helper Global Configuration Fields

Field	Description
UDP Relay Mode	Select enable or disable from the pull down menu. User must enable Relay Mode to relay any other protocols for which an IP helper address has been configured. By Default UDP Relay Mode is disabled.
UDP Destination Port	Shows the destination UDP port ID/Port Name of UDP packets to be relayed.

Table 161: IP Helper Global Configuration Fields (Cont.)

Field	Description
Server Address	Shows the Server Address to which the packets with the given UDP Destination Port will be relayed.
Hit Count	Shows the number of times a packet has been forwarded or discarded according to this entry.
Remove	To delete a configured helper entry, select the Remove check box for the appropriate entry and click Submit .

To add a relay entry, click **Add**. The page refreshes and provides the configurable fields to add a UDP destination port and server IP address.

Figure 181: Adding a Global IP Helper Entry**Table 162: IP Helper Global Configuration Add Fields**

Field	Description
UDP Destination Port (0-65535)	The destination UDP port ID/Port Name of UDP packets to be relayed. Select the protocol from the menu. If you want to configure other than the listed protocols, select Other from the menu. Then user will be prompted with the UDP Destination Port field. Select the DefaultSet to configure for the relay entry for the default set of protocols.
Server Address	The Server Address to which the packets with the given UDP Destination Port will be relayed.

- Click **Submit** to send the updated configuration to the switch. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IP Helper Interface Configuration

Use the IP Helper Interface Configuration page to configure per-interface relay settings.

To display the page, click **LAN > L3 Features > IP Helper > Interface Configuration** in the navigation tree.

Figure 182: IP Helper Interface Configuration

Table 163: IP Helper Interface Configuration Fields

Field	Description
Source IP Interface	Select the interface from the pull down menu to get the relay entries configured on a particular interface. Select All to display all the configured relay entries on all interfaces.
UDP Destination Port	Shows the destination UDP port ID/Port Name of UDP packets to be relayed.
Server Address	Shows the Server Address to which the packets with the given UDP Destination Port will be relayed.
IsDiscard	If True, packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Hit Count	Shows the number of times a packet has been forwarded or discarded according to this entry.
Remove	To delete a configured helper entry, select the Remove check box for the appropriate entry and click Submit .

To add a relay entry, click **Add**. The page refreshes and provides the configurable fields to add a UDP destination port and server IP address.

Figure 183: Adding an IP Helper Entry to an Interface

Table 164: IP Helper Interface Configuration Add Fields

Field	Description
Source IP Interface	The the interface from the pulldown menu to for which user wants to configure the relay entry.
UDP Destination Port	The the Destination UDP port Name from the pull down menu or configure the port number to configure the Relay Entry on selected interface.
Discard	If set to True , packets arriving on the given interface with the given destination UDP port are discarded rather than relayed. Discard entries are used to override global IP helper address entries which otherwise might apply to a packet.
Server Address	The IPv4 address of the server to which packets are relayed for the specific UDP Destination Port.

- Click **Submit** to send the updated configuration to the switch. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Cancel** to cancel the configuration on the screen and reset the data on the screen to the latest value of the switch.

IP Helper Statistics

Use the IP Helper – Helper Statistics page to view IP Helper statistics. To display the page, click **LAN > L3 Features > IP Helper > Statistics** in the navigation tree.

IP Helper Statistics	
DHCP Client Messages Received	0
DHCP Client Messages Relayed	0
DHCP Server Messages Received	0
DHCP Server Messages Relayed	0
UDP Client Messages Received	0
UDP Client Messages Relayed	0
DHCP Client Messages with hops greater than Max	0
DHCP Pkts Received too early	0
Received DHCP Client message with giaddr as our own	0
UDP TTL Expired Pkts Received	0
UDP Pkts Discarded	0

Figure 184: IP Helper Statistics

Table 165: IP Helper – Helper Statistics Fields

Field	Description
DHCP Client Messages Received	The number of valid messages received from a DHCP client. The count is only incremented if IP helper is enabled globally, the ingress routing interface is up, and the packet passes a number of validity checks, such as having a TTL >1 and having valid source and destination IP addresses.
DHCP Client Messages Relayed	The number of DHCP client messages relayed to a server. If a message is relayed to multiple servers, the count is incremented once for each server.
DHCP Server Messages Received	The number of DHCP responses received from the DHCP server. This count only includes messages that the DHCP server unicasts to the relay agent for relay to the client.
DHCP Server Messages Relayed	Specifies the number of DHCP server messages relayed to a client.
UDP Client Messages Received	The number of valid UDP packets received. This count includes DHCP messages and all other protocols relayed. Conditions are similar to those for the first statistic in this table.
UDP Client Messages Relayed	The number of UDP packets relayed. This count includes DHCP messages relayed as well as all other protocols. The count is incremented for each server to which a packet is sent.
DHCP Client Messages with hops greater than Max	Specifies the number of DHCP Client Messages with hops greater than Max.
DHCP Pkts Received too early	Specifies the number of DHCP Pkts Received too early.
Received DHCP Client message with giaddr as our own	Specifies the number of DHCP Client messages received with giaddr as our own.

Table 165: IP Helper – Helper Statistics Fields (Cont.)

Field	Description
UDP TTL Expired Pkts Received	Specifies the number of UDP packets received with expired TTL.
UDP Pkts Discarded	Specifies the number of UDP packets discarded.

Configuring ARP

The ARP protocol associates a layer 2 MAC address with a layer 3 IPv4 address. D-Link DWS-4000 Series software features both dynamic and manual ARP configuration. With manual ARP configuration, you can statically add entries into the ARP table.

ARP is a necessary part of the internet protocol (IP) and is used to translate an IP address to a media (MAC) address, defined by a local area network (LAN) such as Ethernet. A station needing to send an IP packet must learn the MAC address of the IP destination, or of the next hop router, if the destination is not on the same subnet. This is achieved by broadcasting an ARP request packet, to which the intended recipient responds by unicasting an ARP reply containing its MAC address. Once learned, the MAC address is used in the destination address field of the layer 2 header prepended to the IP packet.

The ARP cache is a table maintained locally in each station on a network. ARP cache entries are learned by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), every recipient has the opportunity to store the sender's IP and MAC address in their respective ARP cache. The ARP response, being unicast, is normally seen only by the requestor, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The number of supported ARP entries is platform-dependent 2048 for the D-Link Unified Switch.

Devices can be moved in a network, which means the IP address that was at one time associated with a certain MAC address is now found using a different MAC, or may have disappeared from the network altogether (i.e., it has been reconfigured, disconnected, or powered off). This leads to stale information in the ARP cache unless entries are updated in reaction to new information seen on the network, periodically refreshed to determine if an address still exists, or removed from the cache if the entry has not been identified as a sender of an ARP packet during the course of an ageout interval, usually specified via configuration.

ARP Create

Use the ARP Create page to add an entry to the Address Resolution Protocol table.

To display the page, click **LAN > L3 Features > ARP > ARP Create** in the navigation tree.

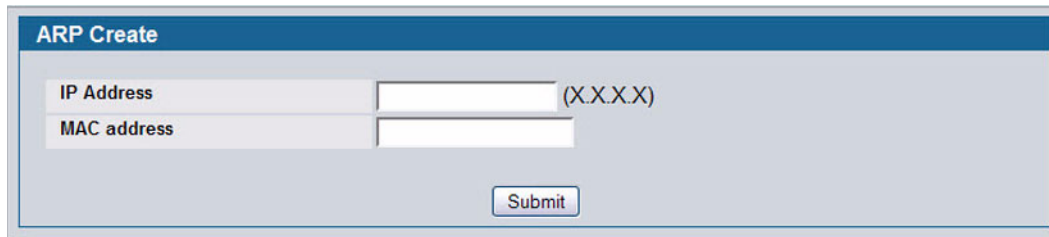


Figure 185: ARP Create

Table 166: ARP Create Fields

Field	Description
IP Address	Enter the IP address you want to add. It must be the IP address of a device on a subnet attached to one of the switch's existing routing interfaces.
MAC Address	The unicast MAC address of the device. Enter the address as six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

- After you enter an IP address and the associated MAC address, click **Submit** to apply the changes to the system and create the entry in the ARP table.

ARP Table Configuration

Use this page to change the configuration parameters for the Address Resolution Protocol Table. You can also use this screen to display the contents of the table.

To display the page, click **LAN > L3 Features > ARP > ARP Table Configuration** in the navigation tree.

The screenshot shows the 'ARP Table Configuration' web page. It features a form with the following fields and values:

- Age Time (secs): 1200 (range: 15 to 21600)
- Response Time (secs): 1 (range: 1 to 10)
- Retries: 4 (range: 0 to 10)
- Cache Size: 2048 (range: 256 to 2048)
- Dynamic Renew: Disable (dropdown menu)
- Total Entry Count: 0
- Peak Total Entries: 0
- Active Static Entries: 0
- Configured Static Entries: 0
- Maximum Static Entries: 64
- Remove from Table: None (dropdown menu)

A 'Submit' button is located below the form. Below the form is a table header with columns: IP Address, MAC address, Slot/Port, Type, and Age.

Figure 186: ARP Table Configuration

Table 167: ARP Table Configuration Fields

Field	Description
Age Time (secs)	Enter the value you want the switch to use for the ARP entry ageout time. You must enter a valid integer, which represents the number of seconds it takes for an ARP entry to age out. The range for this field is 15 to 21600 seconds. The default value for Age Time is 1200 seconds.
Response Time (secs)	Enter the value you want the switch to use for the ARP response timeout. You must enter a valid integer, which represents the number of seconds the switch waits for a response to an ARP request. The range for this field is 1 to 10 seconds. The default value for Response Time is 1 second.
Retries	Enter an integer which specifies the maximum number of times an ARP request is retried. The range for this field is 0 to 10. The default value for Retries is 4.
Cache Size	Enter an integer which specifies the maximum number of entries for the ARP cache. The range for this field is platform-dependent. The default value for Cache Size is 896.
Dynamic Renew	This controls whether the ARP component automatically attempts to renew ARP Entries of type Dynamic when they age out. The default setting is Disable.
Total Entry Count	Total number of entries in the ARP table.

Table 167: ARP Table Configuration Fields (Cont.)

Field	Description
Peak Total Entries	Highest value reached by Total Entry Count. This counter value is restarted whenever the ARP table Cache Size value is changed.
Active Static Entries	Total number of active static entries in the ARP table.
Configured Static Entries	Total number of configured static entries in the ARP table.
Maximum Static Entries	Maximum number of static entries that can be defined.
Remove from Table	Allows you to remove certain entries from the ARP Table. The choices listed specify the type of ARP Entry to be deleted: <ul style="list-style-type: none"> • All Dynamic Entries • All Dynamic and Gateway Entries • Specific Dynamic Gateway Entry • Specific Static Entry
Remove IP Address	This field appears only if you select Specific Dynamic/Gateway Entry or Specific Static Entry in the Remove from Table menu. This field allows you to enter the IP Address against the entry that is to be removed from the ARP Table.

The ARP Table displays at the bottom of the page, and contains the following fields:

Table 168: ARP Table Fields

Field	Description
IP Address	The IP address of a device on a subnet attached to one of the switch's routing interfaces.
MAC Address	The unicast MAC address for the device. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.
Slot/Port	The routing interface associated with the ARP entry.
Type	The type of the ARP entry.
Age	Age since the entry was last refreshed in the ARP Table. The format is hh:mm:ss

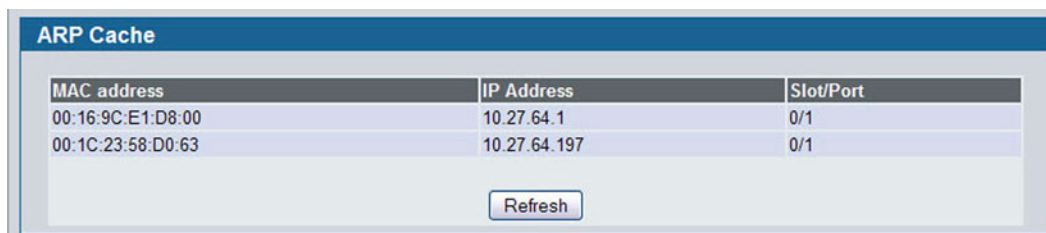
- If you make any changes to the page, click **Submit** to apply the changes to the system.

Viewing ARP Cache

The ARP cache is a table maintained locally in each station on a network. ARP cache entries are learned by examining the source information in the ARP packet payload fields, regardless of whether it is an ARP request or response. Thus, when an ARP request is broadcast to all stations on a LAN segment or virtual LAN (VLAN), every recipient has the opportunity to store the sender's IP and MAC address in their respective ARP cache. The ARP response, being unicast, is normally seen only by the requestor, who stores the sender information in its ARP cache. Newer information always replaces existing content in the ARP cache.

The ARP cache can support 1024 entries, although this size is user-configurable to any value less than 1024. When multiple network interfaces are supported by a device, as is typical of a router, either a single ARP cache is used for all interfaces, or a separate cache is maintained per interface. While the latter approach is useful when network addressing is not unique per interface, this is not the case for Ethernet MAC address assignment so a single ARP cache is employed.

To display the system ARP cache, click **LAN > Monitoring > ARP Cache** page in the navigation tree.



MAC address	IP Address	Slot/Port
00:16:9C:E1:D8:00	10.27.64.1	0/1
00:1C:23:58:D0:63	10.27.64.197	0/1

Figure 187: ARP Cache

Table 169: ARP Cache Fields

Field	Description
MAC Address	Displays the physical (MAC) address of the system in the ARP cache.
IP Address	Displays the IP address associated with the system's MAC address.
Slot/Port	Displays the slot, and port number being used for the connection.

- Click **Refresh** to reload the page and refresh the ARP cache view.
- Click **Clear** to clear all entries from the ARP cache.

Configuring Global and Interface IP Settings

When network devices are in different IP subnets, packets traveling between the subnets must be routed by a network device. By default, the D-Link DWS-4000 Series switch functions as a layer 2 switch. The pages under the IP folder allow you to enable routing and configure port or VLAN IP addresses so that the D-Link DWS-4000 Series switch also performs layer 3 routing and can route IP packets between devices in different subnets.

IP Configuration

Use the IP Configuration page to configure routing parameters for the switch as opposed to an interface.

To display the page, click **LAN > L3 Features > IP > Configuration** in the navigation tree.

IP Configuration	
Default Time to Live	64
Routing Mode	Disable
ICMP Echo Replies	Enable
ICMP Redirects	Enable
ICMP Rate Limit Interval	1000 (0 to 2147483647)
ICMP Rate Limit Burst Size	100 (1 to 200)
Maximum Next Hops	4
Maximum Routes	8000
Global Default Gateway	0.0.0.0 (X.X.X.X)
Configure <input type="checkbox"/>	
Submit	

Figure 188: IP Configuration

Table 170: IP Configuration Fields

Field	Description
Default Time to Live	The default value inserted into the Time-To-Live field of the IP header of datagrams originated by the switch, if a TTL value is not supplied by the transport layer protocol.
Routing Mode	Select Enable or Disable from the dropdown menu. You must enable routing for the switch before you can route through any of the interfaces. Routing is also enabled or disabled per VLAN interface. The default value is Disable .
ICMP Echo Replies	Select Enable or Disable from the dropdown menu. If you select Enable , then only the router can send ECHO replies. By default, ICMP Echo Replies are sent for echo requests.
ICMP Redirects	If this is enabled globally and on the interface level, then only the router can send ICMP redirects.

Table 170: IP Configuration Fields (Cont.)

Field	Description
ICMP Rate Limit Interval	To control the ICMP error packets, you can specify the number of ICMP error packets that are allowed per burst interval. By default, the rate limit is 100 packets per second, i.e. the burst interval is 1000 milliseconds. To disable ICMP rate limiting, set this field to zero. The valid rate interval range is 0 to 2147483647 milliseconds.
ICMP Rate Limit Burst Size	To control the ICMP error packets, you can specify the number of ICMP error packets that are allowed per burst interval. By default, the burst size is 100 packets. When the burst interval is zero, then configuring this field is not a valid option. The valid burst size range is 1 to 200.
Maximum Next Hops	The maximum number of hops supported by the switch. This is a read-only value.
Maximum Routes	The maximum number of routes (routing table size) supported by the switch.
Global Default Gateway	(Optional) To edit this field, select the Configure check box and set the global default gateway to the manually configured value. A default gateway configured in this field is more preferred than a default gateway learned from a DHCP server. Only one default gateway can be configured.

- If you make any changes to the page, click **Submit** to apply the changes to the system.

IP Interface Configuration

Use the IP Interface Configuration page to update IP interface data for this switch.

To display the page, click **LAN > L3 Features > IP > Interface Configuration** in the navigation tree.

Figure 189: IP Interface Configuration

Table 171: IP Interface Configuration Fields

Field	Description
Interface	Select the interface to configure from the dropdown menu. The dropdown menu contains logical interfaces, including loopback interfaces and VLAN routing interfaces.
Routing Interface Status	Shows whether the IPv4 routing is up or down on the interface.
IP Address Configuration Method	Specify whether the selected interface should receive an IP address dynamically through DHCP, or statically through manual IP address assignment. If you configure DHCP as the method, additional buttons display at the bottom of the page that allow you to renew, release, or display DHCP-assigned information.
IP Address	If the configuration method is manual, enter the static IP address for the interface.
Subnet Mask	If the configuration method is manual, enter the subnet mask for the interface. This is also referred to as the subnet/network mask, and defines the portion of the interface's IP address that is used to identify the attached network.

Table 171: IP Interface Configuration Fields (Cont.)

Field	Description
Routing Mode	Setting this Enables or Disables routing for an interface. By default, routing is disabled on port-based routing interfaces and enabled on VLAN-based routing interfaces.
Administrative Mode	The Administrative Mode of the interface. The default value is Enable.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This data is valid only for physical interfaces and is measured in Megabits per second (Mbps).
Forward Net Directed Broadcasts	Select how network directed broadcast packets should be handled. If you select Enable from the dropdown menu network directed broadcasts are forwarded. If you select Disable they are dropped. The default value is Disable.
Active State	The state of the specified interface is either Active or Inactive. An interface is considered active if the link is up and it is in forwarding state.
MAC Address	The burned-in physical address of the specified interface. The format is six two-digit hexadecimal numbers separated by colons, for example 00:06:29:32:81:40. This value is valid for physical interfaces. For logical interfaces, such as VLAN routing interfaces, the field displays the system MAC address.
Encapsulation Type	Select the link layer encapsulation type for packets transmitted from the specified interface from the dropdown menu. The possible values are Ethernet and SNAP. The default is Ethernet.
Proxy ARP	Select to Disable or Enable Proxy ARP for the specified interface from the dropdown menu.
Local Proxy ARP	Select to Disable or Enable Local Proxy ARP for the specified interface from the dropdown menu.
IP MTU	The maximum transmission unit (MTU) size of IP packets sent on an interface. Valid range is (68 to 9198). Default value is 1500.
Bandwidth	The configured bandwidth of the interface is specified in Kbps. The OSPF protocol uses this value to compute the link cost of an interface as the ratio of the reference bandwidth to the interface bandwidth. If no bandwidth is configured, the bandwidth defaults to the actual interface bandwidth for port-based routing interfaces and to 10 Mbps for VLAN routing interfaces. This value does not affect the actual speed of an interface.
Destination Unreachables	Specifies the mode of sending ICMP Destination Unreachables on this interface. If this is disabled, then this interface will not send ICMP Destination Unreachables. By default, the Destination Unreachables mode is Enable .
ICMP Redirects	The router sends an ICMP Redirect on an interface only if Redirects are enabled both globally and on the interface. By default, the ICMP Redirects mode is Enable .

- Click **Submit** to send the updated configuration to the switch. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Helper-IP Address** to proceed to the **Helper Address** configuration page.

IP Statistics

The statistics reported on the IP Statistics page are as specified in RFC 1213.

To display the page, click **LAN > Monitoring > L3 Status > IP Statistics** in the navigation tree.



Note: Figure 190 does not show all of the fields on the page.

IP Statistics	
IpInReceives	247129
IpInHdrErrors	0
IpInAddrErrors	825
IpForwDatagrams	0
IpInUnknownProtos	0
IpInDiscards	0
IpInDelivers	238064
IpOutRequests	158510
IpOutDiscards	0
IpOutNoRoutes	0

Figure 190: IP Statistics

Table 172: IP Statistics Fields

Field	Description
IpInReceives	The total number of input datagrams received from interfaces, including those received in error.
IpInHdrErrors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
IpInAddrErrors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
IpForwDatagrams	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter includes only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.
IpInUnknownProtos	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
IpInDiscards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

Table 172: IP Statistics Fields (Cont.)

Field	Description
IpInDelivers	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
IpOutRequests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.
IpOutDiscards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
IpOutNoRoutes	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this 'no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
IpReasmTimeout	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
IpReasmReqds	The number of IP fragments received which needed to be reassembled at this entity.
IpReasmOKs	The number of IP datagrams successfully re-assembled.
IpReasmFails	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms can lose track of the number of fragments by combining them as they are received.
IpFragOKs	The number of IP datagrams that have been successfully fragmented at this entity.
IpFragFails	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.
IpFragCreates	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
IpRoutingDiscards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
IcmpInMsgs	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.
IcmpInErrors	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
IcmpInDestUnreachs	The number of ICMP Destination Unreachable messages received.
IcmpInTimeExcds	The number of ICMP Time Exceeded messages received.
IcmpInParmProbs	The number of ICMP Parameter Problem messages received.
IcmpInSrcQuenchs	The number of ICMP Source Quench messages received.
IcmpInRedirects	The number of ICMP Redirect messages received.
IcmpInEchos	The number of ICMP Echo (request) messages received.

Table 172: IP Statistics Fields (Cont.)

Field	Description
IcmpInEchoReps	The number of ICMP Echo Reply messages received.
IcmpInTimestamps	The number of ICMP Timestamp (request) messages received.
IcmpInTimestampReps	The number of ICMP Timestamp Reply messages received.
IcmpInAddrMasks	The number of ICMP Address Mask Request messages received.
IcmpInAddrMaskReps	The number of ICMP Address Mask Reply messages received.
IcmpOutMsgs	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.
IcmpOutErrors	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
IcmpOutDestUnreachs	The number of ICMP Destination Unreachable messages sent.
IcmpOutTimeExcds	The number of ICMP Time Exceeded messages sent.
IcmpOutParmProbs	The number of ICMP Parameter Problem messages sent.
IcmpOutSrcQuenchs	The number of ICMP Source Quench messages sent.
IcmpOutRedirects	The number of ICMP Redirect messages sent. For a host, this object is always zero, since hosts do not send redirects.
IcmpOutEchos	The number of ICMP Echo (request) messages sent.
IcmpOutEchoReps	The number of ICMP Echo Reply messages sent.
IcmpOutTimestamps	The number of ICMP Timestamp (request) messages.
IcmpOutTimestampReps	The number of ICMP Timestamp Reply messages sent.
IcmpOutAddrMasks	The number of ICMP Address Mask Request messages sent.

- Click **Refresh** to update the page with the most current data.

Loopback Interfaces

D-Link DWS-4000 Series software provides for the creation, deletion, and management of loopback interfaces. They are dynamic interfaces that are created and deleted via user-configuration. D-Link DWS-4000 Series software supports multiple loopback interfaces.

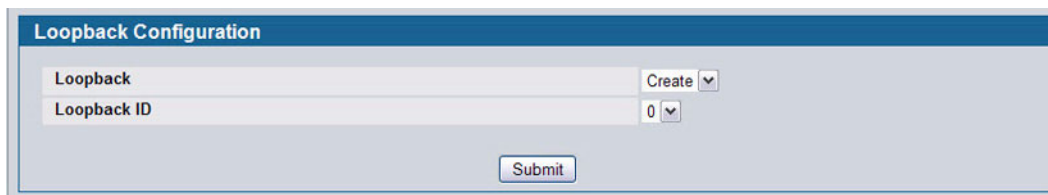
A loopback interface is always expected to be up. As such, it provides a means to configure a stable IP address on the device that may be referred to by other switches. This interface provides the source address for sent packets and can receive both local and remote packets. It is typically used by routing protocols.

A loopback interface is a pseudo-device for assigning local addresses so that the router can be communicated with by this address, which is always up and can receive traffic from any of the existing active interfaces. Thus, given reachability from a remote client, the address of the loopback can be used to communicate with the router through various services such as telnet and SSH. In this way, the address on a loopback behaves identically to any of the local addresses of the router in terms of the processing of incoming packets.

Loopbacks Configuration

Use the Loopbacks Configuration page to create, configure, or remove loopback interfaces. You can also set up or delete a secondary address for a loopback.

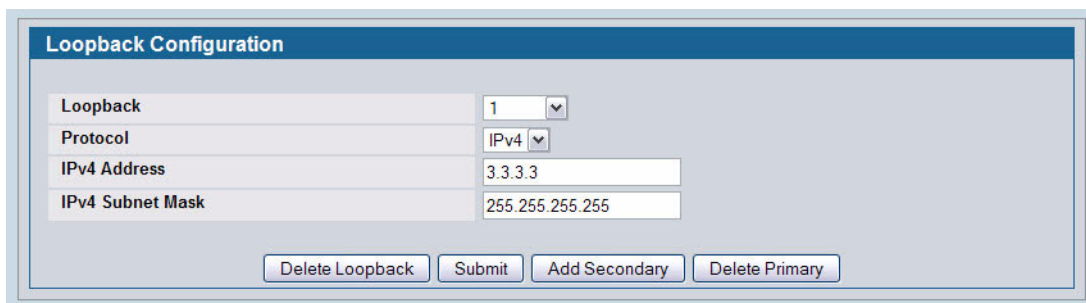
To display the page, click **LAN > L3 Features > Loopbacks > Configuration** in the navigation tree. If no loopback interfaces exist on the system, the page only has two fields, as [Figure 191](#) shows.



The screenshot shows the 'Loopback Configuration' page with a 'Create' form. The form has two fields: 'Loopback' with a dropdown menu set to '1' and 'Loopback ID' with a dropdown menu set to '0'. There is a 'Submit' button at the bottom.

Figure 191: Loopback Configuration—Create

Additional fields display depending on whether or not a loopback has already been created, as shown in [Figure 192](#).



The screenshot shows the 'Loopback Configuration' page with a 'Configured Loopback Interface' form. The form has four fields: 'Loopback' with a dropdown menu set to '1', 'Protocol' with a dropdown menu set to 'IPv4', 'IPv4 Address' with a text input field containing '3.3.3.3', and 'IPv4 Subnet Mask' with a text input field containing '255.255.255.255'. There are four buttons at the bottom: 'Delete Loopback', 'Submit', 'Add Secondary', and 'Delete Primary'.

Figure 192: Configured Loopback Interface

The fields available on the Loopbacks Configuration page depend on whether any loopback interfaces exist and whether the protocol is IPv4 or IPv6. The following table describes all fields, which are not all on the same screen at the same time.

Table 173: Configured Loopback Interface Fields

Field	Description
Loopback	Use the dropdown menu to select from the list of currently configured loopback interfaces. Create is also a valid choice if the maximum number of loopback interfaces has not been created.
Loopback ID	When Create is selected in the Loopback field, this list of available loopback IDs displays.
Protocol	Select IPv4 or IPv6 to configure the corresponding attributes on the loopback interface. The protocol selected affects the fields that are displayed on this page.
IPv4 Address	The primary IPv4 address for this interface in dotted decimal notation. This option only displays when the Protocol specified is IPv4.
IPv4 Subnet Mask	The primary IPv4 subnet mask for this interface in dotted decimal notation. This option only displays when the Protocol specified is IPv4.

The following fields display after a primary address has been configured and you click **Add Secondary**. You can configure multiple secondary addresses.

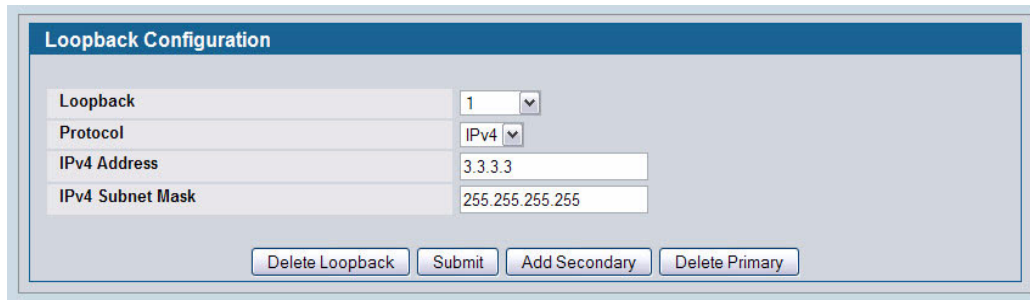
Table 174: Loopback Interface Secondary Address Fields

Field	Description
Secondary Address	Select a configured IPv4 secondary address for the selected Loopback interface from the dropdown menu. A new address can be entered in the Secondary IP Address field by selecting Add Secondary IP Address here (if the maximum number of secondary addresses has not been configured). A primary address must be configured before a secondary address can be added.
Secondary IP Address	The secondary IP address for this interface in dotted decimal notation. This input field is visible only when Add Secondary is selected.
Secondary Subnet Mask	The secondary subnet mask for this interface in dotted decimal notation. This input field is visible only when Add Secondary is selected.

Creating a New Loopback (IPv4)

1. From the **Loopbacks Configuration** page, select **Create** from the **Loopback** menu.
2. Specify an ID to use in the **Loopback ID** field.
3. Click **Submit**.

The Loopback ID field goes away, and additional loopback fields display, as [Figure 193](#) shows.



The screenshot shows a web form titled "Loopback Configuration". It contains the following fields and values:

Field	Value
Loopback	1
Protocol	IPv4
IPv4 Address	3.3.3.3
IPv4 Subnet Mask	255.255.255.255

At the bottom of the form, there are four buttons: "Delete Loopback", "Submit", "Add Secondary", and "Delete Primary".

Figure 193: Loopbacks Configuration—IPv4 Entry

4. In the **Protocol** field, select **IPv4**
5. Enter desired values in the remaining fields.
6. Click **Submit**.

The new loopback is saved, and the web page reappears showing secondary address configuration fields. For an example of the fields on this page, see [Figure 192](#).
7. Optionally, click the **Add Secondary** field to add a secondary IP address and complete the **Secondary Address**, **Secondary IP Address**, and **Secondary Subnet Mask** fields.
8. Click **Submit**.

Removing a Loopback

1. Open the **Loopback Configuration** page.
2. Specify the loopback to remove in the **Loopback** menu.
3. Click **Delete Loopback**.

The loopback is deleted, and the device is updated.

Removing a Secondary Address

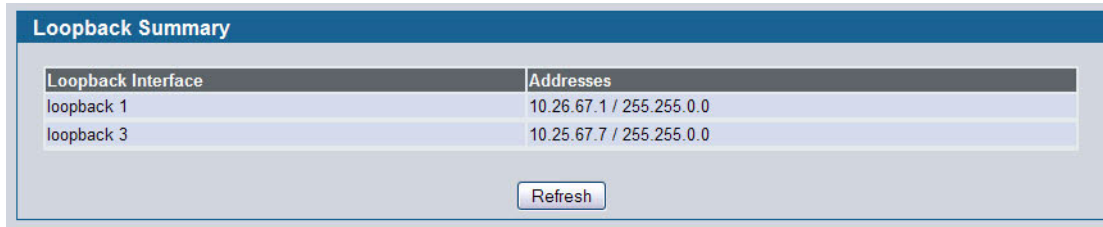
1. Open the **Loopback Configuration** page.
2. Specify the loopback to be affected.
3. Specify the secondary address to be removed.
4. Click **Delete Selected Secondary**.

The secondary address is deleted, and the device is updated.

Loopbacks Summary

Use the Loopbacks Summary page to display a summary of configured loopbacks.

To display the page, click **LAN > Monitoring > L3 Status > Loopback Summary** in the navigation tree.



Loopback Interface	Addresses
loopback 1	10.26.67.1 / 255.255.0.0
loopback 3	10.25.67.7 / 255.255.0.0

Refresh

Figure 194: Loopbacks Summary

Table 175: Loopbacks Summary Fields

Field	Description
Loopback Interface	The ID of the configured loopback interface.
Addresses	A list of the addresses configured on the loopback interface.

- Click **Refresh** to update the information on the screen.

Configuring RIP

RIP is an Interior Gateway Protocol (IGP) based on the Bellman-Ford algorithm and targeted at smaller networks (network diameter no greater than 15 hops). The routing information is propagated in RIP update packets that are sent out both periodically and in the event of a network topology change. On receipt of a RIP update, depending on whether the specified route exists or does not exist in the route table, the router may modify, delete, or add the route to its route table.

RIP Configuration

Use the RIP Configuration page to enable and configure or disable RIP in Global mode.

To display the page, click **LAN > L3 Features > RIP > Configuration** in the navigation tree.

The screenshot shows the 'RIP Configuration' web page. It features a table of configuration options with dropdown menus and text input fields. The options are: RIP Admin Mode (set to Enable), Split Horizon Mode (set to Simple), Auto Summary Mode (set to Disable), Host Routes Accept Mode (set to Enable), Global Route Changes (set to 0), Global Queries (set to 0), Default Information Originate (set to Disable), and Default Metric (set to 1 to 15). A 'Submit' button is positioned at the bottom center of the form.

Figure 195: RIP Configuration

Table 176: RIP Configuration Fields

Field	Description
RIP Admin Mode	Select Enable or Disable from the dropdown menu. If you select Enable, RIP is enabled for the switch. The default is Disable.
Split Horizon Mode	Select None, Simple, or Poison Reverse from the dropdown menu. The default is Simple. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: <ul style="list-style-type: none"> • None: No special processing for this case. • Simple: A route is not included in updates sent to the router from which it was learned. • Poison Reverse: A route is included in updates sent to the router from which it was learned, but the metric is set to infinity.

Table 176: RIP Configuration Fields (Cont.)

Field	Description
Auto Summary Mode	Select Enable or Disable from the dropdown menu. If you select Enable, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries. The default is Disable.
Host Routes Accept Mode	Select Enable or Disable from the dropdown menu. If you select Enable, the router accepts host routes. The default is Enable.
Global Route Changes	Displays the number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.
Global Queries	Displays the number of responses sent to RIP queries from other systems.
Default Information Originate	When enabled, RIP originates a default route (0.0.0.0/0.0.0.0)
Default Metric	Sets a default for the metric of redistributed routes. This field displays the default metric if one has already been set, or blank if not configured earlier. Valid values are 1 to 15.

- If you make changes to the page, click **Submit** to apply the changes to the system.

RIP Interface Configuration

Use the RIP Interface Configuration page to enable and configure or to disable RIP on a specific interface.

To display the page, click **LAN > L3 Features > RIP > Interface Configuration** in the navigation tree.

The screenshot shows the 'RIP Interface Configuration' web page. The configuration fields are as follows:

Field	Value
Slot/Port	0/1
Send Version	RIP-2
Receive Version	RIP-2
RIP Admin Mode	Disable
Authentication Type	None
IP Address	0.0.0.0
Link State	
Bad Packets Received	0
Bad Routes Received	0
Updates Sent	0

Buttons: 'Configure Authentication' and 'Submit'.

Figure 196: RIP Interface Configuration

Table 177: RIP Interface Configuration Fields

Field	Description
Slot/Port	Select the interface for which data is to be configured from the menu.
Send Version	RIP Version that router sends with its routing updates. The default is RIP-2. Possible values are: <ul style="list-style-type: none"> • RIP-1: send RIP version 1 formatted packets via broadcast. • RIP-1c: RIP version 1 compatibility mode. Send RIP version 2 formatted packets via broadcast. • RIP-2: send RIP version 2 packets using multicast. • None: no RIP control packets are sent.
Receive Version	RIP Version of the routing updates that the router must accept. The default is Both. Possible values are: <ul style="list-style-type: none"> • RIP-1: accept only RIP version 1 formatted packets. • RIP-2: accept only RIP version 2 formatted packets. • Both: accept packets in either format. • None: no RIP control packets is accepted.
RIP Admin Mode	Select Enable or Disable from the dropdown menu. Before you enable RIP version 1 or version 1c on an interface, you must first enable network directed broadcast mode on the corresponding interface. The default value is Disable.
Authentication Type	You may select an authentication type other than None by clicking the Modify button. You then see a new screen, where you can select the authentication type from the dropdown menu. Possible values are: <ul style="list-style-type: none"> • None: This is the initial interface state. If you select this option from the dropdown menu on the second screen you are returned to the first screen without any authentication protocols being run. • Simple: If you select Simple you are prompted to enter an authentication key. This key is included, in the clear text, in the RIP header of all packets sent on the network. All routers on the network must be configured with the same key. • Encrypt: If you select Encrypt you are prompted to enter both an authentication key and an authentication ID. Encryption uses the MD5 Message-Digest algorithm. All routers on the network must be configured with the same key and ID.
IP Address	Displays the IP Address of the router interface.
Link State	Specifies whether the RIP interface is up or down.
Bad Packets Received	Displays the number of RIP packets that were found to be invalid or corrupt.
Bad Routes Received	Displays the number of routes, in valid RIP packets, which were ignored for any reason, e.g., the number of triggered RIP updates actually sent on this interface. This explicitly does NOT include full updates sent containing new information.
Updates Sent	Displays the number of route updates sent.

Configuring the RIP Interface

1. Open the **RIP Interface Configuration** page.
2. Specify the interface for which data is to be configured.
3. Enter data into the fields as needed.
4. To change the **Authentication Type**, click **Configure Authentication** to configure different Authentication Types.

The page refreshes and displays the RIP Interface Authentication Configuration page.

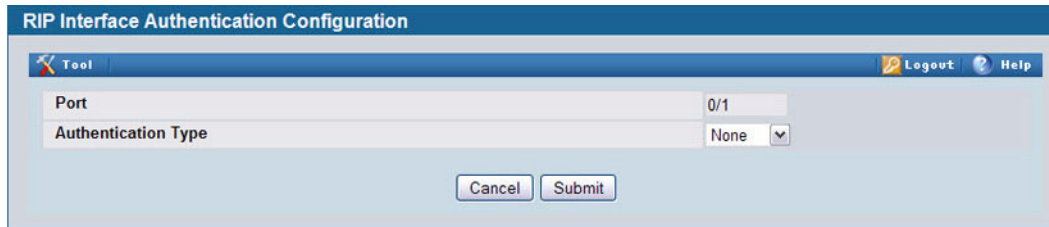


Figure 197: RIP Interface Authentication Configuration

5. Select the type of authentication to use.
If you select Simple or Encrypt as the authentication, the screen refreshes, and additional fields display. Enter the required information into the new fields.
6. Click **Submit** to apply the changes to the system and return to the **RIP Interface Configuration** page.
7. To cancel the authentication configuration and return to the **RIP Interface Configuration** page, click **Cancel**.

RIP Interface Summary

Use the RIP Interface Summary page to display RIP configuration status on an interface.

To display the page, click **LAN > Monitoring > L3 Status > RIP > Interface Summary** in the navigation tree.

Slot/Port	IP Address	Send Version	Receive Version	RIP Admin Mode	Link State
0/1	0.0.0.0	RIP-2	RIP-2	Disable	Link Down

Figure 198: RIP Interface Summary

Table 178: RIP Interface Summary Fields

Field	Description
Slot/Port	The interface, such as the routing-enabled VLAN on which RIP is enabled.
IP Address	The IP Address of the router interface.
Send Version	Specifies the RIP version to which RIP control packets sent from the interface conform. The default is RIP-2. Possible values are: <ul style="list-style-type: none"> • RIP-1: RIP version 1 packets are sent using broadcast. • RIP-1c: RIP version 1 compatibility mode. RIP version 2 formatted packets are transmitted using broadcast. • RIP-2: RIP version 2 packets are sent using multicast. • None: RIP control packets are not transmitted.
Receive Version	Specifies which RIP version control packets are accepted by the interface. The default is Both. Possible values are: <ul style="list-style-type: none"> • RIP-1: only RIP version 1 formatted packets are received. • RIP-2: only RIP version 2 formatted packets are received. • Both: packets are received in either format. • None: no RIP control packets are received.
RIP Admin Mode	Specifies whether RIP is Enabled or Disabled on the interface.
Link State	Specifies whether the RIP interface is up or down.

- Click **Refresh** to update the information on the screen.

RIP Route Redistribution Configuration

Use the RIP Route Redistribution Configuration page to configure which routes are redistributed to other routers using RIP. The allowable values for each fields are displayed next to the field. If any invalid values are entered, an alert message is displayed with the list of all the valid values.

To display the page, click **LAN > L3 Features > RIP > Route Redistribution Configuration** in the navigation menu.

Figure 199: RIP Route Redistribution Configuration

Table 179: RIP Route Redistribution Configuration Fields

Field	Description
Configured Source	If any Source Routes have already been configured for redistribution by RIP, they appear in the dropdown menu. Otherwise, the only available option is Create, which allows you to configure an available source route. Select an existing route to view or modify its parameters.
Available Source	The dropdown menu is populated by only those Source Routes that have not previously been configured for redistribution by RIP. This field is available only if you select Create as the Configured Source. Possible values are: <ul style="list-style-type: none"> • Static: The route was manually configured. • Connected: The route was determined automatically because the host is directly connected. • RIP: The route was determined through RIP.
Metric	Sets the metric value to be used as the metric of redistributed routes. This field displays the metric if the source was pre-configured and can be modified. The valid values are 1 to 15.
Distribute List	Enter the ACL ID for an access list that filters the routes to be redistributed by the destination protocol. Only permitted routes are redistributed.

You configure ACLs through the pages under **LAN > Access Control Lists > IP Access Control Lists**. When used for route filtering, the only fields in an access list that get used are:

- Source IP Address and netmask
- Destination IP Address and netmask
- Action (Permit or Deny)

All other fields (source and destination port, precedence, ToS, etc.) are ignored.

The source IP address is compared to the destination IP address of the route. The source IP netmask in the access list rule is treated as a wildcard mask, indicating which bits in the source IP address must match the destination address of the route. (Note that a 1 in the mask indicates a Don't Care in the corresponding address bit.)

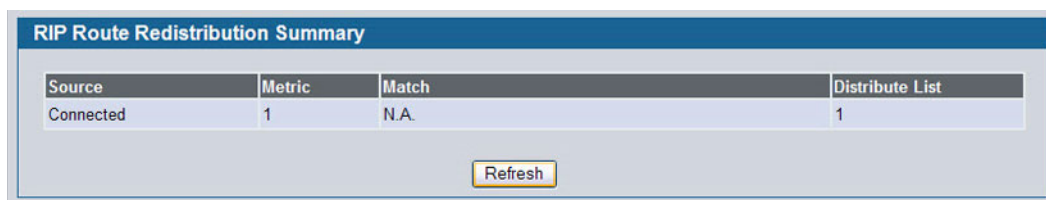
When an access list rule includes a destination IP address and netmask (an extended access list), the destination IP address is compared to the network mask of the destination of the route. The destination netmask in the access list serves as a wildcard mask, indicating which bits in the route's destination mask are significant for the filtering operation.

- If you make changes to the page, click **Submit** to apply the changes to the system.
- To delete a configured route, click **Delete**.

RIP Route Redistribution Summary

Use the RIP Route Redistribution Summary page to display Route Redistribution configurations.

To display the page, click **LAN > Monitoring > L3 Status > RIP > Route Redistribution Summary** in the navigation menu.



Source	Metric	Match	Distribute List
Connected	1	N.A.	1

Figure 200: RIP Route Redistribution Summary

Table 180: RIP Route Redistribution Summary Fields

Field	Description
Source	The protocol used to obtain the route.
Metric	The Metric of redistributed routes for the given source route. Displays Unconfigured when not configured.
Distribute List	The Access List that filters the routes to be redistributed by the Destination Protocol. If the Distribute List is not configured, the field is blank.

- Click **Refresh** to update the information on the screen.

Router Discovery

The Router Discovery protocol is used by hosts to identify operational routers on the subnet. Router Discovery messages are of two types: “Router Advertisements” and “Router Solicitations.” The protocol mandates that every router periodically advertise the IP Addresses it is associated with. Hosts listen for these advertisements and discover the IP Addresses of neighboring routers.

Router Discovery Configuration

Use the Router Discovery Configuration page to enter or change Router Discovery parameters.

To display the page, click **LAN > L3 Features > Router Discovery > Configuration** in the navigation tree.

Figure 201: Router Discovery Configuration

Table 181: Router Discovery Configuration Fields

Field	Description
Slot/Port	Select the router interface for which data is to be configured.
Advertise Mode	Select Enable or Disable from the dropdown menu. If you select Enable, Router Advertisements are transmitted from the selected interface.
Advertise Address	Enter the IP Address to be used to advertise the router.
Maximum Advertise Interval (secs)	Enter the maximum time (in seconds) allowed between router advertisements sent from the interface.
Minimum Advertise Interval (secs)	Enter the minimum time (in seconds) allowed between router advertisements sent from the interface.
Advertise Lifetime (secs)	Enter the value (in seconds) to be used as the lifetime field in router advertisements sent from the interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.
Preference Level	Specify the preference level of the router as a default router relative to other routers on the same subnet. Higher numbered addresses are preferred. You must enter an integer.

- If you make any changes to the page, click **Submit** to apply the changes to the system.

Router Discovery Status

Use the Router Discovery Status page to display Router Discovery data for each port.

To display the page, click **LAN > L3 Features > Router Discovery > Status** in the navigation tree.

Router Discovery Status						
Slot/Port	Advertise Mode	Advertise Address	Maximum Advertise Interval (secs)	Minimum Advertise Interval (secs)	Advertise Lifetime (secs)	Preference Level
0/1	Disable	224.0.0.1	600	450	1800	0
0/2	Disable	224.0.0.1	600	450	1800	0
0/3	Disable	224.0.0.1	600	450	1800	0
0/4	Disable	224.0.0.1	600	450	1800	0
0/5	Disable	224.0.0.1	600	450	1800	0
0/6	Disable	224.0.0.1	600	450	1800	0
0/7	Disable	224.0.0.1	600	450	1800	0
0/8	Disable	224.0.0.1	600	450	1800	0
0/9	Disable	224.0.0.1	600	450	1800	0
0/10	Disable	224.0.0.1	600	450	1800	0
0/11	Disable	224.0.0.1	600	450	1800	0
0/12	Disable	224.0.0.1	600	450	1800	0
0/13	Disable	224.0.0.1	600	450	1800	0
0/14	Disable	224.0.0.1	600	450	1800	0
0/15	Disable	224.0.0.1	600	450	1800	0
0/16	Disable	224.0.0.1	600	450	1800	0
0/17	Disable	224.0.0.1	600	450	1800	0
0/18	Disable	224.0.0.1	600	450	1800	0
0/19	Disable	224.0.0.1	600	450	1800	0
0/20	Disable	224.0.0.1	600	450	1800	0
0/21	Disable	224.0.0.1	600	450	1800	0
0/22	Disable	224.0.0.1	600	450	1800	0
0/23	Disable	224.0.0.1	600	450	1800	0
0/24	Disable	224.0.0.1	600	450	1800	0

Figure 202: Router Discovery Status

Table 182: Router Discovery Status Fields

Field	Description
Slot/Port	The router interface for which data is displayed.
Advertise Mode	The values are Enable or Disable. Enable denotes that Router Discovery is enabled on that interface.
Advertise Address	The IP Address used to advertise the router.
Maximum Advertise Interval(secs)	The maximum time (in seconds) allowed between router advertisements sent from the interface.

Table 182: Router Discovery Status Fields (Cont.)

Field	Description
Minimum Advertise Interval(secs)	The minimum time (in seconds) allowed between router advertisements sent from the interface.
Advertise Lifetime(secs)	The value (in seconds) used as the lifetime field in router advertisements sent from the interface. This is the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts.
Preference Level	The preference level of the router as a default router relative to other routers on the same subnet. Higher numbered addresses are preferred.

- Click **Refresh** to update the information on the screen.

Router

The pages accessible from the **Router** folder allow you to configure the routing table and configure route preferences.

Route Table

The route table manager collects routes from multiple sources: static routes, RIP routes, and local routes. The route table manager may learn multiple routes to the same destination from multiple sources. The route table lists all routes. The best routes table displays only the most preferred route to each destination (see [“Best Routes Table”](#) on page 311 for more information).

To display the page, click **LAN > Monitoring > L3 Status > Route Table** in the navigation tree.

**Figure 203: Route Table****Table 183: Route Table Fields**

Field	Description
Total Number of Routes	The total number of routes in the route table.
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.

Table 183: Route Table Fields (Cont.)

Field	Description
Protocol	This field tells which protocol created the specified route. The possibilities are one of the following: <ul style="list-style-type: none">• Local• Static• Default• RIP
Next Hop Slot/Port	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

- Click **Refresh** to update the information on the screen.

Best Routes Table

The route table manager collects routes from multiple sources: static routes, RIP routes, and local routes. The route table manager may learn multiple routes to the same destination from multiple sources. In that case, the route table manager selects the route with the lowest route preference value to use for forwarding to that destination. Use the Best Routes Table page to display the best routes from the routing table. To view all routes, including multiple routes to the same destination, see [“Route Table” on page 309](#).

To display the page, click **LAN > L3 Features > Router > Best Routes Table** in the navigation tree.

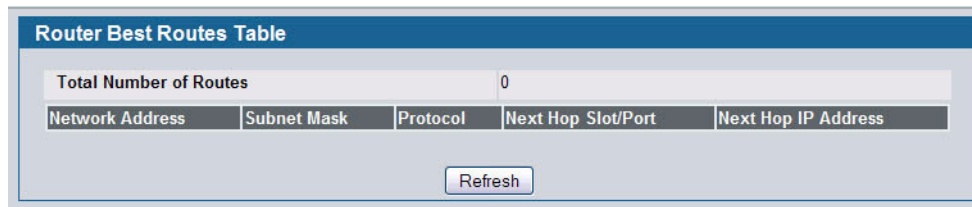


Figure 204: Best Routes Table

Table 184: Best Routes Table Fields

Field	Description
Total Number of Routes	The total number of routes in the route table.
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Protocol	This field tells which protocol created the specified route. The possibilities are one of the following: <ul style="list-style-type: none"> • Local • Static • Default • RIP
Next Hop Slot/Port	The outgoing router interface to use when forwarding traffic to the destination.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network.

- Click **Refresh** to update the information on the screen.

Configured (Static) Routes

Use the Configured Routes page to create and display static routes.

To display the page, click **LAN > L3 Features > Router > Configured Routes** in the navigation tree.



Figure 205: Configured Routes

Table 185: Configured Routes Fields

Field	Description
Network Address	The IP route prefix for the destination.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Next Hop IP	The next hop router address to use when forwarding traffic to the destination.
Next Hop Slot/Port	The outgoing interface to use when forwarding traffic to the destination. For static reject routes it would be Null0. Note: The route will not take effect until a routing interface belonging to the same subnet as the next hop IP is created and activated, and this field will display the next hop slot/port as Unresolved.
Preference	The preferences configured for the added routes.

Adding a Static Route

1. Open the Configured Routes page.
2. Click **Add Route**.

The **Router Route Entry Create** page displays. The fields available on the page vary based on the route type.

3. Next to **Route Type**, select **Default** route, **Static** or **Static Reject** from the menu.
 - **Default:** Enter the default gateway address in the **Next Hop IP Address** field and the the route preference value in the **Preference** field.
 - **Static:** Enter values for **Network Address**, **Subnet Mask**, **Next Hop IP Address**, and **Preference**.
 - **Static Reject:** Packets to these destinations will be dropped.

Figure 206: Create Static Route

Table 186: Route Entry Create Fields

Field	Description
Route Type	Specifies whether the route is to be a Default, Static, or Static Reject route. Packets sent to the static reject route are dropped.
Network Address	Specify the IP route prefix for the destination from the dropdown menu. In order to create a route, a valid routing interface must exist and the next hop IP Address must be on the same network as the routing interface. Routing interfaces are created on the IP Interface Configuration page. Valid next hop IP Addresses can be viewed on the Route Table page.
Subnet Mask	Also referred to as the subnet/network mask, this indicates the portion of the IP interface address that identifies the attached network.
Next Hop IP Address	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path towards the destination. The next router is always one of the adjacent neighbors or the IP address of the local interface for a directly attached network. When creating a route, the next hop IP must be on the same network as the routing interface. Valid next hop IP Addresses can be seen on the Route Table page.
Preference	Specifies a preference value for the configured next hop.

4. Click **Submit.**

The new route is added, and you are returned to the Configured Routes page.

Deleting a Route

Select the check box at the end of the row for the route to delete. Click **Delete** to remove the selected route.

Route Preferences Configuration

Use the Route Preferences Configuration page to configure the default preference for each protocol. These values are arbitrary values that range from 1 to 255, and are independent of route metrics. Most routing protocols use a route metric to determine the shortest path known to the protocol, independent of any other protocol. Routes with a preference of 255 are not used for forwarding.

The best route to a destination is chosen by selecting the route with the lowest preference value. When there are multiple routes to a destination, the preference values are used to determine the preferred route.

To display the page, click **LAN > L3 Features > Router > Route Preferences Configuration** in the navigation tree.

Router Route Preferences Configuration	
Local	0
Static	1 (1 to 255)
RIP	120 (1 to 255)

Figure 207: Route Preferences Configuration

Table 187: Route Preferences Configuration Fields

Field	Description
Local	This field displays the local route preference value of 0. This value is not configurable.
Static	The static route preference value in the router. The default value is 1. The range is 1 to 255.
RIP	The RIP route preference value in the router. The default value is 15. The range is 1 to 255.

- If you make changes to the page, click **Submit** to apply the changes to the system.

VLAN Routing

You can configure the D-Link DWS-4000 Series switch with some ports supporting VLANs and some supporting routing. You can also configure the software to allow traffic on a VLAN to be treated as if the VLAN were a router port.

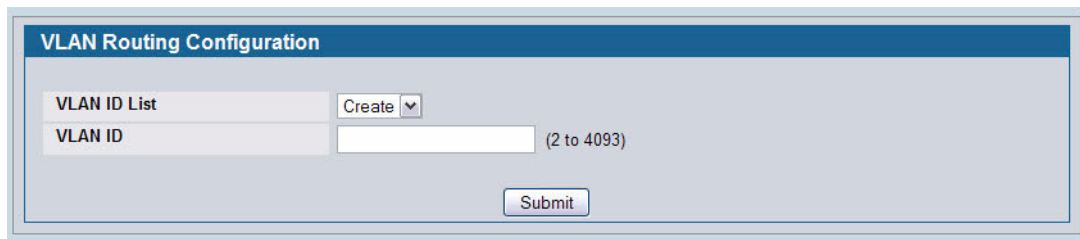
When a port is enabled for bridging (default) rather than routing, all normal bridge processing is performed for an inbound packet, which is then associated with a VLAN. Its MAC Destination Address (MAC DA) and VLAN ID are used to search the MAC address table. If routing is enabled for the VLAN, and the MAC DA of an inbound unicast packet is that of the internal bridge-router interface, the packet is routed. An inbound multicast packet is forwarded to all ports in the VLAN, plus the internal bridge-router interface, if it was received on a routed VLAN.

Since a port can be configured to belong to more than one VLAN, VLAN routing might be enabled for all of the VLANs on the port, or for a subset. VLAN Routing can be used to allow more than one physical port to reside on the same subnet. It could also be used when a VLAN spans multiple physical networks, or when additional segmentation or security is required. This section shows how to configure D-Link DWS-4000 Series Unified Switch software to support VLAN routing. A port can be either a VLAN port or a router port, but not both. However, a VLAN port may be part of a VLAN that is itself a router port.

VLAN Routing Configuration

Use the VLAN Routing Configuration page to configure VLAN Routing interfaces on the system.

To display the page, click **LAN > L3 Features > Router > VLAN Routing Configuration** in the navigation tree. [Figure 208](#) shows the page when no VLAN routing interfaces exist.



The screenshot shows a web interface for configuring VLAN routing. At the top, there is a blue header bar with the text "VLAN Routing Configuration". Below this, there is a form area with a light gray background. The form contains a "VLAN ID List" section with a "Create" dropdown menu. Below that, there is a "VLAN ID" input field with a "(2 to 4093)" range indicator. At the bottom right of the form area, there is a "Submit" button.

Figure 208: VLAN Routing Configuration

Figure 208 shows the page when at least one VLAN routing interface has been created.

VLAN Routing Configuration	
VLAN ID List	588
Interface	4/1
MAC Address	00:17:9A:95:05:CA
IP Address	0.0.0.0
Subnet Mask	0.0.0.0

Delete

Figure 209: VLAN Routing Configuration - Interface Exists

Table 188: VLAN Routing Configuration Fields

Field	Description
VLAN ID	Enter the ID of a VLAN to configure for VLAN Routing. Initially, the field will display the ID of the first VLAN. After you enter a new VLAN ID and click Create , the non-configurable data will be displayed.
Interface	The logical slot and port number assigned to the VLAN Routing Interface.
MAC Address	The MAC Address assigned to the VLAN Routing Interface.
IP Address	The configured IP Address of the VLAN Routing Interface. Note that if a VLAN is created and the IP address is not configured, the page by default shows an IP address of 0.0.0.0. To configure the IP address, go to LAN > L3 Features > Routing > IP > Interface Configuration . In the Interface field on the IP Interface Configuration page, select the interface identified in the Interface field (e.g. 4/1) on the VLAN Routing Configuration page.
Subnet Mask	The configured Subnet Mask of the VLAN Routing Interface. This is 0.0.0.0 when the VLAN Routing Interface is first configured and must be entered on the IP Interface Configuration page.

Creating a VLAN Routing Interface

1. Enter a new VLAN ID in the **VLAN ID** field.
2. Click **Create**.

The page refreshes and displays the interface and MAC address assigned to the new VLAN. The interface is in Slot/Port notation. The IP address and Subnet Mask fields are 0.0.0.0.



Note: Be sure to note the interface Slot/Port assignment so that you select the correct interface to configure from the Interface Configuration page.

3. In the navigation menu, click **LAN > L3 Features > IP > Interface Configuration**.
4. Select the interface assigned to the VLAN.
The IP address and Subnet Mask fields are 0.0.0.0 by default.

5. Enter the IP address and subnet mask for the VLAN, and configure any other interface settings.

IP Interface Configuration	
Interface	4/1
Routing Interface Status	Down
IP Address Configuration Method	Manual
IP Address	192.168.11.54 (X.X.X.X)
Subnet Mask	255.255.255.0
Routing Mode	Enable
Routing Mode	Enable
Administrative Mode	Enable
Link Speed Data Rate	Unknown
Forward Net Directed Broadcasts	Disable
Active State	Inactive
MAC Address	00:17:9A:95:05:CA
Encapsulation Type	Ethernet
Proxy ARP	Enable
Local Proxy ARP	Disable
IP MTU	1500 (68 to 9198) Enter 0 to unconfigure
Bandwidth	10000 (1 to 10000000)
Destination Unreachables	Enable
ICMP Redirects	Enable

Submit Refresh

6. Click **Submit** to apply the settings to the VLAN routing interface.
7. Navigate to the **LAN > Monitoring > VLAN Routing Summary** page to view the new VLAN in the table.

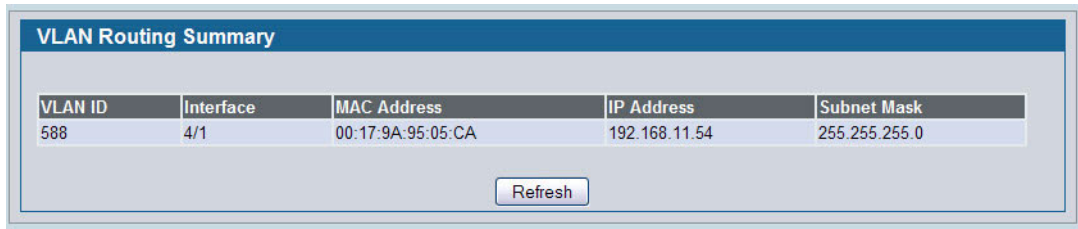
Deleting a VLAN Router Interface

Click **Delete** to delete the selected VLAN routing interface.

VLAN Routing Summary

Use the VLAN Routing Summary page to display information about the VLAN Routing interfaces configured on the system.

To display the page, click **LAN > Monitoring > L3 Status > VLAN Routing Summary** in the navigation tree.



VLAN Routing Summary				
VLAN ID	Interface	MAC Address	IP Address	Subnet Mask
588	4/1	00:17:9A:95:05:CA	192.168.11.54	255.255.255.0

Figure 210: VLAN Routing Summary

Table 189: VLAN Routing Summary Fields

Field	Description
VLAN ID	The ID of the VLAN whose data is displayed in the current table row.
Slot/Port	The logical slot and port number assigned to the VLAN Routing Interface.
MAC Address	The MAC Address assigned to the VLAN Routing Interface.
IP Address	The configured IP Address of the VLAN Routing Interface. Note that if a VLAN is created and the IP address is not configured, the page by default shows an IP address of 0.0.0.0. To configure the IP address, go to LAN > L3 Features > IP > Interface Configuration .
Subnet Mask	The configured Subnet Mask of the VLAN Routing Interface. This is 0.0.0.0 when the VLAN Routing Interface is first configured and must be entered on the IP Interface Configuration page.

Virtual Router Redundancy Protocol (VRRP)

The Virtual Router Redundancy protocol is designed to handle default router failures by providing a scheme to dynamically elect a backup router. The driving force was to minimize “black hole” periods due to the failure of the default gateway router during which all traffic directed towards it is lost until the failure is detected. Though static configuration of default routes is popular, such an approach is susceptible to a single point of failure when the default router fails. VRRP advocates the concept of a “virtual router” associated with one or more IP Addresses that serve as default gateways. In the event that the VRRP Router controlling these IP Addresses (formally known as the Master) fails, the group of IP Addresses and the default forwarding role is taken over by a Backup VRRP Router.

VRRP Configuration

Use the VRRP Configuration page to enable or disable the administrative status of a virtual router.

To display the page, click **LAN > L3 Features > VRRP > VRRP Configuration** in the navigation tree.

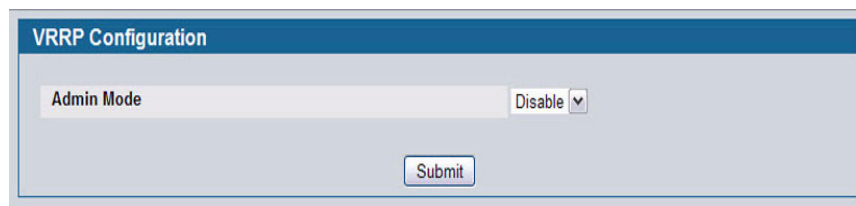


Figure 211: VRRP Configuration

Table 190: VRRP Configuration

Field	Description
Admin Mode	This sets the administrative status of VRRP in the router to active or inactive. Select Enable or Disable from the dropdown menu. The default is Disable.

- If you change the administrative mode, click **Submit** to apply the changes to the system.

Virtual Router Configuration

Use the Virtual Router Configuration page to create a new virtual router or to configure an existing one.

To display the page, click **LAN > L3 Features > VRRP > Virtual Router Interface** in the navigation tree.

Figure 212: Virtual Router Configuration

Table 191: Virtual Router Configuration Fields

Field	Description
VRID	Select Create from the menu to configure a new Virtual Router, or select one of the existing Virtual Routers, listed by interface number and VRID.
VRID	This field is only configurable if you are creating new Virtual Router, in which case enter the VRID in the range 1 to 255.
Interface	This field is only configurable if you are creating new Virtual Router, in which case select the interface for the new Virtual Router from the menu.
Pre-empt Mode	Select Enable or Disable from the dropdown menu. If you select Enable, a backup router preempts the master router if it has a priority greater than the master virtual router's priority, provided that the master is not the owner of the virtual router's IP address. The default is Enable.
Accept Mode	Set the accept mode: <ul style="list-style-type: none"> • Enable: The VRRP master will accept all types of data packets addressed to IP address(es) associated with the virtual router • Disable: The VRRP master will discard all types of data packets addressed to IP address(es) associated with the virtual router if it is not the IP address owner. The default is disable.

Table 191: Virtual Router Configuration Fields (Cont.)

Field	Description
Configured Priority	Enter the priority value to be used by the VRRP router in the election for the master virtual router. If the Virtual IP Address is the same as the interface IP Address, the priority gets set to 255 no matter what you enter. If you enter a priority of 255 when the Virtual and interface IP Addresses are not the same, the priority gets set to the default value of 100.
Priority	The operational priority of the VRRP router. This is relative to the configured priority. The operational priority depends upon the configured priority, and the priority decrements configured through the tracking process.
Advertisement Interval (secs)	Enter the time, in seconds, between the transmission of advertisement packets by this virtual router. Enter a number between 1 and 255. The default value is 1 second.
Interface IP Address	Indicates the IP Address associated with the selected interface.
IP Address	Enter the IP Address associated with the Virtual Router. The default is 0.0.0.0, which you must change prior to clicking Create .
Authentication Type	Select the type of Authentication for the Virtual Router from the dropdown menu. The default is None. The choices are: <ul style="list-style-type: none"> • 0-None: No authentication is performed. • 1-Simple: Authentication is performed using a text password.
Authentication Data	If you selected simple authentication, enter the password.
Status	Select active or inactive from the dropdown menu to start or stop the operation of the Virtual Router. The default is inactive.

Command Buttons

- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Secondary IP Address** to proceed to the Secondary IP Address configuration page.
- Click **Delete** to delete the selected Virtual Router. Note that the router cannot be deleted if there are secondary addresses configured.
- Click **Track Interface** to proceed to the VRRP Track Interface configuration page.
- Click **Track Route** to proceed to the VRRP Track Route configuration page.

Configuring a Secondary VRRP Address

To configure a secondary VRRP address, first configure one IP address (the primary address) for the VR. Then, you can add multiple secondary addresses to that interface.

- Click **Submit** to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Delete** to delete the selected secondary IP address.
- Click **Cancel** to return to the Virtual Router Configuration page.

Creating a New Virtual Router

1. From the **Virtual Router Configuration** page, select **Create** from the VRID and Slot/Port menu.
2. Specify the VRID, the virtual router address, and the interface for the new virtual router.
3. Define the remaining fields as needed.
4. Click **Create** to apply the changes to the system.

The new virtual router is saved, and the device is updated.

Modifying a Virtual Router

To modify the settings for an existing virtual router, select its ID from the VRID and Slot/Port menu and change the fields as needed. Click **Submit** to apply the changes to the system.

VRRP Interface Tracking Configuration

Use VRRP Interface Tracking to track a specific interface IP state within the router that can alter the priority level of a virtual router for a VRRP group. An exception to this is, if that VRRP group is the IP address owner, its priority is fixed at 255 and cannot be reduced through the tracking process.

To display the page, click **LAN > L3 Features > VRRP > Virtual Router Configuration** in the navigation tree, then click the **Track Interface** button.

Figure 213: VRRP Interface Tracking Configuration

Table 192: VRRP Interface Tracking Configuration Fields

Field	Description
Slot/Port	The interface associated with the Virtual Router ID.
Virtual Router ID	The Virtual Router ID for which data is to be displayed.
Tracking Interface	The Tracked Interface for which data is to be displayed.
Priority Decrement	The priority decrement for the tracked interface. The valid range is 1 to 254. The default value is 10.
Interface State	The IP state of the tracked interface.
Remove	Removes the selected Tracking Interface from the VRRP tracked list.

- Click **Add** to proceed to the VRRP Interface Tracking page.
- Click **Submit** to apply the new configuration. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Refresh** to refresh the page with the most current data from the switch.
- Click **Cancel** to return to the Virtual Router Configuration page.

VRRP Interface Tracking

Use the VRRP Interface Tracking page to add an interface to the tracking list. This page is accessible by clicking **Add** from the [Virtual Router Configuration](#) page.

Figure 214: VRRP Interface Tracking

Table 193: VRRP Track Interface Fields

Field	Description
Slot/Port	The interface associated with the Virtual Router ID.
Virtual Router ID	The Virtual Router ID for which data is to be displayed.
Track Slot/Port	Displays all routing interfaces which are not yet tracked for this Virtual Router ID and interface configuration. Exceptions to this: loopback and tunnels could not be tracked.
Priority Decrement	The priority decrement for the tracked interface. The valid range is 1-254. The default value is 10.

- Click **Submit** to send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Cancel** to return to the VRRP Interface Tracking Configuration page.

VRRP Route Tracking Configuration

Use VRRP Route Tracking Configuration to track specific route IP states within the router that can alter the priority level of a virtual router for a VRRP group.

To display the page, click **LAN > L3 Features > VRRP > Virtual Router Configuration** in the navigation tree, then click the **Track Route** button.

VRRP Route Tracking Configuration				
Interface	6/2			
Virtual Router ID	10			
VRRP Tracking Routes List				
Tracking Route Pfx	Tracking Route PfxLen	Priority Decrement	Reachable	Remove
10.27.65.0	24	10	FALSE	<input type="checkbox"/>
<input type="button" value="Add"/> <input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="Cancel"/>				

Figure 215: VRRP Route Tracking Configuration

Table 194: VRRP Route Tracking Configuration Fields

Field	Description
Interface	The interface associated with the Virtual Router ID.
Virtual Router ID	The Virtual Router ID for which tracking data is to be displayed.
Tracking Route Pfx	The prefix of the tracked route.
Tracking Route PfxLen	The prefix length of the tracked route.
Priority Decrement	Enter the priority decrement for the tracked route. The valid range is 1-254. The default value is 10.
Reachable	The reachability of the tracked route.
Remove	Removes the selected tracking routes from the VRRP tracked list.

- Click **Add** to proceed to the VRRP Route Tracking page.
- Click **Submit** to send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a Save configuration is performed.
- Click **Refresh** to refresh the page with the most current data from the switch.
- Click **Cancel** to return to the Virtual Router Configuration page.

VRRP Route Tracking

Use the VRRP Route Tracking page to add a route into the tracking list. To access this page, click **Add** from the [VRRP Route Tracking](#) page.

Virtual Router Tracking Route Add	
Interface	6/2
Virtual Router ID	10
Track Route Pfx	<input type="text" value="10.27.65.0"/>
Track Route PfxLen	<input type="text" value="24"/> (1 to 32)
Priority Decrement	<input type="text" value="10"/> (1 to 254)
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 216: VRRP Route Tracking

Table 195: VRRP Route Tracking Fields

Field	Description
Interface	The Interface associated with the Virtual Router ID.
Virtual Router ID	The Virtual Router ID for which data is to be displayed.
Track Route Pfx	The prefix of the route.
Track Route PfxLen	The prefix length of the route.
Priority Decrement	The priority decrement for the route. The valid range is 1-254. The default value is 10.

- Click **Submit** to send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a Save is performed.
- Click **Cancel** to return to the VRRP Route Tracking Configuration page.

Virtual Router Status

Use the Virtual Router Status page to display virtual router status.

To display the page, click **LAN > Monitoring > L3 Status > Virtual Router Status** in the navigation tree.

VRID	Slot/Port	Priority	Pre-empt Mode	Advertisement Interval (secs)	Virtual IP Address	Interface IP Address	Address Owner	VMAC Address	Auth Type	State	Status	Secondary IP Address
1	0/1	100	Enable	1	1.1.1.1	0.0.0.0	False	00:00:5E:00:01:01	None	Initialize	Active	

Figure 217: Virtual Router Status

Table 196: Virtual Router Status Fields

Field	Description
VRID	Virtual Router Identifier.
Slot/Port	Indicates the interface associate with the VRID.
Priority	The priority value used by the VRRP router in the election for the master virtual router.
Pre-empt Mode	<ul style="list-style-type: none"> • Enable: If the Virtual Router is a backup router, it preempts the master router if it has a priority greater than the master virtual router's priority provided that the master is not the owner of the virtual router IP address. • Disable: If the Virtual Router is a backup router it does not preempt the master router even if its priority is greater.
Advertisement Interval(secs)	The time, in seconds, between the transmission of advertisement packets by this virtual router.
Virtual IP Address	The IP Address associated with the Virtual Router.
Interface IP Address	The actual IP Address associated with the interface used by the Virtual Router.
Owner	Set to True if the Virtual IP Address and the Interface IP Address are the same, otherwise set to False. If this parameter is set to True, the Virtual Router is the owner of the Virtual IP Address, and always wins an election for master router when it is active.
VMAC Address	The virtual MAC Address associated with the Virtual Router, composed of a 24-bit organizationally unique identifier, the 16-bit constant identifying the VRRP address block and the 8-bit VRID. The Virtual MAC address is: 00:00:5e:00:01:XX, where XX is the VRID.
Auth Type	The type of authentication in use for the Virtual Router <ul style="list-style-type: none"> • None: Specifies that the authentication type is none. • Simple: Specifies that the authentication type is a simple text password.
State	The current state of the Virtual Router: <ul style="list-style-type: none"> • Initialize • Master • Backup
Status	The current status of the Virtual Router: <ul style="list-style-type: none"> • Inactive • Active
Secondary IP Address	A secondary VRRP address configured for the primary VRRP.

- Click **Refresh** to update the information on the page with the most current data from the switch.

Virtual Router Statistics

Use the Virtual Router Statistics page to display statistics for a specified virtual router.

To display the page, click **LAN > Monitoring > L3 Status > Virtual Router Statistics** in the navigation tree.

Figure 218 shows the fields on the **Virtual Router Statistics** page for a switch that has one or more virtual routers configured.

Virtual Router Statistics	
Router Checksum Errors	0
Router Version Errors	0
Router VRID Errors	0
Slot/Port	6/2
VRID	10
Up Time	0 days, 0 hours, 0 minutes, 0 secs
State Transitioned To Master	0
Advertisement Received	0
Advertisement Interval Errors	0
Authentication Failure	0
IP TTL Errors	0
Zero Priority Packets Received	0
Zero Priority Packets Sent	0
Invalid Type Packets Received	0
Address List Errors	0
Invalid Authentication Type	0
Authentication Type Mismatch	0
Packet Length Errors	0

Refresh

Figure 218: Virtual Router Statistics—Virtual Router Configured

The Virtual Router Statistics page contains the fields listed below. Many of the fields display only when there is a valid VRRP configuration.

Table 197: Virtual Router Statistics Fields

Field	Description
Router Checksum Errors	The total number of VRRP packets received with an invalid VRRP checksum value.
Router Version Errors	The total number of VRRP packets received with an unknown or unsupported version number.
Router VRID Errors	The total number of VRRP packets received with an invalid VRID for this virtual router.
VRID and Slot/Port	Select the existing Virtual Router, listed by interface number and VRID, for which you want to display statistical information.
VRID	the VRID for the selected Virtual Router.

Table 197: Virtual Router Statistics Fields (Cont.)

Field	Description
Slot/Port	The interface for the selected Virtual Router.
Up Time	The time, in days, hours, minutes and seconds, that has elapsed since the virtual router transitioned to the initialized state.
State Transitioned to Master	The total number of times that this virtual router's state has transitioned to Master.
Advertisement Received	The total number of VRRP advertisements received by this virtual router.
Advertisement Interval Errors	The total number of VRRP advertisement packets received for which the advertisement interval was different than the one configured for the local virtual router.
Authentication Failure	The total number of VRRP packets received that did not pass the authentication check.
IP TTL Errors	The total number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
Zero Priority Packets Received	The total number of VRRP packets received by the virtual router with a priority of 0.
Zero Priority Packets Sent	The total number of VRRP packets sent by the virtual router with a priority of 0.
Invalid Type Packets Received	The number of VRRP packets received by the virtual router with an invalid value in the Type field.
Address List Errors	The total number of packets received for which the address list does not match the locally configured list for the virtual router.
Invalid Authentication Type	The total number of packets received with an unknown authentication type.
Authentication Type Mismatch	The total number of packets received with an authentication type different to the locally configured authentication method.
Packet Length Errors	The total number of packets received with a packet length less than the length of the VRRP header.

- Click **Refresh** to update the screen with the most current information.

Section 6: Configuring Quality of Service

This section gives an overview of Quality of Service (QoS) and explains the QoS features available from the Quality of Service navigation tree menu, which include the following:

- [“Configuring Class of Service”](#)
- [“Configuring Differentiated Services”](#)
- [“Configuring Auto VoIP”](#)

In a typical switch, each physical port consists of one or more queues for transmitting packets on the attached network. Multiple queues per port are often provided to give preference to certain packets over others based on user-defined criteria. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission. As queues become full, packets have no place to be held for transmission and get dropped by the switch.

QoS is a means of providing consistent, predictable data delivery by distinguishing between packets that have strict timing requirements from those that are more tolerant of delay. Packets with strict timing requirements are given “special treatment” in a QoS capable network. With this in mind, all elements of the network must be QoS-capable. The presence of at least one node which is not QoS-capable creates a deficiency in the network path and the performance of the entire packet flow is compromised.

Configuring Class of Service

The Class of Service (CoS) queueing feature lets you directly configure certain aspects of switch queueing. This provides the desired QoS behavior for different types of network traffic when the complexities of DiffServ are not required. The priority of a packet arriving at an interface can be used to steer the packet to the appropriate outbound CoS queue through a mapping table. CoS queue characteristics that affect queue mapping, such as minimum guaranteed bandwidth, transmission rate shaping, etc., are user-configurable at the queue (or port) level. The system supports eight (0 to 7) queues per port.

Mapping 802.1p Priority

The IEEE 802.1p feature allows traffic prioritization at the MAC level. The switch can prioritize traffic based on the 802.1p tag attached to the L2 frame. Each port on the switch has multiple queues to give preference to certain packets over others based on the class of service (CoS) criteria you specify. When a packet is queued for transmission in a port, the rate at which it is serviced depends on how the queue is configured and possibly the amount of traffic present in the other queues of the port. If a delay is necessary, packets get held in the queue until the scheduler authorizes the queue for transmission.

Use the 802.1p Priority Mapping page in the Class of Service folder to assign 802.1p priority values to various traffic classes on one or more interfaces.

To display the page, click **LAN > QoS > Class of Service > 802.1p Priority Mapping** in the navigation tree.

Figure 219: 802.1p Priority Mapping

Table 198: 802.1p Priority Mapping

Field	Description
Interface	Selects the interface to which the class of service configuration is applied.
802.1p Priority	Displays the 802.1p priority to be mapped. Priority goes from low (0) to high (7). For example, traffic with a priority of 0 is for most data traffic and is sent using “best effort.” Traffic with a higher priority, such as 6, might be time-sensitive traffic, such as voice or video.
Traffic Class	The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent. To change the default priority-to-queue mapping, select a new traffic class value from the drop-down menu.

- If you make any changes to the page, click **Submit** to apply the new values to the system.

Trust Mode Configuration

Use the Trust Mode Configuration page to set the class of service trust mode of an interface. Each port in the switch can be configured to trust one of the packet fields (802.1p or IP DSCP), or to not trust any packet’s priority designation (untrusted mode). If the port is set to a trusted mode, it uses a mapping table appropriate for the trusted field being used. This mapping table indicates the CoS queue to which the packet should be forwarded on the appropriate egress port(s). Of course, the trusted field must exist in the packet for the mapping table to be of any use, so there are default actions performed when this is not the case. These actions involve directing the packet to a specific CoS level configured for the ingress port as a whole, based on the existing port default priority as mapped to a traffic class by the current 802.1p mapping table.

Alternatively, when a port is configured as untrusted, it does not trust any incoming packet priority designation and uses the port default priority value instead. All packets arriving at the ingress of an untrusted port are directed to a specific CoS queue on the appropriate egress port(s) in accordance with the configured default priority of the ingress port. This process is also used for cases where a trusted port mapping is unable to be honored, such as when a non-IP packet arrives at a port configured to trust the IP precedence or IP DSCP value.

To display the Trust Mode Configuration page, click **LAN > QoS > Class of Service > Trust Mode Configuration** in the navigation menu.

802.1p Priority	Traffic Class
0	1
1	0
2	0
3	1
4	2
5	2
6	3
7	3

Figure 220: Trust Mode Configuration

Table 199: Trust Mode Configuration Fields

Field	Description
Interface	The menu contains all CoS configurable interfaces. Select the Global option to apply the same trust mode to all interfaces. Select an individual interface from the menu to override the global settings on a per-interface basis.
Interface Trust Mode	Specifies whether or not an interface (or all interfaces if the Slot/Port field is set to Global) trust a particular packet marking when the packet enters the port. The default value is trust dot1p. The mode can only be one of the following: <ul style="list-style-type: none"> • untrusted • trust dot1p • trust ip-dscp
Non-IP Traffic Class	This field appears if the trust mode for the selected interface is trust ip-dscp. The field displays the traffic class (queue) to which all non-IP traffic is directed when in the interface trust mode is trust ip-dscp. The value is fixed to 1.
Untrusted Traffic Class	This field appears if the trust mode for the selected interface is untrusted. The field displays the traffic class (queue) to which all traffic is directed when in untrusted mode. The value is fixed to 1.

The **Trust Mode Configuration** page also displays the Current 802.1p Priority Mapping table. For information about 802.1p priority mapping, see [“Mapping 802.1p Priority” on page 329](#).

To access the 802.1 priority mapping configuration page, click **LAN > QoS > Class of Service > 802.1p Priority Mapping** in the navigation menu. For more information, see [“Mapping 802.1p Priority” on page 329](#).

- If you make changes to the **Trust Mode Configuration** page, click **Submit** to apply the changes to the system.
- Click **Restore Defaults** to reset the selected interface (or all interfaces, if Global is selected) to the default trust value.

IP DSCP Mapping Configuration

Use the IP DSCP Mapping Configuration page to map an IP DSCP value to an internal traffic class.

To display the IP DSCP Mapping Configuration page, click **LAN > QoS > Class of Service > IP DSCP Mapping Configuration** in the navigation menu.

IP DSCP Value	Traffic Class
0	1
1	1
2	1
3	1
4	1
5	1

Figure 221: IP DSCP Mapping Configuration

Table 200: IP DSCP Mapping Configuration Fields

Field	Description
Interface	The menu contains all CoS configurable interfaces. The only option is Global, which means that the IP DSCP mapping configuration applies to all interfaces and cannot be applied on a per-interface basis.
IP DSCP Values	Lists the IP DSCP values to which you can map an internal traffic class. The values range from 0-63.
Traffic Class	The traffic class is the hardware queue for a port. Higher traffic class values indicate a higher queue position. Before traffic in a lower queue is sent, it must wait for traffic in higher queues to be sent. Valid range is 0 to 7.

- If you make changes to the page, click **Submit** to apply the changes to the system. Click **Restore Defaults** to reset all interfaces to the default trust value.

CoS Interface Configuration

Use the CoS Interface Configuration page to apply an interface shaping rate to all ports or to a specific port.

To display the CoS Interface Configuration page, click **LAN > QoS > Class of Service > CoS Interface Configuration** in the navigation menu.

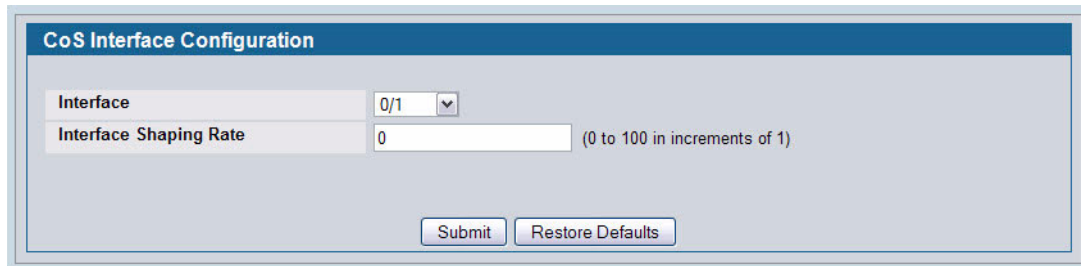


Figure 222: Interface Configuration

Table 201: Interface Configuration Fields

Field	Description
Interface	Selects the CoS configurable interface to be affected by the Interface Shaping Rate. Select Global to apply a rate to all interfaces. Select an individual port to override the global setting.
Interface Shaping Rate	Sets the limit on how much traffic can leave a port. The limit on maximum transmission bandwidth has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The specified value represents a percentage of the maximum negotiated bandwidth. The default value is zero (0). Valid values are 0-100, in increments of 1. A value of 0 means the maximum is unlimited.

- If you make changes to the page, click **Submit** to apply the changes to the system. Click **Restore Defaults** to reset all interfaces to the default trust value.

CoS Interface Queue Configuration

Use the CoS Interface Queue Configuration page to define what a particular queue does by configuring switch egress queues. User-configurable parameters control the amount of bandwidth used by the queue, the queue depth during times of congestion, and the scheduling of packet transmission from the set of all queues on a port. Each port has its own CoS queue-related configuration.

The configuration process is simplified by allowing each CoS queue parameter to be configured globally or per-port. A global configuration change is automatically applied to all ports in the system.

To display the Interface Queue Configuration page, click **LAN > QoS > Class of Service > CoS Interface Queue Configuration** in the navigation menu.

Figure 223: Interface Queue Configuration

Table 202: Interface Queue Configuration Fields

Field	Description
Interface	Specifies the interface (physical, LAG, or Global) to configure.
Minimum Bandwidth Allocated	Shows the sum of individual Minimum Bandwidth values for all queues in the interface. The sum cannot exceed the defined maximum of 100. This value is considered while configuring the Minimum Bandwidth for a queue in the selected interface.
Queue ID	Use the menu to select the queue per interface to be configured.
Minimum Bandwidth	Specify the minimum guaranteed bandwidth allocated to the selected queue on the interface. Setting this value higher than its corresponding Maximum Bandwidth automatically increases the maximum to the same value. The default value is 0. The valid range is 0 to 100, in increments of 1. The value zero (0) means no guaranteed minimum. The sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum 100.

Table 202: Interface Queue Configuration Fields (Cont.)

Field	Description
Scheduler Type	<p>Selects the type of queue processing from the dropdown menu. Options are Weighted and Strict. Defining on a per-queue basis allows the user to create the desired service characteristics for different types of traffic.</p> <ul style="list-style-type: none"> • Weighted: Weighted round robin associates a weight to each queue. This is the default. • Strict: Strict priority services traffic with the highest priority on a queue first
Queue Management Type	<p>Displays the type of queue depth management techniques used for all queues on this interface. Queue Management Type can only be Taildrop. The default value is Taildrop. All packets on a queue are safe until congestion occurs. At this point, any additional packets queued are dropped.</p>

- If you make changes to the page, click **Submit** to apply the changes to the system.
- Click **Restore Defaults for all Queues** to reset the settings for the selected interface.
- To reset the defaults for all interfaces, select Global from the **Slot/Port** menu before you click the button.

CoS Interface Queue Status

To display the Interface Queue Status page, click **LAN > Monitoring > Class of Service > Interface Queue Status** in the navigation menu.

Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
0	0	weighted	taildrop
1	0	weighted	taildrop
2	0	weighted	taildrop
3	0	weighted	taildrop
4	0	weighted	taildrop
5	0	weighted	taildrop
6	0	weighted	taildrop
7	0	weighted	taildrop

Figure 224: Interface Queue Status

For information about the fields the page displays, see [Table 202 on page 334](#).

Configuring Differentiated Services

The QoS feature contains Differentiated Services (DiffServ) support that allows traffic to be classified into streams and given certain QoS treatment in accordance with defined per-hop behaviors.

Standard IP-based networks are designed to provide “best effort” data delivery service. “Best effort” service implies that the network delivers the data in a timely fashion, although there is no guarantee that it will. During times of congestion, packets may be delayed, sent sporadically, or dropped. For typical Internet applications, such as e-mail and file transfer, a slight degradation in service is acceptable and in many cases unnoticeable. Conversely, any degradation of service has undesirable effects on applications with strict timing requirements, such as voice or multimedia.

To use DiffServ for QoS, the web pages accessible from the Differentiated Services menu must first be used to define the following categories and their criteria:

1. **Class:** Create classes and define class criteria.
2. **Policy:** Create policies, associate classes with policies, and define policy statements.
3. **Service:** Add a policy to an inbound interface

Packets are classified and processed based on defined criteria. The classification criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs. A policy can contain multiples classes. When the policy is active, the actions taken depend on which class matches the packet.

Packet processing begins by testing the class match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

The Differentiated Services menu page contains links to the various Diffserv configuration and display features.

Diffserv Configuration

Packets are filtered and processed based on defined criteria. The filtering criteria is defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per-class instance basis, and it is these attributes that are applied when a match occurs.

The configuration process begins with defining one or more match criteria for a class. Then one or more classes are added to a policy. Policies are then added to interfaces.

Packet processing begins by testing the match criteria for a packet. The ‘all’ class type option defines that each match criteria within a class must evaluate to true for a packet to match that class. The ‘any’ class type option defines that at least one match criteria must evaluate to true for a packet to match that class. Classes are tested in the order in which they were added to the policy. A policy is applied to a packet when a class match within that policy is found.

Use the Diffserv Configuration page to display DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables.

To display the page, click **LAN > Quality of Service > Differentiated Services > Diffserv Configuration** in the navigation menu.

MIB Table	Current Size / Max Size
Class table	0 / 32
Class Rule table	0 / 192
Policy table	0 / 64
Policy Instance table	0 / 768
Policy Attributes table	0 / 2304
Service table	0 / 116

Figure 225: Diffserv Configuration

Table 203: Diffserv Configuration Fields

Field	Description
Diffserv Admin Mode	Turns admin mode on and off. The default value is Enable. While disabled, the DiffServ configuration is retained and can be changed, but it is not active. While enabled, Differentiated Services are active.
MIB Table	
Class Table	Displays the current and maximum number of rows of the class table.
Class Rule Table	Displays the current and maximum number of rows of the class rule table.
Policy Table	Displays the current and maximum number of rows of the policy table.
Policy Instance Table	Displays the current and maximum number of rows of the policy instance table.
Policy Attributes Table	Displays the current and maximum number of rows of the policy attributes table.
Service Table	Displays the current and maximum number of rows of the service table.

- If you change the DiffServ admin mode, click **Submit** to apply the change to the system.

Class Configuration

Use the Class Configuration page to add a new Diffserv class name, or to rename or delete an existing class. The page also allows you to define the criteria to associate with a DiffServ class. As packets are received, these DiffServ classes are used to prioritize packets. You can have multiple match criteria in a class. The logic is a Boolean logical AND for this criteria.

To display the page, click **LAN > QoS > Differentiated Services > Class Configuration** in the navigation menu.

The fields available on the Class Configuration page depend on whether you create a new class or configure a class that has already been created.

Figure 226 shows the Class Configuration page when the Class Selector option is Create.

The screenshot shows the 'DiffServ Class Configuration' form. The 'Class Selector' dropdown is set to 'Create'. The 'Class Name' field is empty, with a note '(1 to 31 alphanumeric characters)'. The 'Class Type' dropdown is set to 'All', and the 'Class Layer 3 Protocol' dropdown is set to 'IPv4'. At the bottom, there are 'Submit' and 'Cancel' buttons.

Figure 226: Diffserv Class Configuration

Figure 227 shows the Class Configuration page when the Class Selector option shows a configured class. The class has two class match selectors configured.

The screenshot shows the 'DiffServ Class Configuration' form for an existing class. The 'Class Selector' dropdown is set to 'class1'. The 'Class Name' field contains 'class1', with a note '(1 to 31 alphanumeric characters)'. To the right of the 'Class Name' field are 'Rename' and 'Delete' buttons. The 'Class Type' is 'All' and the 'Class Layer 3 Protocol' is 'IPv4'. Below these fields is a 'Class Match Selector' dropdown. At the bottom, there is a table with two columns: 'Match Criteria' and 'Values'.

Match Criteria	Values
Destination IP Address	192.168.10.3 (255.255.255.0)
Destination L4 Port	80(http/www)

Figure 227: Diffserv Class Configuration

Table 204: Diffserv Class Configuration Fields

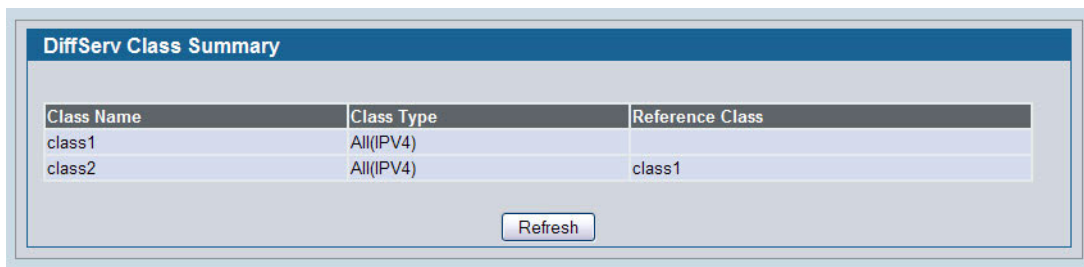
Field	Description
Class Selector	To configure a new DiffServ class, select Create. To modify or view an existing class, select the name of the class from the dropdown menu.
Class Name	Enter a class name. To create a new class, select the class type and click Submit . To rename an existing class, click Rename after you enter the class name.
Class Type	Lists all of the class types. Currently the hardware supports only the Class Type value All , which means all the various match criteria defined for the class should be satisfied for a packet match. All signifies the logical AND of all the match criteria.
Class Layer 3 Protocol	The DiffServ feature supports classification of IPv4 packets only.
Class Match Selector	<p>The menu lists all match criteria you can add to a specified class. To configure the criteria, select a match criteria from the list, and then click Add Match Criteria. The screen changes to the criteria configuration page for that class. After you configure the criteria, click Submit to apply the criteria to the class and return to the Class Configuration page. To return to the Class Configuration page without applying the criteria, click Cancel. The match criteria and configurable fields are as follows:</p> <ul style="list-style-type: none"> • Destination IP Address: Requires a packet's destination IP address to match the address listed here. In the IP Address field, enter a valid destination IP address in dotted decimal format. In the IP Mask field, enter a valid subnet mask to determine which bits in the IP address are significant. Note that this is <i>not</i> a wildcard mask. • Destination Layer 4 Port: Requires a packet's TCP/UDP destination port to match the port you select. Select the desired L4 keyword from the list on which the rule can be based. If you select Other, the screen refreshes and a Port ID field appears. Enter a user-defined Port ID by which packets are matched to the rule. The valid range is 0–65535. • Any: All packets are considered to match the specified class and no additional input information is needed. • IP DSCP: Matches the packet's DSCP to the class criteria's when selected. Select the DSCP type from the menu or enter a DSCP value to match. If you select Other, enter a custom value in the DSCP Value field that appears. The valid range is 0–63. • IP Precedence: Matches the packet's IP Precedence value to the class criteria's when Enter a value in the range of 0–7. • IP TOS: Matches the packet's Type of Service bits in the IP header to the class criteria's when selected and a value is entered. In the TOS Bits field, enter a two-digit hexadecimal number to match the bits in a packet's TOS field. In the TOS Mask field, specify the bit positions that are used for comparison against the IP TOS field in a packet.

Table 204: Diffserv Class Configuration Fields (Cont.)

Field	Description
Class Match Selector (cont.)	<ul style="list-style-type: none"> • Protocol: Requires a packet's layer 4 protocol to match the protocol you select. If you select Other, enter a protocol number in the field that appears. The valid range is 0-255. • Reference Class: Selects a class to start referencing for criteria. If the specified class references another class, the Reference Class match criterion disappears from the match list to prevent you adding another class reference, since a specified class can reference at most one other class of the same type. Additionally, a Remove Class Reference button appears on the screen. Click the button to remove the current class reference. • Source IP Address: Requires a packet's source port IP address to match the address listed here. In the IP Address field, enter a valid source IP address in dotted decimal format. In the IP Mask field, enter a valid subnet mask to determine which bits in the IP address are significant. Note that this is <i>not</i> a wildcard mask. • Source Layer 4 Port: Requires a packet's TCP/UDP source port to match the port you select. Select the desired L4 keyword from the list on which the rule can be based. If you select Other, the screen refreshes and a Port ID field appears. Enter a user-defined Port ID by which packets are matched to the rule. The valid range is 0–65535.

DiffServ Class Summary

The DiffServ Class Summary page provides an overview of the classes that have been configured on the switch. To display the page, click **LAN > Monitoring > Differentiated Services > Class Summary** in the navigation menu.



DiffServ Class Summary		
Class Name	Class Type	Reference Class
class1	All(IPV4)	
class2	All(IPV4)	class1

Refresh

Figure 228: Class Summary

Policy Configuration

Use the Policy Configuration page to associate a collection of classes with one or more policy statements.

To display the page, click **LAN > QoS > Differentiated Services > Policy Configuration** in the navigation menu.

The fields available on the Policy Configuration page depend on whether you create a new class or configure a class that has already been created.

Figure 229 shows the Policy Configuration page when the Policy Selector option is Create.

The screenshot shows a web form titled "DiffServ Policy Configuration". It contains three main input fields: "Policy Selector" with a dropdown menu set to "Create", "Policy Name" with a text input field and a note "(1 to 31 Alphanumeric Characters)", and "Policy Type" with a dropdown menu set to "In". A "Submit" button is located at the bottom right of the form.

Figure 229: Policy Configuration

Figure 230 shows the Policy Configuration page when the Policy Selector option shows a configured policy that has a member class. To configure a member class, see [“Class Configuration” on page 338](#).

The screenshot shows the "DiffServ Policy Configuration" page with the "Policy Selector" dropdown set to "p1". The "Policy Name" field contains "p1" and has a note "(1 to 31 alphanumeric characters)". To the right of the "Policy Name" field are "Rename" and "Delete" buttons. Below this, the "Policy Type" dropdown is set to "In". There are two more dropdown menus: "Available Class List" set to "class2" with an "Add Selected Class" button, and "Member Class List" set to "class1" with a "Remove Selected Class" button.

Figure 230: Policy Configuration

Table 205: Policy Configuration Fields

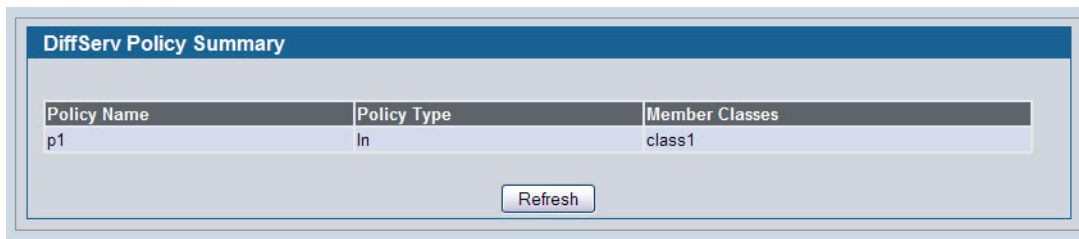
Field	Description
Policy Selector	To create a new policy, select Create from the menu; another page appears to facilitate creation of a new policy. To change a policy name or to modify the class list members, select the policy name from the menu. To delete an existing policy select it from the menu, and then click Delete .
Policy Name	If you select Create from the Policy Selector menu, enter a name to associate with the class(es). The name is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying a policy. To modify the name of an existing policy, select it from the Policy Selector menu and enter a new name in the Policy Name field, and then click Rename .

Table 205: Policy Configuration Fields (Cont.)

Field	Description
Policy Type	The available policy type is <i>In</i> , which indicates the type is specific to inbound traffic. <i>Out</i> indicates the type is specific to outbound traffic direction. This field is only configurable when you create a new policy. After policy creation, this becomes a non-configurable field displaying the configured policy type.
Available Class List	The menu lists all existing DiffServ class names. The list is automatically updated as a new class is added or removed from the policy. To associate a DiffServ class with a policy, select the name of the class from the list, and then click Add Selected Class .
Member Class List	The menu lists all DiffServ classes that have been added to the policy. names. To remove a DiffServ class from a policy, select the name of the class from the list, and then click Remove Selected Class . This list is automatically updated as a new class is added or removed from the policy.

DiffServ Policy Summary

The DiffServ Class Summary page provides an overview of the policies that have been configured on the switch. To display the page, click **LAN > Monitoring > Differentiated Services > Policy Summary** in the navigation menu.



DiffServ Policy Summary		
Policy Name	Policy Type	Member Classes
p1	In	class1

Figure 231: Policy Summary

Policy Class Definition

Use the Policy Class Definition page to associate a class to a policy and to define attributes for that policy-class instance.

To display the page, click **LAN > QoS > Differentiated Services > Policy Class Definition** in the navigation menu.

Figure 232: Policy Class Definition

Depending on the selected policy attribute, when you click **Configure Selected Attribute**, a page displays to enable entering an appropriate value. [Table 206](#) describes all fields available on these pages.

Table 206: Policy Class Definition Fields

Field	Description
Policy Selector	Select the policy to associate with a member class from the menu.
Policy Type	The read-only field shows the type of policy.
Member Class List	Select the member class to associate with this policy name from the menu.
Policy Attribute Selector	<p>The menu lists all attributes supported for this type of policy, from which one can be selected. To configure the attributes, select an attribute from the list, and then click Configure Selected Attribute. The screen changes to the attribute configuration page for that attribute. After you configure the attribute, click Submit to apply the criteria to the class and return to the Policy Class Definition page. To return to the Policy Class Definition page without applying the attribute, click Cancel. The attributes and configurable fields are as follows:</p> <ul style="list-style-type: none"> • Assign Queue: Assigns the packets of this policy-class to a queue. Enter an integer from 0-7 in the Queue Id Value field. • Drop Packets: Select this field to drop packets for this policy-class. There are no fields to configure. Once you select Drop, click Configure Select Attribute, and then click Submit, the attribute is added to the policy. • Mark CoS: Enter the specified Class of Service queue number to mark all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7. • Mark IP DSCP: Use this attribute to mark all packets for the associated traffic stream with IP DSCP value you choose from the menu.

Table 206: Policy Class Definition Fields (Cont.)

Field	Description
Policy Attribute Selector (Cont.)	<ul style="list-style-type: none"> • Mark IP Precedence: Use this attribute to mark all packets for the associated traffic stream with the IP Precedence value you enter in the IP Precedence Value field. • Mirror Interface: Use this attribute to specify the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. • Police Simple: Use this attribute to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. The Police Simple attribute configuration page has the following configurable fields: <ul style="list-style-type: none"> – Color Mode: The policing style is color blind. – Committed Rate (Kbps): Used to monitor arrival rate of incoming packets for this class. The range is 1 to 4294967295 kilobits per second (Kbps). – Committed Burst Size (KB): Used to determine the amount of conforming traffic allowed. The range is 1 to 128 KBytes. – Conform Action Selector: Determines what happens to packets that are considered conforming (below the police rate). Select one of the following actions: <ul style="list-style-type: none"> • Send: (default) These packets are presented unmodified by DiffServ to the system forwarding element. • Drop: These packets are immediately dropped. • Mark IP DSCP: These packets are marked by DiffServ with the specified DSCP value before being presented to the system forwarding element. This selection requires that the DSCP value field be set. • Mark IP Precedence: These packets are marked by DiffServ with the specified IP Precedence value before being presented to the system forwarding element. This selection requires that the Mark IP Precedence value field be set. – Violate Action: Determines what happens to packets that are considered non-conforming (above the police rate). Select one of the following actions: <ul style="list-style-type: none"> • Drop: (default) These packets are immediately dropped. • Mark IP DSCP: These packets are marked by DiffServ with the specified DSCP value before being presented to the system forwarding element. This selection requires that the DSCP value field be set. • Mark IP Precedence: These packets are marked by DiffServ with the specified IP Precedence value before being presented to the system forwarding element. This selection requires that the Mark IP Precedence value field be set. • Send: (default) These packets are presented unmodified by DiffServ to the system forwarding element.

DiffServ Policy Attribute Summary

The DiffServ Policy Attribute Summary page provides an overview of the attributes that have been configured for each policy. To display the page, click **LAN > Monitoring > Differentiated Services > Policy Attribute Summary** in the navigation menu.

Policy Name	Policy Type	Class Name	Attribute	Attribute Details
p1	In	class1	Mark CoS	CoS Value: 3
p2	In	class2	None	Best Effort will be used

Figure 233: Policy Attribute Summary

Service Configuration

Use the Service Configuration page to activate a policy on a port.

To display the page, click **LAN > QoS > Differentiated Services > Service Configuration** in the navigation menu.

Interface: 0/1
Policy In: p1

Figure 234: Service Configuration

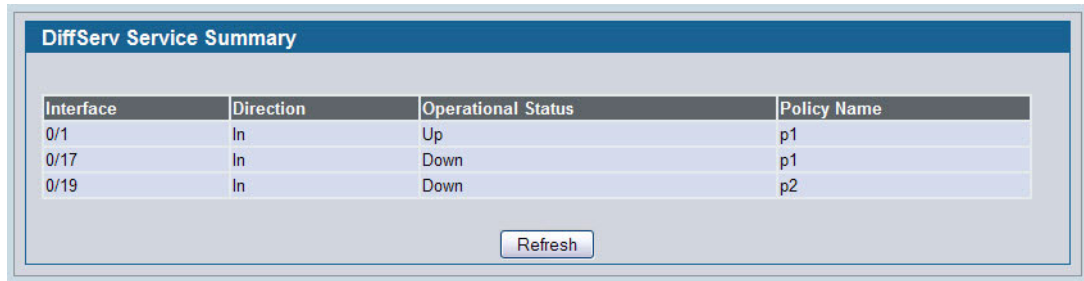
Table 207: Service Configuration Fields

Field	Description
Interface	Selects the interface (physical, LAG, or All) to be affected from menus. This is a list of all valid slot number and port number combinations in the system, including all interfaces.
Policy In	This lists all the policy names of type 'In' to be associated with the port which can be selected from a menu. If 'None' is selected, this will detach the policy from the interface in this direction.
Direction	This field displays only when All is selected from the Interface menu. Select the traffic direction of this service interface.

To activate a policy on an interface, select the interface and the policy, and then click **Submit**.

DiffServ Service Summary

The DiffServ Service Summary page provides an overview of the policies-port associations. To display the page, click **LAN > Monitoring > Differentiated Services > Service Summary** in the navigation menu.



Interface	Direction	Operational Status	Policy Name
0/1	In	Up	p1
0/17	In	Down	p1
0/19	In	Down	p2

Figure 235: Service Summary

Service Statistics

Use the Service Statistics page to display service-level statistical information about all interfaces that have DiffServ policies attached.

To display the page, click **LAN > Monitoring > Differentiated Services > Service Statistics** in the navigation menu.



Interface	Direction	Operational Status	Offered Octets	Discarded Octets	Sent Octets
0/1	In	Up			
0/17	In	Down			
0/19	In	Down			

Figure 236: Service Statistics

Table 208: Service Statistics Fields

Field	Description
Counter Mode Selector	Use the menu to determine the format of the displayed counter values, which must be either Octets or Packets. The default is Octets.
Service Statistics	
Interface	Shows the interface for which service statistics are to display.
Direction	Shows the direction of packets for which service statistics display.

Table 208: Service Statistics Fields (Cont.)

Field	Description
Operational Status	Shows the operational status of this service interface, which is either Up or Down.
Offered Octets	Shows the total number of packets/octetets offered to all class instances in this service policy before their defined DiffServ treatment is applied. This is the overall count per-interface, per-direction.
Discarded Octets/Packets	Shows the total number of packets/octetets discarded for all class instances in this service policy for any reason due to DiffServ treatment. This is the overall count per-interface, per-direction.
Sent Octets/Packets	Shows the total number of packets/octetets forwarded for all class instances in this service policy after their defined DiffServ treatments were applied. In this case, forwarding means the traffic stream was passed to the next functional element in the data path, such as the switching or routing function of an outbound link transmission element. This is the overall count per-interface, per-direction.

Click **Refresh** to update the information on the screen.

Service Detailed Statistics

Use the Service Detailed Statistics page to display class-oriented statistical information for the policy, which is specified by the interface and direction. The Member Classes drop-down menu is populated on the basis of the specified interface and direction and hence the attached policy (if any). Highlighting a member class name displays the statistical information for the policy-class instance for the specified interface and direction.

To display the page, click **LAN > Monitoring > Differentiated Services > Service Detailed Statistics** in the navigation menu.

Figure 237: Service Detailed Statistics

Table 209: Service Detailed Statistics Fields

Field	Description
Counter Mode Selector	Selects the format of the displayed counter values, which must be either Octets or Packets. The default is Octets.
Interface	List of all valid slot number and port number combinations in the system that have a DiffServ policy currently attached in the In direction.
Direction	Selects the direction of packets for which service statistics are to display. Only shows the direction(s) for which a DiffServ policy is currently attached.
Policy Name	Displays the policy currently attached to the selected interface and direction.
Operational Status	Displays the operational status of the policy currently attached to the specified interface and direction. The value is either Up or Down.
Member Classes	List of all DiffServ classes currently defined as members of the selected Policy Name. Choose one member class name at a time to display its statistics. If no class is associated with the chosen policy, then nothing will be populated in the list.
Offered Packets/Octets	Displays the count of the packets/octets offered to this class instance before the defined DiffServ treatment is applied.
Discarded Packets/Octets	Displays the count of packets/octets discarded for this class instance for any reason due to DiffServ treatment of the traffic class.

Click **Refresh** to update the information on the screen.

Configuring Auto VoIP

Voice over Internet Protocol (VoIP) allows you to make telephone calls using a computer network over a data network like the Internet. With the increased prominence of delay-sensitive applications (voice, video, and other multimedia applications) deployed in networks today, proper QoS configuration will ensure high-quality application performance. The Auto VoIP feature is intended to provide an easy classification mechanism for voice packets so that they can be prioritized above data packets in order to provide better QoS.

The Auto-VoIP feature explicitly matches VoIP streams in Ethernet switches and provides them with a better class of service than ordinary traffic. If you enable the Auto-VoIP feature on an interface, the interface scans incoming traffic for the following call-control protocols:

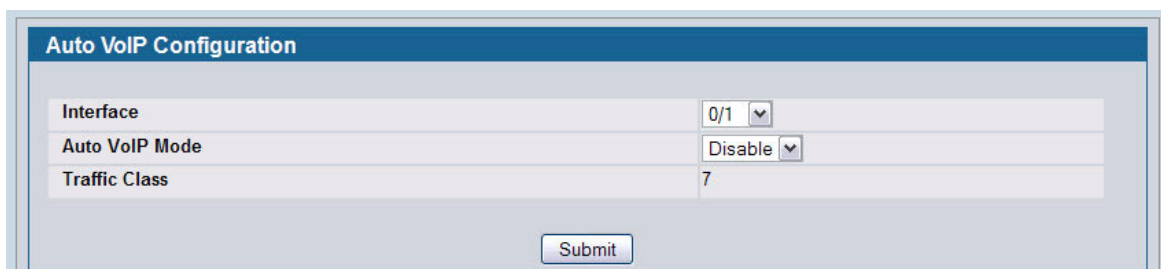
- Session Initiation Protocol (SIP)
- H.323
- Skinny Client Control Protocol (SCCP)

When a call-control protocol is detected the switch assigns the traffic in that session to the highest CoS queue, which is generally used for time-sensitive traffic.

Auto VoIP Configuration

Use the Auto VoIP Configuration page to configure the Auto VoIP settings.

To display the Auto VoIP Configuration page, click **LAN > QoS > Auto VoIP > Auto VoIP Configuration** in the navigation menu.



The screenshot shows a web interface titled "Auto VoIP Configuration". It contains three configuration fields:

Interface	0/1
Auto VoIP Mode	Disable
Traffic Class	7

At the bottom of the form is a "Submit" button.

Figure 238: Auto VoIP Configuration

Table 210: Auto VoIP Configuration Fields

Field	Description
Interface	Specifies all Auto VoIP configurable interfaces. The All option represents the most recent configuration settings done for all ports. These settings may be overridden on a per-interface basis.
Auto VoIP Mode	Use to either Enable or Disable the Auto VoIP mode. The default is Disable .
Traffic Class	Displays the traffic class used for VoIP traffic. The default value is 7.

- If you change any of the settings on the page, click **Submit** to send the updated configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a Save is performed.
- Click **Refresh** to update the page with the most current data from the switch.

Auto VoIP Summary

To display the Auto VoIP Summary page, click **LAN > Monitoring > Auto VoIP Summary** in the navigation menu.



Auto VoIP Summary		
Interface	Auto VoIP Mode	Traffic Class
0/1	Enable	7
0/2	Disable	7
0/3	Disable	7
0/4	Enable	7
0/5	Disable	7
0/6	Disable	7
0/7	Disable	7
0/8	Disable	7

Figure 239: Auto VoIP Summary

For information about the fields the page displays, see [Table 210](#).

Section 7: Configuring Access Control Lists

Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources. ACLs are used to provide traffic flow control, restrict contents of routing updates, decide which types of traffic are forwarded or blocked, and above all provide security for the network. D-Link DWS-4000 Series software supports IPv4 and MAC ACLs. The total number of MAC and IP ACLs supported by D-Link DWS-4000 Series software is 100.

The Access Control Lists folder contains links to the following folders and web pages:

- [“Configuring IP Access Control Lists”](#)
- [“MAC Access Control Lists”](#)
- [“ACL Interface Configuration”](#)

You first create an IPv4-based or MAC-based rule and assign a unique ACL ID. Then, you define the rules, which can identify protocols, source and destination IP and MAC addresses, and other packet-matching criteria. Finally, you use the ID number to assign the ACL to a port.

Configuring IP Access Control Lists

IP access control lists (ACL) allow network managers to define classification actions and rules for specific ports. ACLs are composed of access control entries (ACE), or rules, that consist of the filters that determine traffic classifications. The total number of rules that can be defined for each ACL is 12. These rules are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken, including dropping the packet or disabling the port, and the additional rules are not checked for a match. For example, a network administrator defines an ACL rule that says port number 20 can receive TCP packets. However, if a UDP packet is received the packet is dropped.

To configure an ACL:

1. Use the [“IP ACL Configuration”](#) page to define the IP ACL type and assign an ID to it.
2. Use the [“IP ACL Rule Configuration”](#) page to create rules for the ACL.
3. Use the [“ACL Interface Configuration”](#) page to assign the ACL by its ID number to a port.

IP ACL Configuration

Use the IP ACL Configuration page to add or remove IP-based ACLs. On this menu the interfaces to which an IP ACL applies must be specified, as well as whether it applies to inbound or outbound traffic. Rules for the IP ACL are specified/created using the “[IP ACL Rule Configuration](#)” page.

To display the IP ACL Configuration page, click **LAN > Access Control Lists > IP Access Control Lists > Configuration** in the navigation menu.

Table	Current Size / Max Size
ACL	3 / 100

Figure 240: IP ACL Configuration

Table 211: IP ACL Configuration Fields

Field	Description
IP ACL	Select a type of ACL to create, or select an existing ACL to delete from the dropdown menu. You can create the following types of IP ACLs: <ul style="list-style-type: none"> • Standard IP ACL: Allows you to permit or deny traffic from a source IP address. • Extended IP ACL: Allows you to permit or deny specific types of layer 3 or layer 4 traffic from a source IP address to a destination IP address. This type of ACL provides more granularity and filtering capabilities than the standard IP ACL. • Named IP ACL: Allows you to create an Extended IP ACL that is identified by a name rather than a number. These ACLs have the same capabilities as Extended IP ACLs with respect to match criteria and actions supported.
IP ACL ID	Enter an ID number for the ACL to configure. This field appears if you select Create Standard IP ACL or Create Extended IP ACL from the IP ACL dropdown menu. For a standard IP ACL, the acceptable ID values are 1-99. For an extended IP ACL, the acceptable ID values are 101-199.
IP ACL Name	This field appears if you select Create New Named IP ACL from the IP ACL dropdown menu. Specify an IP ACL Name string which includes only alphanumeric characters. The name must start with an alphabetic character. This field will display the name of the currently selected IP ACL if the ACL has already been created.

The ACL Table at the bottom of the page shows the current size of the ACL table versus the maximum size of the ACL table. The current size is equal to the number of configured IPv4 and IPv6 ACLs plus the number of configured MAC ACLs. The maximum size is 100.

- To add an IP ACL, select the type of ACL to add from the **IP ACL** menu, enter an ACL ID in the appropriate field, and then click **Submit**.
- To delete an IP ACL, select the ACL ID from the **IP ACL** menu, and then click **Delete**. The **Delete** button only appears if a configured IP ACL is selected.

IP ACL Rule Configuration

Use the **IP ACL Rule Configuration** page to define rules for IP-based ACLs created using the IP Access Control List Configuration page. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. Additionally, you can specify to assign traffic to a particular queue and/or mirror the traffic to a particular port.



Note: There is an implicit "deny all" rule at the end of an ACL list. This means that if an ACL is applied to a packet and if none of the explicit rules match, then the final implicit "deny all" rule applies and the packet is dropped.

To display the **IP ACL Rule Configuration** page, click **LAN > QoS > Access Control Lists > IP Access Control Lists > Rule Configuration** in the navigation menu.

The fields available on the page depend on whether you select a standard, extended, or named IP ACL from the IP ACL field, whether the rule action is permit or deny, and whether you select Create Rule or an existing rule from the Rule field.

Figure 241 shows the fields available when Create Rule is selected in the **Rule** field.

IP ACL Rule Configuration	
IP ACL	10
Rule	Create Rule
Rule ID	<input type="text"/> (1-127)
Action	Deny
Match Every	False
<input type="button" value="Submit"/>	

Figure 241: IP ACL Rule Configuration (Create Rule)

Figure 242 shows the fields available when you create a rule for an extended IP ACL.

The screenshot shows the 'IP ACL Rule Configuration' window. It contains the following fields and values:

Field	Value	Action
IP ACL	105	
Rule	1	
Action	Deny	Configure
Logging	False	Configure
Time Range Name		Configure
Protocol	255(IP)	Configure
Match Every	False	Configure
Source IP Address	192.168.8.1	Configure
Source IP wildcard mask	0.0.0.0	Configure
Source L4 Port	80(http/www)	Configure
Destination IP Address		Configure
Destination IP wildcard mask		Configure
Destination L4 Port		Configure
Service Type		Configure

At the bottom center of the window is a 'Delete' button.

Figure 242: IP ACL Rule Configuration (Extended ACL Rule)

Table 212 shows all possible fields on the IP ACL Rule Configuration page. The actual fields available on the page depend on what type of rule you configure, whether you create a new rule or modify an existing rule, and whether the rule action is Permit or Deny.

Table 212: IP ACL Rule Configuration Fields

Field	Description
IP ACL	The menu contains the existing IP ACLs configured on the page. To set up a new IP ACL, see “Configuring IP Access Control Lists” on page 351 .
Rule	Select an existing Rule ID to modify or select Create Rule to configure a new ACL Rule. New rules cannot be created if the maximum number of rules has been reached. For each rule, a packet must match all the specified criteria in order to be true against that rule and for the specified rule action (Permit/Deny) to take place.
Rule ID	This field is only available if you select Create Rule from the Rule field. Enter a new Rule ID which is a whole number in the range of 1 to 12 that will be used to identify the rule. After you click Submit , the new ID is created and you can configure the rule settings. The number of rules you can create in an ACL is platform dependent.
Action	Selects the ACL forwarding action. Click Configure to change the action. Select the desired action from the dropdown menu, and then click Submit or Cancel to return to the Rule Configuration page. Possible values are; <ul style="list-style-type: none"> • Permit. Forwards packets which meet the ACL criteria. • Deny. Drops packets which meet the ACL criteria.

Table 212: IP ACL Rule Configuration Fields (Cont.)

Field	Description
Logging	This field is only visible for a Deny Action. When set to True, logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule went into effect during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval.
Time Range Name	Use this field to impose a time limitation on the ACL rule. When you click Configure , you can select a configured time range or create a new named time range. To configure the time range values, use the LAN > Administration > Time Ranges > Time Range Entry Configuration page. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
Assign Queue ID	This field is only visible when the Action is Permit. Use this field to specify the hardware egress queue identifier used to handle all packets matching this AP ACL Rule. Click Configure , and then enter an identifying queue number (0 to 7) in the appropriate field. Click Submit or Cancel to return to the Rule Configuration page.
Mirror Interface	This field is only visible when the Action is Permit. Use this field to specify the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. Click Configure , and then select an interface from the dropdown list. Packets that meet the rule are mirrored on the interface you select. Click Submit or Cancel to return to the Rule Configuration page.
Match Every	Requires a packet to match the criteria of this ACL. Click Configure , and then select True or False from the dropdown list. Then click Submit or Cancel to return to the Rule Configuration page. True signifies that all packets will match the selected IP ACL and Rule and will be either permitted or denied. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen do not appear. To configure specific match criteria for the rule, remove the rule and re-create it, or reconfigure 'Match Every' to 'False' for the other match criteria to be visible.
Protocol Keyword	Specify that a packet's IP protocol is a match condition for the selected IP ACL rule. The possible values are ICMP, IGMP, IP, TCP, and UDP. Either the 'Protocol Keyword' field or the 'Protocol Number' field can be used to specify an IP protocol value as a match criteria. Click Configure , and then select the protocol keyword from the dropdown list. Click Submit or Cancel to return to the Rule Configuration page.
Protocol Number	Specify that a packet's IP protocol is a match condition for the selected IP ACL rule and identify the protocol by number. The protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255. Either the 'Protocol Number' field or the 'Protocol Keyword' field can be used to specify an IP protocol value as a match criteria.

Table 212: IP ACL Rule Configuration Fields (Cont.)

Field	Description
Source IP Address	Requires a packet's source port IP address to match the address listed here. Click Configure , and then enter an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's source IP Address. You also configure the Source IP Mask on the page.
Source IP Mask	Specifies the source IP address wildcard mask. Wild card masks determines which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all of the bits are important. Wildcard masking for ACLs operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0's) in a bit position that must be checked. A '1' in a bit position of the ACL mask indicates the corresponding bit can be ignored. This field is required when you configure a source IP address. After you enter the desired information for the Source IP Address and Source IP Mask, click Submit or Cancel to return to the Rule Configuration page.
Source L4 Port	Requires a packet's TCP/UDP source port to match the port listed here. Click Configure access the configuration page, then complete one of the following fields: <ul style="list-style-type: none"> • Source L4 Keyword: Select the desired L4 keyword from a list of source ports on which the rule can be based. If you select a keyword other than Other, the screen refreshes and the Source L4 Port Number field disappears. • Source L4 Port Number: If the source L4 keyword is Other, enter a user-defined Port ID by which packets are matched to the rule.
Destination IP Address	Requires a packet's destination port IP address to match the address listed here. Click Configure , and then enter an IP Address in the appropriate field using dotted-decimal notation. The address you enter is compared to a packet's destination IP Address. You also configure the Destination IP Mask on the page.
Destination IP Mask	Specify the IP mask in dotted-decimal notation to be used with the Destination IP Address value.
Destination L4 Port	Requires a packet's TCP/UDP destination port to match the port listed here. Click Configure access the configuration page, then complete one of the following fields: <ul style="list-style-type: none"> • Destination L4 Keyword: Select the desired L4 keyword from a list of destination ports on which the rule can be based. If you select a keyword other than Other, the screen refreshes and the Destination L4 Port Number field disappears. • Destination L4 Port Number: If the destination L4 keyword is Other, enter a user-defined Port ID by which packets are matched to the rule. The valid range is 0 to 65535.

Table 212: IP ACL Rule Configuration Fields (Cont.)

Field	Description
Service Type	<p>Select one of the following three Match conditions for the extended IP ACL rule. These are alternative ways of specifying a match condition for the same Service Type field in the IP header, however each uses a different user notation. After a selection is made, the appropriate value can be specified:</p> <ul style="list-style-type: none"> • IP DSCP: This field matches the packet DSCP value to the rule. Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 63. The IP DSCP is selected by selecting one of the DSCP keyword values from a menu. If a value is to be selected by specifying its numeric value, then select the 'Other' option in the menu and a text box will appear where you can enter the numeric value of the DSCP. • IP Precedence: The IP Precedence field in a packet is defined as the high-order three bits of the Service Type octet in the IP header. This is an optional configuration. This field matches the packet IP Precedence value to the rule when checked. Enter the IP Precedence value, an integer from 0 to 7, to match. Either the DSCP value or the IP Precedence value is used to match packets to ACLs. • IP TOS Bits: The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. Matches on the Type of Service bits in the IP header when checked. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of 0xA0 and a TOS Mask of 0xFF. This is an optional configuration. <ul style="list-style-type: none"> – TOS Bits: This value is a hexadecimal number from 00 to FF. Requires the bits in a packet's TOS field to match the two-digit hexadecimal number entered here. – TOS Mask: This value is a hexadecimal number from 00 to FF. Specifies the bit positions that are used for comparison against the IP TOS field in a packet.

Modifying an IP-based Rule



Note: Rules can be modified only when the ACL to which they belong is not bound to an interface.

1. Open the **IP ACL Rule Configuration** page.
2. Select **the desired ACL from the IP ACL menu**.
3. Select the desired rule from the **Rule ID** menu.
4. Modify the remaining fields as needed.
5. Click **Submit**.

The IP-based rule is modified, and the device is updated.

Adding a New Rule to an IP-based ACL

1. Open the **IP ACL Rule Configuration** page.
2. Select **the desired ACL from the IP ACL menu**.
3. Specify Create Rule for **Rule ID** and enter a new ID number.
4. Define the remaining fields as needed.
5. Click **Submit**.

The new rule is assigned to the specified IP-based ACL.

Deleting a Rule from an IP-based ACL

1. Open the **IP ACL Rule Configuration** page.
2. Select **the desired ACL from the IP ACL menu**.
3. Select the rule to delete from the **Rule** field.
4. Click **Delete**.

The new rule is assigned to the specified IP-based ACL.

5. Click **Refresh** to update the page with the most current information.

IP ACL Summary

Use the IP ACL Summary page to view a summary of the IP ACLs that have been configured on the switch. To access the page, click **LAN > Monitoring > Access Control Lists > IP Access Control Lists > Summary**.




IP ACL ID/Name	Rules	Direction	Interface	VLAN
10	0	In Bound	0/15	
105	1			
acl1	0			

Figure 243: IP ACL Summary

IP ACL Rule Summary

Use the IP ACL Rule Summary page to view a summary of the IP ACLs that have been configured on the switch. To access the page, click **LAN > Monitoring > Access Control Lists > IP Access Control Lists > Summary**.



IP ACL ID/Name	Rules	Direction	Interface	VLAN
10	0	In Bound	0/15	
105	1			
acl1	0			

Refresh

Figure 244: IP ACL Rule Summary

MAC Access Control Lists

A MAC ACL consists of a set of rules which are matched sequentially against a packet. When a packet meets the match criteria of a rule, the specified rule action (Permit/Deny) is taken and the additional rules are not checked for a match. On this menu the interfaces to which an MAC ACL applies must be specified. Rules for the MAC ACL are specified/created using the MAC ACL Rule Configuration menu.

To configure a MAC ACL:

1. Use the [“MAC ACL Configuration”](#) page to define the ACL type and assign an ID to it.
2. Use the [“MAC ACL Rule Configuration”](#) page to create rules for the ACL.
3. Use the [“ACL Interface Configuration”](#) to assign the ACL by its ID number to a port or VLAN.

MAC ACL Configuration

The MAC ACL Configuration page allows network administrators to define a MAC-based ACL.

To display the MAC ACL Configuration page, click **LAN > QoS > Access Control Lists > MAC Access Control Lists > Configuration** in the navigation tree.

Figure 245: MAC ACL Configuration

Table 213: MAC ACL Configuration Fields

Field	Description
MAC ACL	The options in the dropdown menu allow you to create a new MAC ACL or select an existing MAC ACL that you want to rename.
MAC ACL Name	Enter a name for the MAC ACL. The name string may include alphabetic, numeric, dash, underscore, or space characters only. The name must start with an alphabetic character. This field displays the name of the currently selected MAC ACL if the ACL has already been created.

The ACL Table at the bottom of the page shows the current size of the ACL table versus the maximum size of the ACL table. The current size is equal to the number of configured IPv4 ACLs plus the number of configured MAC ACLs. The maximum size is 100.

- To add a MAC ACL, select **Create New Extended MAC ACL** from the **MAC ACL** menu, enter a name for the ACL in the appropriate field, and then click **Submit**.
- To rename a MAC ACL, select the ACL name from the **MAC ACL** menu. Enter a new name for the ACL in the appropriate field, and then click **Rename**. The **Rename** button only appears if a configured MAC ACL is selected.
- To delete a MAC ACL, select the ACL name from the **MAC ACL** menu, and then click **Delete**. The **Delete** button only appears if a configured MAC ACL is selected.

MAC ACL Rule Configuration

Use the MAC ACL Rule Configuration page to define rules for MAC-based ACLs. The access list definition includes rules that specify whether traffic matching the criteria is forwarded normally or discarded. A default 'deny all' rule is the last rule of every list.

To display the MAC ACL Rule Configuration page, click **LAN > QoS > Access Control Lists > MAC Access Control Lists > Rule Configuration** in the navigation menu.

The fields available on the page depend on whether the rule action is permit or deny, and whether you select **Create Rule** or an existing rule from the **Rule** field.

Figure 246 shows the fields available when Create New Rule is selected in the **Rule** field.

The screenshot shows the 'MAC ACL Rule Configuration' form with the following fields and values:

MAC ACL	mac-acl1
Rule	Create New Rule
Rule ID	(1 to 12)
Action	Deny
Match Every	False

A 'Submit' button is located at the bottom of the form.

Figure 246: MAC ACL Rule Configuration (Create Rule)

Figure 247 shows the fields available when you configure a MAC ACL rule with a Deny action.

The screenshot shows the 'MAC ACL Rule Configuration' form with the following fields and values:

MAC ACL Name	mac-acl1	
Rule	2	
Action	Deny	Configure
Logging	False	Configure
Time Range Name		Configure
Match Every	False	Configure
CoS		Configure
Destination MAC		Configure
Destination MAC Mask		Configure
Ethertype Key		Configure
Source MAC		Configure
Source MAC Mask		Configure
VLAN		Configure

A 'Delete' button is located at the bottom of the form.

Figure 247: MAC ACL Rule Configuration (Deny Action)

Figure 248 shows the fields available when you create a rule for a MAC ACL.

The screenshot shows the 'MAC ACL Rule Configuration' window. It contains a table of fields with their current values and 'Configure' buttons for each. At the bottom, there is a 'Delete' button.

Field	Value	Action
MAC ACL Name	mac-ac1	
Rule	3	
Action	Permit	Configure
Time Range Name		Configure
Assign Queue ID		Configure
Mirror Interface		Configure
Match Every	False	Configure
CoS		Configure
Destination MAC		Configure
Destination MAC Mask		Configure
Ethertype Key		Configure
Source MAC		Configure
Source MAC Mask		Configure
VLAN		Configure

Delete

Figure 248: MAC ACL Rule Configuration (Permit Action)

Table 214 shows all possible fields on the MAC ACL Rule Configuration page. The actual fields available on the page depend on whether you create a new rule or modify an existing rule, and whether the rule action is Permit or Deny.

Table 214: MAC ACL Rule Configuration Fields

Field	Description
MAC ACL	Specifies an existing MAC ACL. To set up a new MAC ACL use the “ MAC Access Control Lists ” page.
Rule	Select an existing Rule ID to modify or select Create Rule to configure a new ACL Rule. Enter a whole number in the range of 1 to 12 that will be used to identify the rule. New rules cannot be created if the maximum number of rules has been reached. For each rule, a packet must match all the specified criteria in order to be true against that rule and for the specified rule action (Permit/Deny) to take place.
Rule ID	This field is only available if you select Create Rule from the Rule field. Enter a new Rule ID. After you click Submit , the new ID is created and you can configure the rule settings. You can create up to 12 rules for each ACL.
Action	Specify what action should be taken if a packet matches the rule's criteria: <ul style="list-style-type: none"> • Permit: Forwards packets that meet the ACL criteria. • Deny: Drops packets that meet the ACL criteria.

Table 214: MAC ACL Rule Configuration Fields (Cont.)

Field	Description
Logging	This field is only visible for a Deny Action. When set to True, logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule went into effect during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval.
Time Range Name	Use this field to impose a time limitation on the ACL rule. When you click Configure , you can select a configured time range or create a new named time range. To configure the time range values, use the LAN > Administration > Time Ranges > Time Range Entry Configuration page. If a time range with the specified name does not exist and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.
Assign Queue ID	This field is only visible when the Action is Permit. Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Click Configure , and then enter an identifying number from 0 to 6 in the appropriate field. Click Submit or Cancel to return to the Rule Configuration page.
Match Every	Requires a packet to match the criteria of this ACL. Click Configure , and then select True or False from the dropdown list. Then click Submit or Cancel to return to the Rule Configuration page. Match Every is exclusive to the other filtering rules, so if Match Every is True, the other rules on the screen do not appear. False indicates that it is not mandatory for every packet to match the selected ACL Rule.
Mirror Interface	This field is only visible when the Action is Permit. Specifies the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device.
CoS	Specifies the 802.1p user priority to compare against an Ethernet frame. Requires a packet's class of service (CoS) to match the CoS value listed here. Click Configure , and then enter a CoS value between 0 and 7 to apply this criteria. Click Submit or Cancel to return to the Rule Configuration page.
Destination MAC Address	Requires an Ethernet frame's destination port MAC address to match the address listed here. Click Configure , and then enter a MAC address in the appropriate field. The valid format is xx_xx_xx_xx_xx_xx. The BPDU keyword may be specified using a Destination MAC Address of 01:80:C2:xx:xx:xx. Click Submit or Cancel to return to the Rule Configuration page.
Destination MAC Mask	If desired, enter the MAC Mask associated with the Destination MAC to match. The MAC address mask specifies which bits in the destination MAC to compare against an Ethernet frame. Use F's and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. For example, if the MAC address is aa_bb_cc_dd_ee_ff, and the mask is 00_00_ff_ff_ff_ff, all MAC addresses with aa_bb_xx_xx_xx_xx result in a match (where x is any hexadecimal number). Click Submit or Cancel to return to the Rule Configuration page.

Table 214: MAC ACL Rule Configuration Fields (Cont.)

Field	Description
EtherType Key	Requires a packet's EtherType to match the EtherType you select. Click Configure , and then select the EtherType value from the dropdown menu. If you select User Value, you can enter a custom EtherType value.
Ethertype User Value	This field only appears if you select User Value from the EtherType dropdown list. The value you enter specifies a customized EtherType to compare against an Ethernet frame. The valid range of values is (0x0600 to 0xFFFF).
Source MAC Address	Requires a packet's source port MAC address to match the address listed here. Click Configure , and then enter a MAC address in the appropriate field. The valid format is xx:xx:xx:xx:xx:xx.
Source MAC Mask	If desired, enter the MAC mask for the source MAC address to match. Use F's and zeros in the MAC mask, which is in a wildcard format. An F means that the bit is not checked, and a zero in a bit position means that the data must equal the value given for that bit. The valid format is xx:xx:xx:xx:xx:xx. Click Submit or Cancel to return to the Rule Configuration page.
VLAN	Requires a packet's VLAN ID to match the ID listed here. Click Configure , and then enter the VLAN ID to apply this criteria. The valid range is 1–3965. Either VLAN Range or VLAN can be configured. Click Submit or Cancel to return to the Rule Configuration page.

Adding a New Rule to a MAC-based ACL

Once you configure a MAC ACL, you can add rules to the ACL.

1. Open the **MAC ACL Rule Configuration** page.
2. If more than one MAC ACL is configured on the system, select the desired ACL from the MAC ACL menu.
3. From the **Rule** menu, select Create New Rule.
4. Enter a new ID number for the rule.
5. Configure the remaining rule criteria as needed.
6. Click **Submit**.

The new rule is assigned to the specified MAC-based ACL.


Removing a Rule From a MAC-based ACL

1. From the **MAC ACL Rule Configuration** page, select an ACL from the **MAC ACL** field.
2. Select a rule from the **Rule** menu.
3. Click **Delete**.

The rule is removed from the MAC-based ACL, and the device is updated.

MAC ACL Summary

Use the MAC ACL Summary page to view a summary of the MAC ACLs that have been configured on the switch. To access the page, click **LAN > Monitoring > Access Control Lists > MAC Access Control Lists > Summary**.

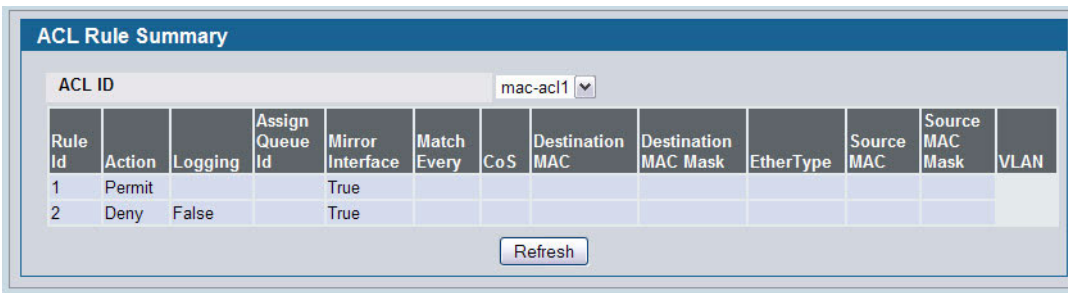


MAC ACL Name	Rules	Direction	Interface	VLAN
mac-acl1	2	In Bound	0/16	

Figure 249: MAC ACL Summary

MAC ACL Rule Summary

Use the MAC ACL Rule Summary page to view a summary of the MAC ACLs that have been configured on the switch. To access the page, click **LAN > Monitoring > Access Control Lists > MAC Access Control Lists > Summary**.



ACL ID: mac-acl1

Rule Id	Action	Logging	Assign Queue Id	Mirror Interface	Match Every	CoS	Destination MAC	Destination MAC Mask	EtherType	Source MAC	Source MAC Mask	VLAN
1	Permit			True								
2	Deny	False		True								

Figure 250: MAC ACL Rule Summary

ACL Interface Configuration

When an ACL is bound to an interface, all the rules that have been defined are applied to the selected interface. Use the ACL Interface Configuration page to assign ACLs and Interfaces and prioritize the ACLs that are bound to each interface. To display the ACL Interface Configuration page, click **LAN > QoS > Access Control Lists > Interface Configuration** in the navigation menu.

Figure 251: ACL Interface Configuration

If an ACL has been assigned to the interface, it displays in the table at the bottom of the page.

Table 215: ACL Interface Configuration Fields

Field	Description
Interface	Select the interface or LAG from the menu.
Direction	Specifies the packet filtering direction for the ACL. The system supports Inbound filtering. inbound filtering means the system applies the ACL rules to packets as they enter the interface.
ACL Type	Use the menu to select the ACL type to which incoming packets are matched. Packets can be matched to IP- or MAC-based ACLs.
IP/MAC ACL	Select the ACL of the specified type to apply to the interface from the dropdown menu.
Sequence Number	Assigns the priority of this ACL. If more than one ACL is applied to an interface, then the match criteria for the highest sequence ACLs are checked first. A lower number indicates higher priority. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If you do not specify a sequence number, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. The valid range is 1-4294967295.

Assigning an ACL to an Interface

1. Open the **ACL Interface Configuration** page.
2. Select the interface from the Slot/Port field to which you want to bind the ACL.
3. Select the type of ACL in the **ACL Type** field.
4. Select the ACL ID or name to bind to the interface.



Note: Whenever an ACL is assigned on a port or LAG, flows from that ingress interface that do not match the ACL are matched to the default rule, which is Drop unmatched packets.

5. Specify the priority in the **Sequence** field.
6. Click **Submit**.
The ACL is attached to the specified interface(s).

Removing an ACL from an Interface

If an ACL is bound to an interface, the **Remove** button appears on the page when you select the interface from the Slot/Port menu. To remove the ACL from the interface, select the type of ACL to remove and its ID or name, and then click **Remove**.

Section 8: Managing Device Security

Use the features in the Security folder on the navigation tree menu to set management security parameters for port, user, and server security.

The Security folder contains links to the following features:

- [“Configuring Port Security”](#)
- [“SSL/Secure HTTP Configuration”](#)
- [“Secure Shell \(SSH\) Configuration”](#)
- [“Configuring Port Security”](#)
- [“RADIUS Settings”](#)
- [“Port Access Control”](#)
- [“TACACS+ Settings”](#)

Configuring Port Security

Port Security can be enabled on a per-port basis. When a port is locked, only packets with allowable source MAC addresses can be forwarded. All other packets are discarded. A MAC address can be defined as allowable by one of two methods: dynamically or statically. Note that both methods are used concurrently when a port is locked.

Dynamic locking implements a “first arrival” mechanism for Port Security. You specify how many addresses can be learned on the locked port. If the limit has not been reached, then a packet with an unknown source MAC address is learned and forwarded normally. Once the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. Note that you can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.

Static locking allows you to specify a list of MAC addresses that are allowed on a port. The behavior of packets is the same as for dynamic locking: only packets with an allowable source MAC address can be forwarded.

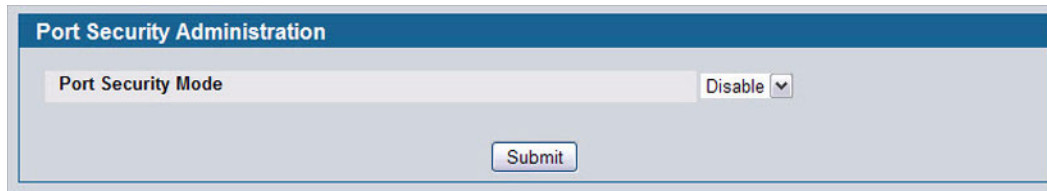
To see the MAC addresses learned on a specific port, see [“Configuring and Searching the Forwarding Database” on page 178](#).

Disabled ports can only be activated from the **Configuring Ports** page.

Port Security Administration

Use the Port Security Administration page to enable or disable the port security feature on your switch.

To access the Port Security Administration page, click **LAN > Security > Port Security Administration** in the navigation tree.



Port Security Administration	
Port Security Mode	Disable ▾
<input type="button" value="Submit"/>	

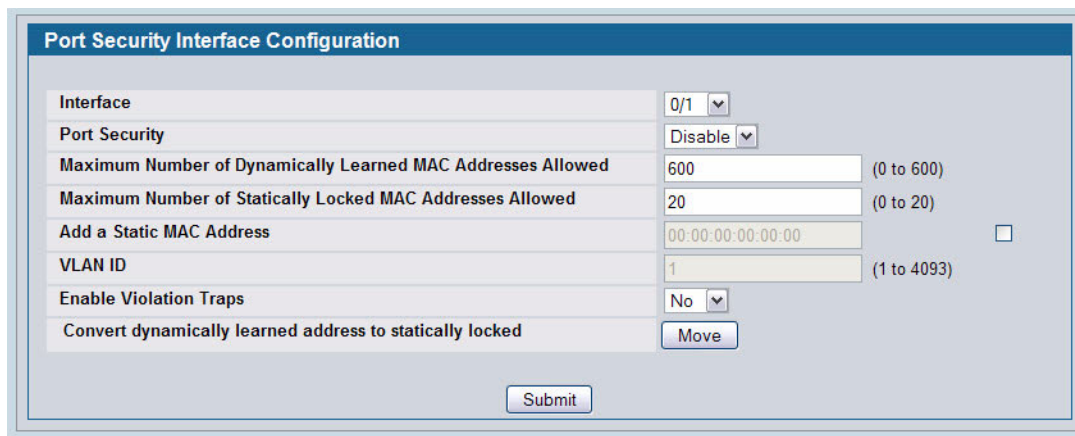
Figure 252: Port Security Administration

- Select **Enable** or **Disable** from the **Port Security Mode** list and click **Submit**.

Port Security Interface Configuration

Use this page to configure the port security feature on a selected interface.

To access the Port Security Interface Configuration page, click **LAN > Security > Port Security Interface** in the navigation tree.



Port Security Interface Configuration	
Interface	0/1 ▾
Port Security	Disable ▾
Maximum Number of Dynamically Learned MAC Addresses Allowed	600 (0 to 600)
Maximum Number of Statically Locked MAC Addresses Allowed	20 (0 to 20)
Add a Static MAC Address	00:00:00:00:00:00 <input type="checkbox"/>
VLAN ID	1 (1 to 4093)
Enable Violation Traps	No ▾
Convert dynamically learned address to statically locked	<input type="button" value="Move"/>
<input type="button" value="Submit"/>	

Figure 253: Port Security Interface Configuration

Table 216: Port Security Interface Configuration Fields

Field	Description
Interface	Select the physical interface or the LAG on which to configure port security information.
Port Security	Determines whether port security is enabled. The default mode is Disable. <ul style="list-style-type: none"> • Enable: Locks the port so that only packets with allowable source MAC addresses can be forwarded. All other packets are discarded. • Disable: The port is not locked, so no port security restrictions are applied.
Maximum Number of Dynamically Learned MAC Addresses Allowed	Sets the maximum number of dynamically learned MAC addresses on the selected interface. Once the limit is reached, no more addresses are learned on the port. Any packets with source MAC addresses that were not already learned are discarded. You can effectively disable dynamic locking by setting the number of allowable dynamic entries to zero.
Maximum Number of Statically Locked MAC Addresses Allowed	Sets the maximum number of statically locked MAC addresses on the selected interface.
Add a Static MAC Address	Adds a MAC address to the list of statically locked MAC addresses for the selected interface. Only packets with an allowable source MAC address can be forwarded.
VLAN ID	Adds a corresponding VLAN ID for the MAC Address being added to the list of statically locked MAC addresses for the selected interface.
Enable Violation Traps	Enables or disables the sending of new violation traps designating when a packet with a disallowed MAC address is received on a locked port. Value is No by default.
Convert dynamically learned address to static locked	When you click Move , all the dynamically learned entries on this interface are added to the static MAC address list for this interface. After moving them, you can view them in the Port Security Static page.

- If you make any changes to the page, click **Submit** to apply the new settings to the system.

Port Security Static

Use the Port Security Static page to view static MAC addresses configured on an interface.

To access the Port Security Static page, click **LAN > Security > Port Security Static** in the navigation tree.

Figure 254: Port Security Static

Table 217: Port Security Static Fields

Field	Description
Interface	Select the physical interface or the LAG on which to view the dynamically learned MAC addresses.
MAC Address	This column lists the static MAC addresses, if any, configured on the selected port.
VLAN ID	Displays the VLAN ID corresponding to the statically configured MAC address.
Delete a static MAC Address	Enter the address of the statically configured MAC address to delete. All MAC addresses that are available to be deleted appear in the MAC Address – VLAN ID table.
VLAN ID	Enter the VLAN ID that corresponds to the statically configured MAC address to delete.

- After you enter the MAC address and VLAN ID of the statically configured MAC address to delete, click **Submit** to remove the MAC address from the port and apply the new settings to the system. The screen refreshes, and the MAC address no longer appears in the table on the page.

Port Security Dynamic

Use the Port Security Dynamic page to view a table with the dynamically learned MAC addresses on an interface. With dynamic locking, MAC addresses are learned on a “first arrival” basis. You specify how many addresses can be learned on the locked port.

To access the Port Security Dynamic page, click **LAN > Monitoring > Port Security > Port Security Dynamic** in the navigation tree.

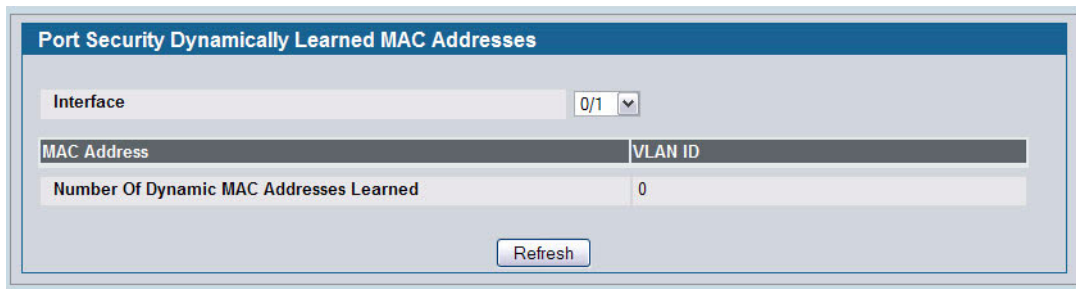


Figure 255: Port Security Dynamic

Table 218: Port Security Dynamic Fields

Field	Description
Interface	Select the physical interface or the LAG on which to view the dynamically learned MAC addresses.
MAC Address	This column lists the dynamically learned MAC addresses, if any, on the selected port.
VLAN ID	Displays the VLAN ID corresponding to the dynamically learned MAC address.

Port Security Violation Status

Use the Port Security Violation Status page to enable or disable the port security feature on your switch.

To access the Port Security Violation Status page, click **LAN > Monitoring > Port Security > Port Security Violation** in the navigation tree.

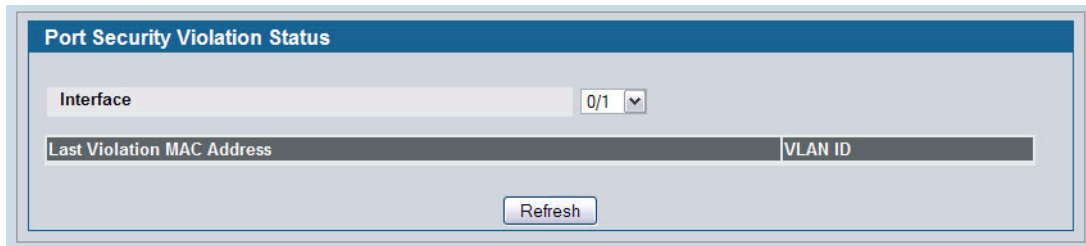


Figure 256: Port Security Violation Status

Table 219: Port Security Violation Status Fields

Field	Description
Interface	Select the physical interface or the LAG on which to view security violation information.
Last Violation MAC Address	Displays the source MAC address of the last packet that was discarded at a locked port.
VLAN ID	Displays the VLAN ID corresponding to the Last Violation MAC address.

SSL/Secure HTTP Configuration

Secure HTTP enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. When you manage the switch by using a Web interface, secure HTTP can help ensure that communication between the management system and the switch is protected from eavesdroppers and man-in-the-middle attacks.

Use the Secure HTTP Configuration page to configure the settings for HTTPS communication between the management station and the switch.

To display the Secure HTTP Configuration page, click **LAN > Security > SSL Configuration** in the navigation menu.

Secure HTTP Configuration	
HTTPS Admin Mode	Disable
TLS Version 1	Enable
SSL Version 3	Enable
HTTPS Port	443 (1 to 65535)
HTTPS Session Soft Timeout (Minutes)	5 (1 to 60)
HTTPS Session Hard Timeout (Hours)	24 (1 to 168)
Maximum Number of HTTPS Sessions	16 (0 to 16)
Certificate Present?	True
Certificate Generation Status	No certificate generation in progress

Buttons: Delete Certificate, Refresh, Download Certificates, Generate Certificate, Submit

Figure 257: Secure HTTP Configuration

Table 220: Secure HTTP Configuration Fields

Field	Description
Admin Mode	Enables or Disables the Administrative Mode of Secure HTTP. The currently configured value is shown when the web page is displayed. The default value is Disable. You can only download SSL certificates when the HTTPS Admin mode is disabled.
TLS Version 1	Enables or Disables Transport Layer Security Version 1.0. The currently configured value is shown when the web page is displayed. The default value is Enable.
SSL Version 3	Enables or Disables Secure Sockets Layer Version 3.0. The currently configured value is shown when the web page is displayed. The default value is Enable.
HTTPS Port	Sets the HTTPS Port Number. The value must be in the range of 1 to 65535. Port 443 is the default value. The currently configured value is shown when the web page is displayed.
HTTPS Session Soft Timeout	Sets the inactivity timeout for HTTPS sessions. The value must be in the range of (1 to 60) minutes. The default value is 5 minutes. The currently configured value is shown when the web page is displayed.

Table 220: Secure HTTP Configuration Fields (Cont.)

Field	Description
HTTPS Session Hard Timeout	Sets the hard timeout for HTTPS sessions. This timeout is unaffected by the activity level of the session. The value must be in the range of (1 to 168) hours. The default value is 24 hours. The currently configured value is shown when the web page is displayed.
Maximum Number of HTTPS Sessions	Sets the maximum allowable number of HTTPS sessions. The value must be in the range of (0 to 16). The default value is 16. The currently configured value is shown when the web page is displayed.

For the Web server on the switch to accept HTTPS connections from a management station, the Web server needs a public key certificate. The DWS-4000 Series switch has a self-generated certificate installed on it by default. The switch can also generate its own certificates, or you can generate these externally (i.e., off-line) and download them to the switch.

Generating Certificates

To have the switch generate the certificates:

1. Click **Generate Certificate**.

The page refreshes with the message “Certificate generation in progress”.

2. Click **Submit** to complete the process.

The page refreshes with the message “No certificate generation in progress” and the Certificate Present field displays as “True”.

Downloading SSL Certificates

Before you download a file to the switch, the following conditions must be true:

- The file to download from the TFTP server is on the server in the appropriate directory.
- The file is in the correct format.
- The switch has a path to the TFTP server.

Use the following procedures to download an SSL certificate.

1. Click the **Download Certificates** button at the bottom of the page.



Note: The **Download Certificates** button is only available if the HTTPS admin mode is disabled. If the mode is enabled, disable it and click Submit. When the page refreshes, the **Download Certificates** button appears.

The **Download Certificates** button links to the **File Download** page, as [Figure 258 on page 376](#) shows.

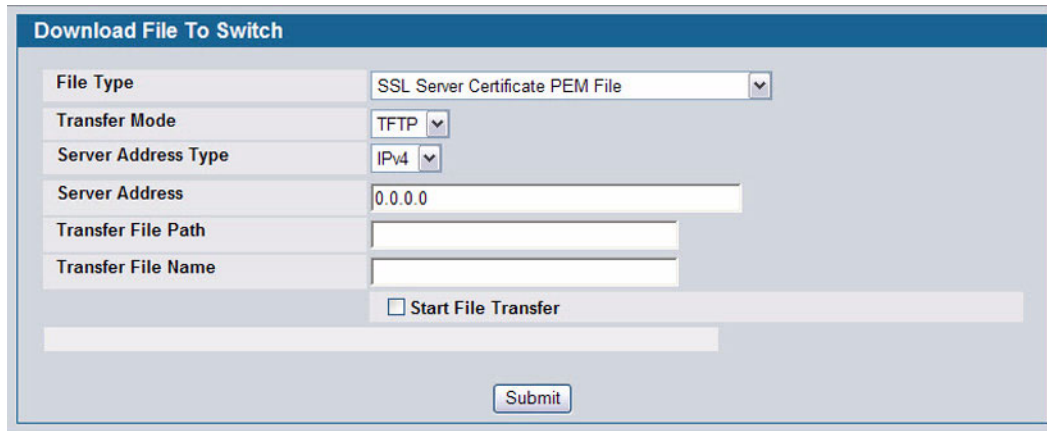


Figure 258: File Download

2. From the **File Type** field on the File Download page, select one of the following types of SSL files to download:
 - SSL Trusted Root Certificate PEM File: SSL Trusted Root Certificate File (PEM Encoded).
 - SSL Server Certificate PEM File: SSL Server Certificate File (PEM Encoded).
 - SSL DH Weak Encryption Parameter PEM File: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded).
 - SSL DH Strong Encryption Parameter PEM File: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded).
3. Verify the IP address of the TFTP server and ensure that the software image or other file to be downloaded is available on the TFTP server.
4. Complete the **TFTP Server IP Address** and **TFTP File Name** (full path without TFTP server IP address) fields.
5. Select the **Start File Transfer** check box, and then click **Submit**.

After you click Submit, the screen refreshes and a “File transfer operation started” message appears. After the software is downloaded to the device, a message appears indicating that the file transfer operation completed successfully.
6. To return to the Secure HTTP Configuration page, click **LAN > Security > SSL Configuration** in the navigation menu.
7. To enable the HTTPS admin mode, select Enable from the **HTTPS Admin Mode** field, and then click **Submit**.

Secure Shell (SSH) Configuration

If you use the command-line interface (CLI) to manage the switch from a remote system, you can use Secure Shell (SSH) to establish a secure connection. SSH uses public-key cryptography to authenticate the remote computer.

Secure Shell Configuration

Use the Secure Shell Configuration page to configure the settings for secure command-line based communication between the management station and the switch.

To display the Secure Shell Configuration page, click **LAN > Security > Secure Shell > SSH Configuration** in the navigation menu.

Secure Shell Configuration	
Admin Mode	Disable
SSH Version 1	Enable
SSH Version 2	Enable
SSH Connections Currently in Use	0
Maximum number of SSH Sessions Allowed	5
SSH Session Timeout (minutes)	5
Keys Present	
Key Generation Status	No key generation in progress
<input type="button" value="Refresh"/> <input type="button" value="Download Host Keys"/> <input type="button" value="Generate RSA Keys"/> <input type="button" value="Generate DSA Key"/> <input type="button" value="Submit"/>	

Figure 259: Secure Shell Configuration

Table 221: Secure Shell Configuration Fields

Field	Description
Admin Mode	This select field is used to Enable or Disable the administrative mode of SSH. The currently configured value is shown when the web page is displayed. The default value is Disable.
SSH Version 1	This select field is used to Enable or Disable Protocol Level 1 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.
SSH Version 2	This select field is used to Enable or Disable Protocol Level 2 for SSH. The currently configured value is shown when the web page is displayed. The default value is Enable.
SSH Connections in Use	Displays the number of SSH connections currently in use in the system.
Maximum Number of SSH Sessions Allowed	This select field is used to configure the maximum number of inbound SSH sessions allowed on the switch. The currently configured value is shown when the web page is displayed. The range of acceptable values for this field is (0-5).

Table 221: Secure Shell Configuration Fields (Cont.)

Field	Description
SSH Session Timeout (Minutes)	This text field is used to configure the inactivity timeout value for incoming SSH sessions to the switch. The acceptable range for this value is (1-160) minutes.
Keys Present	Displays which keys: RSA, DSA, or both are present (if any).
Key Generation Status	Displays which keys: RSA or DSA, are being generated.

- Click **Refresh** to update the current page with the most current settings and status.
- Click **Download Host Keys** to link to the File Transfer page for the Host Key download. Note that to download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.
- Click **Generate RSA Host Keys** to begin generating the RSA host keys. Note that to generate SSH key files, SSH must be administratively disabled and there can be no active SSH session.
- Click **Generate DSA Host Key** to begin generating the DSA host key. Note that to generate SSH key files, SSH must be administratively disabled and there can be no active SSH session.
- Click **Delete** to delete the corresponding key file (RSA or DSA), if it is present.
- If you make changes to the page, click **Submit** to apply the changes to the system.

Downloading SSH Host Keys

For the switch to accept SSH connections from a management station, the switch needs SSH host keys or certificates. The switch can generate its own keys or certificates, or you can generate these externally (i.e., off-line) and download them to the switch.

To download an SSH host key from a TFTP server to the switch, use the instructions in [“Downloading SSL Certificates” on page 375](#). However, from the File Type field on the File Download page, select one of the following key file types to download:

- **SSH-1 RSA Key File:** SSH-1 Rivest-Shamir-Adleman (RSA) Key File.
- **SSH-2 RSA Key PEM File:** SSH-2 Rivest-Shamir-Adleman (RSA) Key File (PEM Encoded).
- **SSH-2 DSA Key PEM File:** SSH-2 Digital Signature Algorithm (DSA) Key File (PEM Encoded).

Captive Portal Configuration

The Captive Portal (CP) feature allows you to block both wired and wireless clients from accessing the network until user verification has been established. You can configure CP verification to allow access for both guest and authenticated users. Authenticated users must be validated against a database of authorized Captive Portal users before access is granted. The database can be stored locally on the switch or on a RADIUS server.

The Captive Portal folder contains links to the following pages that help you view and configure system Captive Portal settings:

- [“Captive Portal Global Configuration”](#)
- [“CP Configuration”](#)
- [“Local User”](#)
- [“Interface Association”](#)
- [“CP Global Status”](#)
- [“Interface Status”](#)
- [“Client Connection Status”](#)
- [“SNMP Trap Configuration”](#)

Captive Portal Global Configuration

From the CP **Global Configuration** page, you can control the administrative state of the CP feature and configure global settings that affect all captive portals configured on the switch.

To configure the global CP settings, click **LAN > Security > Captive Portal > Global Configuration**.



Note: Note that the same Captive Portal folder is accessible from the LAN tab as well as the WLAN tab in the navigation tree. The global configuration items are applicable to Wired CP as well as Wireless CP regardless of where you access the CP folder from.

Global Configuration	
Enable Captive Portal	<input type="checkbox"/>
CP Global Operational Status	Disabled
CP Global Disable Reason	Administrator Disabled
Additional HTTP Port	<input type="text" value="0"/> (0 to 65535, 0 - Disable)
Additional HTTP Secure Port	<input type="text" value="0"/> (0 to 65535, 0 - Disable)
Peer Switch Statistics Reporting Interval (secs)	<input type="text" value="120"/> (15 to 3600, 0 - Disable)
Authentication Timeout (secs)	<input type="text" value="300"/> (60 to 600)
<input type="button" value="Submit"/> <input type="button" value="Refresh"/>	

Figure 260: Captive Portal Global Configuration

The following table describes the global CP fields you can view or configure.

Table 222: Captive Portal Global Configuration

Field	Description
Enable Captive Portal	Select the check box to enable the CP feature on the switch. Clear the check box to disable the captive portal feature.
CP Global Operational Status	Shows whether the CP feature is enabled.
CP Global Disable Reason	If CP is disabled, this field displays the reason, which can be one of the following: <ul style="list-style-type: none"> • None • Administratively Disabled • No IPv4 Address • Routing Enabled, but no IPv4 routing interface
Additional HTTP Port	HTTP traffic uses port 80, but you can configure an additional port for HTTP traffic. Enter a port number between 0-65535 (excluding ports 80, 443, and the configured switch management secure port).
Additional HTTP Secure Port	HTTP traffic over SSL (HTTPS) uses port 443, but you can configure an additional port for HTTPS traffic. Enter a port number between 0-65535 (excluding ports 80, 443, and the configured switch management secure port).
Peer Switch Statistics Reporting Interval	When clustering is supported on the switch, enter a value to determine how often the switch sends its authenticated client statistics to the Cluster Controller. The interval is in seconds. Enter a value of 0 to prevent the switch from reporting the statistics.
Authentication Timeout	To access the network through a portal, the wireless client must first enter authentication information on an authentication Web page. Enter the number of seconds to keep the authentication session open with the client. When the timeout expires, the switch disconnects any active TCP or SSL connection with the client.

CP Configuration

From the CP Configuration page, you can view summary information about captive portals on the system, add a captive portal, and configure existing captive portals.

Use the **CP Summary** page to create or delete captive portal configurations. The switch supports 10 CP configurations. CP configuration 1 is created by default and can not be deleted. Each captive portal configuration can have unique guest or group access modes and a customized acceptance use policy that displays when the client connects.

To view summary information about existing captive portals, or to add or delete a captive portal, click **LAN > Security > Captive Portal > CP Configuration**.

Configuration	Mode	Protocol	Verification	Languages
<input type="checkbox"/> 1-Default	Enable	HTTP	Local	1
<input type="checkbox"/> 2-CP-config	Enable	HTTP	Guest	1
<input type="checkbox"/> 3-CP-radius	Enable	HTTP	RADIUS	1

Figure 261: Captive Portal Summary

To create a CP configuration, enter the configuration name in the text box and click **Add**. After you add the configuration, the CP Configuration page for that configuration appears and a new tab with the name of that configuration is created.

To delete an existing CP, select the check box for the CP to remove, and then click **Delete**.

To configure the settings for an existing CP, click the name in the Configuration column or click the appropriate tab.



Note: In this document, the names captive portal or CP or portal are sometimes used in place of CP Configuration.

Table 223 describes the fields on the **CP Summary** page.

Table 223: Captive Portal Summary

Field	Description
Configuration	Shows the captive portal ID and name. To access the configuration page for an exiting CP, click the configuration name.
Mode	Shows whether the CP is enabled.

Table 223: Captive Portal Summary (Cont.)

Field	Description
Protocol	Indicates whether the portal uses HTTP or HTTPS.
Verification	Specifies which type of user verification to perform: <ul style="list-style-type: none"> • Guest: The user does not need to be authenticated by a database. • Local: The switch uses a local database to authenticated users. • RADIUS: The switch uses a database on a remote RADIUS server to authenticate users. To configure authorized users on the local or remote RADIUS database, see “Local User” on page 390 .
Languages	Shows the number of languages that are configured for this captive portal.

Changing the Captive Portal Settings

By default, the switch has one captive portal. You can change the settings for that captive portal, and you can also create and configure up to nine additional portals. After you create a captive portal from the **CP Summary** page, you can change its settings.

The screenshot displays the 'CP Configuration' page in a web browser. At the top, there are tabs for 'CP Summary', 'Default', 'CP-config', and 'CP-radius'. Below these, there are sub-tabs for 'CP Configuration' and '(English)'. The main content area is titled 'CP Configuration' and contains the following settings:

- Enable Captive Portal:**
- Configuration Name:** CP-config
- Protocol Mode:** HTTP HTTPS
- Verification Mode:** Guest Local RADIUS
- User Logout Mode:**
- Enable Redirect Mode:**
- Redirect URL:** [Empty field]
- RADIUS Auth Server:** Default-RADIUS-Server
- User Group:** 1-Default

On the right side, there are several rate and timeout settings, all set to 0 (unlimited):

- Idle Timeout (secs):** 0 (0 to 900)
- Session Timeout (secs):** 0 (0 to 86400)
- Max Up Rate (bytes/sec):** 0 (0 = unlimited)
- Max Down Rate (bytes/sec):** 0 (0 = unlimited)
- Max Receive (bytes):** 0 (0 = unlimited)
- Max Transmit (bytes):** 0 (0 = unlimited)
- Max Total (bytes):** 0 (0 = unlimited)

At the bottom, there is a table for configuring languages:

Code	Language
en	(English)

Buttons for 'Add', 'Delete', 'Modify', 'Clear', 'Delete', 'Submit', and 'Refresh' are located at the bottom of the configuration area.

Figure 262: Captive Portal Configuration

Table 224 describes the fields on the **CP Configuration** page.

Table 224: CP Configuration

Field	Description
Enable Captive Portal	Select the check box to enable the CP. Clear the check box to disable it.
Configuration Name	This field allows you to change the name of the portal added from the CP Summary page.
Protocol Mode	Choose whether to use HTTP or HTTPS as the protocol for the portal to use during the verification process. <ul style="list-style-type: none"> • HTTP: Does not use encryption during verification • HTTPS: Uses the Secure Sockets Layer (SSL), which requires a certificate to provide encryption. The certificate is presented to the user at connection time.
Verification Mode	Select the mode for the CP to use to verify clients: <ul style="list-style-type: none"> • Guest: The user does not need to be authenticated by a database. • Local: The switch uses a local database to authenticated users. • RADIUS: The switch uses a database on a remote RADIUS server to authenticate users.
User Logout Mode	Select this option to allow an authenticated client to deauthenticate from the network. If this option is clear or the user does not specifically request logout, the client connection status remains <i>authenticated</i> until the CP deauthenticates the user, for example by reaching the idle timeout or session timeout values.
Enable Redirect Mode	Select this option to specify that the CP should redirect the newly authenticated client to the configured URL. If this option is clear, the user sees the locale-specific welcome page after a successful verification.
Redirect URL	Specify the URL to which the newly authenticated client is redirected if the URL Redirect Mode is enabled.
RADIUS Auth Server	If the verification mode is RADIUS, click the ... button and select the name of the RADIUS server used for client authentications. The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the clients. To configure RADIUS server information, go to LAN > Security > RADIUS > RADIUS Authentication Server Configuration .
Idle Timeout	Enter the number of seconds a user can remain idle before automatically being logged out. If the value is set to 0 then the timeout is not enforced. The default value is 0. Note: The idle time cannot be enforced in this release for a Wired Captive Portal client due to hardware limitations.
Session Timeout	Enter the number of seconds to wait before terminating a session. A user is logged out once the session timeout is reached. If the value is set to 0 then the timeout is not enforced. The default value is 0.
Max Up Rate	Enter the maximum speed, in bytes per second, that a client can transmit traffic when using the captive portal. This setting limits the bandwidth at which the client can send data into the network.
Max Down Rate	Enter the maximum speed, in bytes per second, that a client can receive traffic when using the captive portal. This setting limits the bandwidth at which the client can receive data from the network.
Max Receive	Enter the maximum number of bytes that a client is allowed to receive when using the captive portal. After this limit has been reached the user will be disconnected.

Table 224: CP Configuration (Cont.)

Field	Description
Max Transmit	Enter the maximum number of bytes that a client is allowed to transmit when using the captive portal. After this limit has been reached the user will be disconnected.
Max Total	Enter the maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received). After this limit has been reached the user will be disconnected.
User Group	<p>If the Verification Mode is Local or RADIUS, assign an existing User Group to the captive portal or create a new group. All users who belong to the group are permitted to access the network through this portal. The User Group list is the same for all CP configurations on the switch.</p> <p>The User Group field also allows you to add, delete, or rename user groups for all captive portals.</p> <ul style="list-style-type: none"> • To assign an existing user group to the CP, select it from the drop-down menu. • To create a new user group, enter the group name in the blank field and click Add. • To change the name of an existing user group, select the name to change from the drop-down menu, enter the new name in the blank field, and click Modify. • To delete a user group, select it from the drop-down menu and click Delete. <p>Note: The User Group fields are unavailable if the Verification Mode is Guest.</p>
Code	Enter the IANA Language Subtag code for the language. All codes are listed in the IANA Language Subtag Registry. If the language is currently supported by the switch, the code is filled in automatically when you select the language.
Language	To add a captive portal configuration in a language that is supported by the switch, click the ... button to display and select the language to use for the captive portal.

Customizing the Captive Portal Web Page

When a wireless client connects to the access point, the user sees a Web page. The **CP Web Page Customization** page allows you to customize the appearance of that page with specific text and images.

You can create up to five location-specific Web pages for each captive portal as long as the pages all use the same verification type; either guest or authorized user web pages. This allows you to create pages in a variety of languages to accommodate a diverse group of users.

To access the **CP WEB Customization** page, click the language link above the page title. For example, to customize the way the English version of the captive portal page looks, click **(English)**.

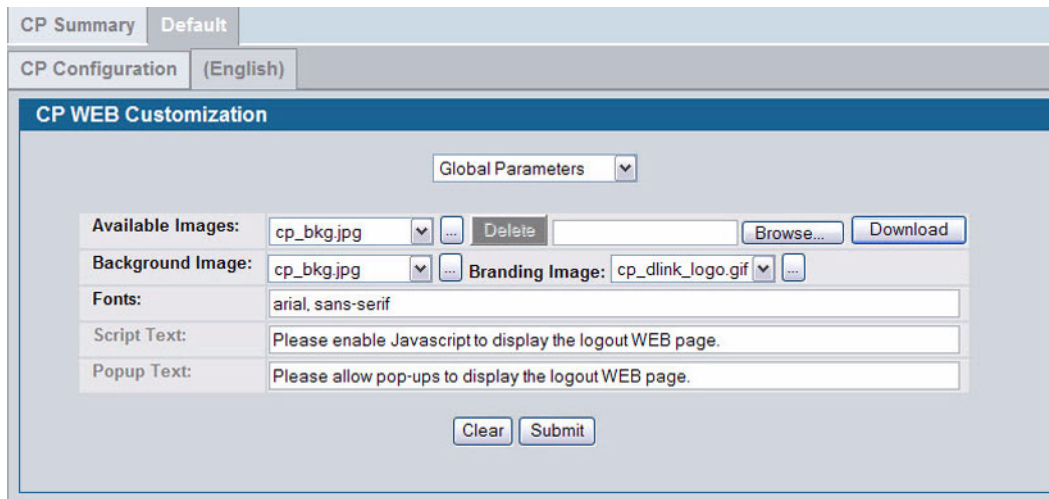
Use the menu above the customization fields to select the area of the captive portal Web page to customize. The page areas are divided into the following five categories:

- **Global Parameters**—Contains settings that can be shared across other CP pages.
- **Authentication Page**—Contains settings that affect the page users see when they first attempt to connect to the network through the CP.
- **Welcome Page**—Contains settings that affect the page users see when they successfully connect to the network.
- **Logout Page**—Contains settings that affect the client logout window users see after they successfully authenticate. This window contains the logout button.
- **Logout Success Page**—Contains settings that affect the page users see after they successfully deauthenticate.

The fields available on the **CP WEB Customization** page depend on the category you select from the menu. After you modify the fields within a category, make sure you click **Submit** before you select a different category; otherwise, your changes are not saved.

To see an example of the Authentication, Welcome, Logout, or Logout Success page, click **Preview**. The page opens in a new browser window.

To configure the portal users in a remote RADIUS server, see [“Configuring Users in a Remote RADIUS Server” on page 393](#).



The screenshot shows a web configuration interface for 'CP WEB Customization'. At the top, there are tabs for 'CP Summary' and 'Default', and a sub-section for 'CP Configuration' with '(English)' selected. The main area is titled 'CP WEB Customization' and contains a 'Global Parameters' dropdown menu. Below this, there are several configuration fields: 'Available Images' with a dropdown showing 'cp_bkg.jpg', a 'Delete' button, and 'Browse...' and 'Download' buttons; 'Background Image' with a dropdown showing 'cp_bkg.jpg' and a 'Browse...' button; 'Branding Image' with a dropdown showing 'cp_dlink_logo.gif' and a 'Browse...' button; 'Fonts' with a text input field containing 'arial, sans-serif'; 'Script Text' with a text input field containing 'Please enable Javascript to display the logout WEB page.'; and 'Popup Text' with a text input field containing 'Please allow pop-ups to display the logout WEB page.'. At the bottom of the form are 'Clear' and 'Submit' buttons.

Figure 263: CP Web Page Customization — Global Parameters

CP Summary Default

CP Configuration (English)

CP WEB Customization

Authentication Page

Background Image: cp_bkg.jpg Branding Image: cp_dlink_logo.gif

Browser Title: Captive Portal

Page Title: Welcome!

Colors: Separator: #326BA0 Foreground: #999999 Background: #BFBFBF

Account Image: login_key.jpg Account Title: Enter your Username.

User Label: Username

Password Label: Password

Button Label: Connect

Acceptance Use Policy

Check here to indicate that you have read and accepted the Acco

Instructional Text: To start using this service, enter your credentials and click the Connect button.

Denied Message: Error: Invalid Credentials, please try again!

Resource Message: Error: Limited Resources, please reconnect and try again later!

Timeout Message: Error: Timed Out, please reconnect and try again!

Busy Message: Connecting, please be patient

No Accept Message: Error: You must acknowledge the Acceptance Use Policy before connecting!

Clear Preview Submit

Figure 264: CP Web Page Customization — Authentication page

CP Summary Default

CP Configuration (English)

CP WEB Customization

Welcome Page

Branding Image: cp_dlink_logo.gif

Browser Title: Captive Portal

Title: Congratulations!

Text: You are now authorized and connected to the network.

Clear Preview Submit

Figure 265: CP Web Page Customization — Welcome Page

Figure 266: CP Web Page Customization — Logout Page

Figure 267: CP Web Page Customization — Logout Success Page

Table 225 describes the fields on the **CP Web Page Customization** page.

Table 225: CP Web Page Customization

Field	Description
Global Parameters	
Available Images	<p>The menu shows the images that are available to use for the page background, branding and the account image. To add images, click Browse and select an image on your local system (or accessible from your local system). Click Download to download the image to the switch.</p> <p>The image should be 5KB max, 200x200 pixels, GIF or JPG format.</p> <p>To delete an image from the list, select the file name from the menu and click Delete. You can only delete images that you download.</p>

Table 225: CP Web Page Customization

Field	Description
Background Image	Select the name of the image to display as the page background. Use the drop-down menu to display the file names of the available images. Click the ... button to display the available images. Click the image to select it. To specify that no background image is to be used, select <No Selection>.
Branding Image	Select the name of the image file to display on the top left corner of the page. This image is used for branding purposes, such as the company logo. Use the drop-down menu to display the file names of the available images. Click the ... button to display the available images. Click the image to select it. To specify that no branding image is to be used, select <No Selection>.
Fonts	Enter the name of the font to use for all text on the CP page.
Script Text	Specify the text to indicate that users must enable JavaScript to display the logout WEB page. This field is only applicable when the User Logout Mode is enabled, but you can modify the text whether the feature is enabled or disabled.
Popup Text	Specify the text to indicate that users must allow pop-up windows to display the logout WEB page. This field is only applicable when the User Logout Mode is enabled, but you can modify the text whether the feature is enabled or disabled.
Authentication Page	
Background Image	Shows the name of the current background image on the Authentication Page. This field can be modified from the CP WEB Customization Global Parameters page.
Branding Image	Shows the name of the current branding image on the Authentication Page. This field can be modified from the CP WEB Customization Global Parameters page.
Browser Title	Enter the text to display on the client's Web browser title bar or tab.
Page Title	Enter the text to use as the page title. This is the text that identifies the page.
Colors	Select the colors to use for the CP page. Click the ... button, and then select the color to use. The sample account information is updated with the colors you choose.
Account Image	Select the image that will display on the Captive Portal page above the login field. The image display area is 55H X 310W pixels. Note: Your image will be resized to fit the display area. To download a new image, use the Available Images field from the CP WEB Customization Global Parameters page.
Account Title	Enter the summary text to display that instructs users to authenticate.
User Label	Enter the text to display next to the field where the user enters the username.
Password Label	Enter the text to display next to the field where the user enters the password.
Button Label	Enter the text to display on the button the user clicks to connect to the network.
Acceptance Use Policy Text Box	Enter the text to display in the Acceptance Use Policy field. The acceptance use policy instructs users about the conditions under which they are allowed to access the network. The policy can contain up to 8192 text characters.
Acceptance Check Box Prompt	Enter the text to display next to the box that the user must select to indicate that he or she accepts the terms of use.
Instructional Text	Enter the detailed text to display that instructs users to authenticate. This text appears under the button.

Table 225: CP Web Page Customization

Field	Description
Denied Message	Enter the text to display when the user does not provide valid authentication information. This message displays after the user clicks the button to connect to the network.
Resource Message	Enter the text to display when the system has rejected authentication due to system resource limitations. This message displays after the user clicks the button to connect to the network.
Timeout Message	Enter the text to display when the system has rejected authentication because the authentication transaction took too long. This could be due to user input time, or a timeout due to the overall transaction.
Busy Message	Enter the text to display when the Captive Portal is processing the authentication request. This message displays after the user clicks the button to connect to the network.
No Accept Message	Enter the text to display when the user did not accept the acceptance use policy. This message displays after the user clicks the button to connect to the network.
Welcome Page	
Background Image	Shows the name of the current background image on the Welcome Page. This field can be modified from the CP WEB Customization Global Parameters page.
Branding Image	Shows the name of the current branding image on the Welcome Page. This field can be modified from the CP WEB Customization Global Parameters page.
Welcome Title	Enter the title to display to greet the user after he or she successfully connects to the network.
Welcome Text	Enter the optional text to display to further identify the network to be access by the CP user. This message displays under the Welcome Title.
Logout Page	
Note: The fields on this page are only applicable when the User Logout Mode is enabled, but you can modify the fields whether the feature is enabled or disabled.	
Browser Title	Enter the text to display on the title bar of the Logout page.
Page Title	Enter the text to use as the page title. This is the text that identifies the page.
Instructional Text	Enter the detailed text to display that confirms that the user has been authenticated and instructs the user how to deauthenticate.
Button Label	Enter the text to display on the button the user clicks to deauthenticate.
Confirmation Text	Enter the detailed text to display that prompts users to confirm the deauthentication process.
Logout Success Page	
Note: The fields on this page are only applicable when the User Logout Mode is enabled, but you can modify the fields whether the feature is enabled or disabled.	
Background Image	Shows the name of the current background image on the Logout Success page. This field can be modified from the CP WEB Customization Global Parameters page.
Branding Image	Shows the name of the current branding image on the Logout Success page. This field can be modified from the CP WEB Customization Global Parameters page.
Browser Title	Enter the text to display on the title bar of the Logout Success page.
Title	Enter the text to use as the page title. This is the text that identifies the page.
Content	Enter the text to display that confirms that the user has been deauthenticated.

Local User

You can configure a portal to accommodate guest users and authorized users. Guest users do not have assigned user names and passwords. Authorized users provide a valid user name and password that must first be validated against a local database or RADIUS server. Authorized users can gain network access once the switch confirms the user's credentials.

The **Local User Summary** page allows you to add authorized users to the local database, which can contain up to 1024 user entries. You can also delete users from the local database from the **Local User Summary** page.

To view and configure CP users in the local database, click **LAN > Security > Captive Portal > Local User**.

Any users that are already configured are listed on the **Local User Summary** page.

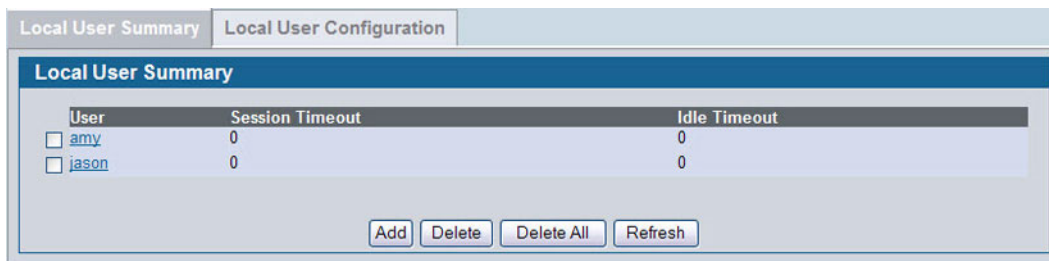


Figure 268: Captive Portal Local User Summary

Table 226 describes the fields on the **Local User Summary** page.

Table 226: Local User Summary

Field	Description
User	Identifies the name of the user.
Session Timeout	Shows the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically. A value of 0 means that the user does not have a Session Timeout limit.
Idle Timeout	Shows the number of seconds the user can remain idle before the switch automatically logs the user out. A value of 0 means that the user will not be logged out automatically.

To access the configuration page for a specific user listed on the page, click the user name.

The following buttons are available at the bottom of the Local User table:

- **Add:** Click **Add** to add a new user to the Local User database.
- **Delete:** Select the check box next to the user to remove and click **Delete**. Select multiple check boxes to delete more than one user at a time.
- **Delete All:** Click **Delete All** to remove all configured users from the local database.
- **Refresh:** Click **Refresh** to update the page with the most current information.

Adding a Local User

When you click **Add** from the Local User Summary page, the screen refreshes, and you can add a new user to the Local User database. To configure additional parameters for the new user, return to the Local User Summary page and click the name of the new user. The captive portal Global Status page displays the maximum number of users the Local User database supports.

Figure 269: Adding a New User

The following table describes the fields available when you add a new user to the local CP database. After you complete the fields, click **Add** to add the user and return to the Local User Summary page.

Table 227: Local User Configuration

Field	Description
User Name	Enter the name of the user.
Password	Enter a password for the user. The password length can be from 8 to 64 characters.
User Group	Assign the user to at least one User Group. To assign a user to more than one group, press the Ctrl key and click each group. New users are assigned to the 1-Default user group by default.

Configuring Users in the Local Database

From the **Local User Configuration** page, you can configure additional settings for an existing CP user in the local database. When you add a user, you can set maximum data transmission rates to control bandwidth usage. The timeouts and transmission limits are configured on a per-user basis.

Figure 270: Local User Configuration

Table 228 describes the fields you use to configure CP users in the local database.

Table 228: Local User Configuration

Field	Description
User Name	Enter the name of the user.
Password	Enter a password for the user. The password length can be from 8 to 64 characters.
User Group	Assign the user to at least one User Group. To assign a user to more than one group, press the Ctrl key and click each group. New users are assigned to the 1-Default user group by default.
Session Timeout	Enter the number of seconds a user is permitted to remain connected to the network. Once the Session Timeout value is reached, the user is logged out automatically. A value of 0 means that the user does not have a Session Timeout limit.
Idle Timeout	Enter the number of seconds the user can remain idle before the switch automatically logs the user out. A value of 0 means that the user does not have an idle timeout limit.
Max Up Rate	Enter the maximum speed, in bytes per second, that the user can transmit traffic when using the captive portal. This setting limits the bandwidth at which the user can send data into the network.
Max Down Rate	Enter the maximum speed, in bytes per second, that the user can receive traffic when using the captive portal. This setting limits the bandwidth at which the user can receive data from the network.
Max Receive	Enter the maximum number of bytes that the user is allowed to receive when using the captive portal. After this limit has been reached the user will be disconnected.

Table 228: Local User Configuration (Cont.)

Field	Description
Max Transmit	Enter the maximum number of bytes that the user is allowed to transmit when using the captive portal. After this limit has been reached the user will be disconnected.
Max Total	Enter the maximum number of bytes the user is allowed to transfer (sum of bytes transmitted and received). After this limit has been reached the user will be disconnected.

Configuring Users in a Remote RADIUS Server

You can use a remote RADIUS server client authorization. You must add all users to the RADIUS server. The local database in the DWS-4000 Series switch does not share any information with the remote RADIUS database.

Table 229 indicates the RADIUS attributes you use to configure authorized captive portal clients. The table indicates both RADIUS attributes and vendor-specific attributes (VSA). VSAs are denoted in the Attribute column and are comma delimited (vendor id, attribute id). For each user entry in the RADIUS user database, you can set maximum data transmission rates to control bandwidth usage. The timeouts and transmission limits are configured on a per-user basis.

Table 229: Captive Portal User RADIUS Attributes

Attribute	Number	Description	Range	Usage	Default
User-Name	1	User name to be authorized	1-32 characters	Required	None
User-Password	2	User password	8-64 characters	Required	None
Session-Timeout	27	Logout once session timeout is reached (seconds). If the attribute is 0 or not present then use the value configured for the captive portal.	Integer (seconds)	Optional	0
Idle-Timeout	28	Logout once idle timeout is reached (seconds). If the attribute is 0 or not present then use the value configured for the captive portal.	Integer (seconds)	Optional	0
WISPr-Bandwidth-Max-Up	14122, 7	Maximum client transmit rate (b/s). Limits the bandwidth at which the client can send data into the network. If the attribute is 0 or not present, then use the value configured for the captive portal.	Integer	Optional	–

Table 229: Captive Portal User RADIUS Attributes

Attribute	Number	Description	Range	Usage	Default
WISPr-Bandwidth-Max-Down	14122, 8	Maximum client receive rate (b/s). Limits the bandwidth at which the client can receive data from the network. If the attribute is 0 or not present, then use the value configured for the captive portal.	Integer	Optional	–
D-Link-Max-Input-Octets	171, 124	Maximum number of octets the user is allowed to transmit. After this limit has been reached, the user will be disconnected. If the attribute is 0 or not present, then use the value configured for the captive portal.	Integer	Optional	–
D-Link-Max-Output-Octets	171, 125	Maximum number of octets the user is allowed to receive. After this limit has been reached, the user will be disconnected. If the attribute is 0 or not present, then use the value configured for the captive portal.	Integer	Optional	–
D-Link-Max-Total-Octets	171, 126	Maximum number of octets the user is allowed to transfer (sum of octets transmitted and received). After this limit has been reached, the user will be disconnected. If the attribute is 0 or not present, then use the value configured for the captive portal.	Integer	Optional	–

Interface Association

From the **Interface Association** page, you can associate a configured captive portal with a specific physical interface or wireless network (SSID). The CP feature only runs on the wired or wireless interfaces that you specify. A CP can have multiple interfaces associated with it, but an interface can be associated to only one CP at a time.



Note: When associating a physical (wired) interface with a captive portal configuration, note the following restrictions:

- Captive portal and STP should not be enabled on the same physical interface.
- Captive portal and 802.1X cannot be enabled on the same physical interface.
- Port security and captive portal cannot be enabled on the same physical interface.
- If a physical interface is made a LAG member, the captive portal becomes disabled on the interface.

To associate interfaces with CPs, click **Security > Captive Portal > Interface Association**.

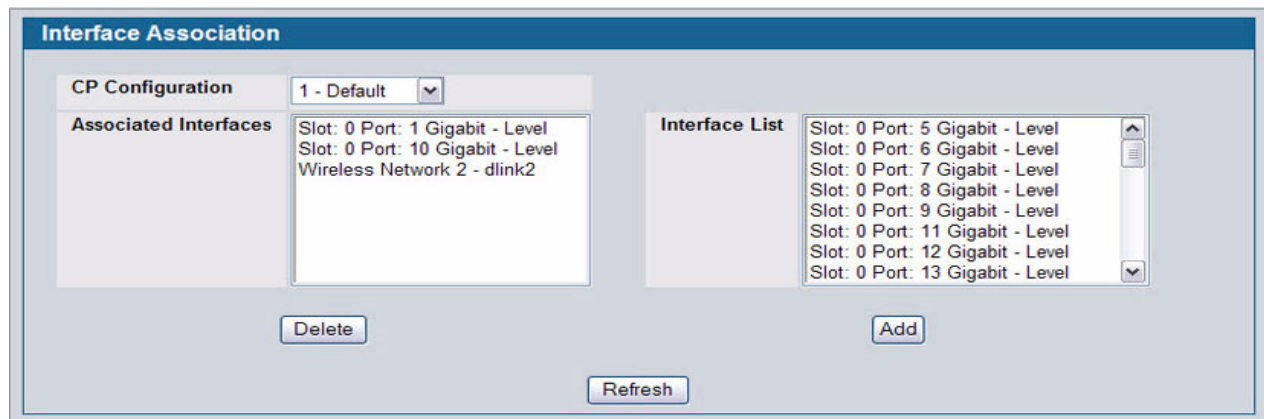


Figure 271: Interface Association

Table 230 describes the fields on the **Interface Association** page.

Table 230: Global Captive Portal Configuration

Field	Description
CP Configuration	Lists the captive portals configured on the switch by number and name.
Associated Interfaces	Lists the interfaces that are currently associated with the selected captive portal. Wireless interfaces are identified by the wireless network number and SSID. Physical (wired) interfaces are identified by the Port Description that includes slot number, port number, and interface type.
Interface List	Lists the interfaces available on the switch that are not currently associated with a CP. Wireless interfaces are identified by the wireless network number and SSID. Physical (wired) interfaces are identified by the Port Description that includes slot number, port number, and interface type.

Use the following steps to associate one or more interfaces with a captive portal.

1. Select the desired captive portal from the CP Configuration list.
2. Select the interface or interfaces from the Interface List. To select more than one interface, hold CTRL and click multiple interfaces.
3. Click **Add**.



Note: When you associate an interface with a captive portal, the interface is removed from the Interface List. Each interface can be associated with only one CP at a time.

Use the following steps to remove an interface from the Associated Interfaces list for a captive portal.

1. Select the desired captive portal from the CP Configuration list.
2. In the Associated Interfaces field, select the interface or interfaces to remove. To select more than one interface, hold CTRL and click multiple interfaces.
3. Click **Delete**.

The interface is removed from the Associated Interface list and appears in the Interface List.

CP Global Status

The **CP Global Status** page contains a variety of information about the CP feature. From the **CP Global Status** page, you can access information about the CP activity and interfaces.

To view captive portal status information, click **LAN > Security > Captive Portal > CP Status**.

Global Status		CP Activation and Activity Status	
Global Status			
CP Global Operational Status	Disabled	CP IP Address	
CP Global Disable Reason	Administrator Disabled	Supported Captive Portals	10
Supported Local Users	128	Configured Captive Portals	3
Configured Local Users	2	Active Captive Portals	0
System Supported Users	1024	Authenticated Users	0
Refresh			

Figure 272: Global Captive Portal Status

Table 231 describes the fields displayed on the **CP Global Status** page.

Table 231: Global Captive Portal Status

Field	Description
CP Global Operational Status	Shows whether the CP feature is enabled.
CP Global Disable Reason	Indicates the reason for the CP to be disabled, which can be one of the following: <ul style="list-style-type: none"> • None • Administratively Disabled • No IPv4 Address • Routing Enabled, but no IPv4 routing interface
Supported Local Users	Shows the number of entries that the Local User database supports.
Configured Local Users	Shows the number of users configured in the system.
System Supported Users	Shows the number of authenticated users that the system can support.
CP IP Address	Shows the captive portal IP address
Supported Captive Portals	Shows the number of supported captive portals in the system.
Configured Captive Portals	Shows the number of captive portals configured on the switch.
Active Captive Portals	Shows the number of captive portal instances that are operationally enabled.
Authenticated Users	Shows the number of users currently authenticated to all captive portal instances on this switch.

Viewing CP Activation and Activity Status

The **CP Activation and Activity Status** page provides information about each CP configured on the switch.



Figure 273: CP Activation and Activity Status

The **CP Activation and Activity Status** page has a drop-down menu that contains all captive portals configured on the switch. When you select a captive portal, the activation and activity status for that portal displays.

Table 232 describes the information that displays for each portal.

Table 232: CP Activation and Activity Status

Field	Description
Operational Status	Indicates whether the captive portal is enabled or disabled.
Disable Reason	<p>If the captive portal is disabled, then this field indicates the reason. The portal instance may be disabled for the following reasons:</p> <ul style="list-style-type: none"> • None - CP is enabled. • Administratively Disabled • RADIUS Authentication mode enabled, but RADIUS server is not defined. • Not associated with any interfaces. • The associated interfaces do not exist or do not support the CP capability.
Blocked Status	<p>Indicates whether authentication attempts to the captive portal are currently blocked. Use the Block and Unblock buttons to control the blocked status. If the CP is blocked, users cannot gain access to the network through the CP. Use this function to temporarily protect the network during unexpected events, such as denial of service attacks.</p> <p>Block and Unblock are only available when the CP operational status is Enabled. The blocked status is an operational parameter and does not persist across switch reboot even if the switch configuration is saved before a reboot.</p>
Authenticated Users	Shows the number of users that successfully authenticated to this captive portal and are currently using the portal.

The following buttons are available on the **CP Activation and Activity** page:

- **Block**—Click **Block** to prevent users from gaining access to the network through the selected captive portal.
- **Unblock**—If the Blocked Status of the selected captive portal is **Blocked**, click **Unblock** to allow access to the network through the captive portal.
- **Refresh**—Click **Refresh** to update the screen with the most current information.

Interface Status

The pages available from the **Interface Status** link provide information about the captive portal interfaces and their capabilities.

Viewing Interface Activation Status

The **Interface Activation Status** page shows information for every interface assigned to a captive portal instance. Use the drop-down menus to select the portal or interface for which you want to view information.

Field	Description
Operational Status	Disabled
Disable Reason	Administrator Disabled
Blocked Status	Not Blocked
Authenticated Users	0

Figure 274: Interface Activation Status

The following table describes the fields on the **Interface Activation Status** page.

Table 233: Interface Activation Status

Field	Description
Operational Status	Shows whether the portal is active on the specified interface.
Disable Reason	If the selected CP is disabled on this interface, this field indicates the reason, which can be one of the following: <ul style="list-style-type: none"> • Interface Not Attached • Disabled by Administrator
Blocked Status	Indicates whether the captive portal is temporarily blocked for authentications.
Authenticated Users	Displays the number of authenticated users using the captive portal instance on this interface.

Viewing Interface Capability Status

The **Interface Capability Status** page contains information about interfaces that can have CPs associated with them. The page also contains status information for various capabilities. Specifically, this page indicates what services are provided through the CP to clients connected on this interface. The list of services is determined by the interface capabilities.

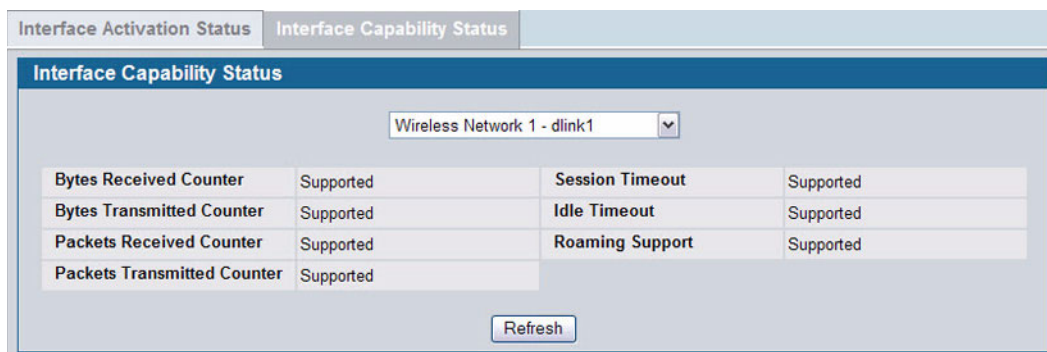


Figure 275: Interface Capability Status

The drop-down menu contains all the wired and wireless interfaces available on the switch. Each wireless interface is identified by its wireless network number and SSID. Physical (wired) interfaces are identified by the Port Description that includes slot number, port number, and interface type.

Use the drop-down menu to select the interface with the information to display.

[Table 234](#) describes the fields on the **Interface Capability Status** page.

Table 234: Interface and Capability Status

Parameter	Description
Bytes Received Counter	Shows whether the interface supports displaying the number of bytes received from each client.
Bytes Transmitted Counter	Shows whether the interface supports displaying the number of bytes transmitted to each client.
Packets Received Counter	Shows whether the interface supports displaying the number of packets received from each client.
Packets Transmitted Counter	Shows whether the interface supports displaying the number of packets transmitted to each client.
Session Timeout	Shows whether the interface supports client session timeout. This attribute is supported on all interfaces.
Idle Timeout	Shows whether the interface supports a timeout when the user does not send or receive any traffic.
Roaming Support	Shows whether the interface supports client roaming. Only wireless interfaces support client roaming.

Client Connection Status

From the Client Connection Status page, you can access several pages that provide information about clients that are connected to the switch through the CP.

Use the **Client Summary page to view summary information** about all authenticated wireless clients that are connected through the captive portal. From this page, you can manually force the captive portal to disconnect one or more authenticated clients. The list of wireless clients is sorted by client MAC address.

If the switch supports clustering and there are peer switches in the cluster, some of the clients displayed on the page might be connected to the network through other switches. For more information about the client, and to view information about which switch handled the authentication for the client, click the MAC address of the client.

To view information about the wireless clients connected to the DWS-4000 Series switch through the captive portal, click **LAN > Security > Captive Portal > Client Connection Status**.

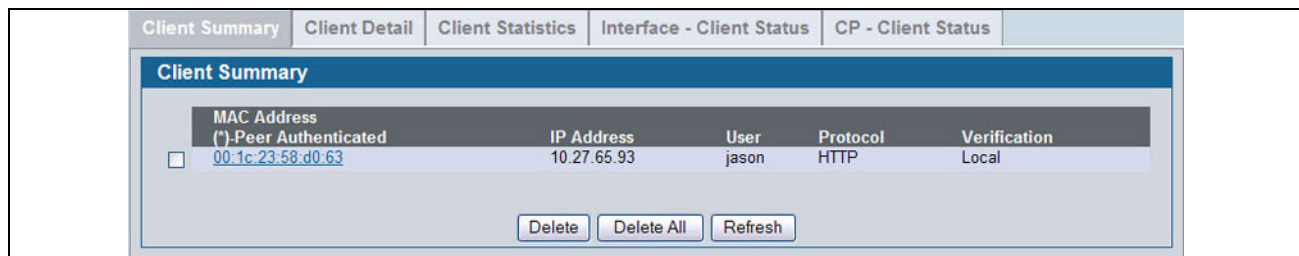


Figure 276: Client Summary

The following table describes the fields on the **Client Summary** page.

Table 235: Client Summary

Field	Description
MAC Address	Identifies the MAC address of the wireless client (if applicable). If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In other words, the cluster controller was not the authenticator.
IP Address	Identifies the IP address of the wireless client (if applicable).
User	Displays the user name (or Guest ID) of the connected client.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.

To force the captive portal to disconnect an authenticated client, select the check box next to the client MAC address and click **Delete**. To disconnect all clients from all captive portals, click **Delete All**.

Viewing Client Details

The **Client Detail** page shows detailed information about each client connected to the network through a captive portal.

Client Detail			
00:1c:23:58:d0:63 ▼			
Client IP Address	10.27.65.93	User Name	jason
CP Configuration	1-Default	Interface	Slot: 0 Port: 1 Gigabit - Level
Protocol	HTTP	Verification	Local
Session Time	0d:00:02:57	Switch MAC Address	00:17:9A:95:00:60
Switch Type	Local	Switch IP Address	10.27.65.148

Figure 277: Client Detail

The drop-down menu lists each associated client by MAC address. To view status information for a different client, select its MAC address from the list.

[Table 236](#) describes the fields on the **Client Detail** page.

Table 236: Client Detail

Field	Description
Client IP Address	Identifies the IP address of the wireless client (if applicable).
CP Configuration	Identifies the CP configuration the wireless client is using.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Session Time	Shows the amount of time that has passed since the client was authorized.
Switch Type	Shows whether the switch handling authentication for this client is the local switch or a peer switch in the cluster.
User Name	Displays the user name (or Guest ID) of the connected client.
Interface	Identifies the interface the wireless client is using.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.
Switch MAC Address	Shows the MAC address of the switch handling authentication for this client. If clustering is supported, this field might display the MAC address of a peer switch in the cluster.
Switch IP Address	Shows the IP address of the switch handling authentication for this client. If clustering is supported, this field might display the IP address of a peer switch in the cluster.

Viewing the Client Statistics

Use the **Client Statistics** page to view information about the traffic a client has sent or received.

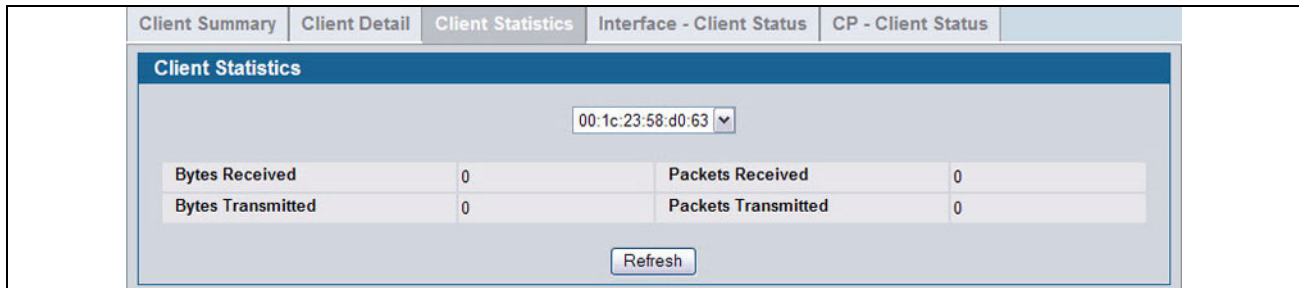


Figure 278: Client Statistics

The drop-down menu lists each associated client by MAC address. To view statistical information for a client, select it from the list.

[Table 237](#) describes the fields on the **Client Statistics** page.

Table 237: Client Interface Association Connection Statistics

Field	Description
Bytes Transmitted	Total bytes the client has transmitted
Bytes Received	Total bytes the client has received
Packets Transmitted	Total packets the client has transmitted
Packets Received	Total packets the client has received

Viewing the Client Interface Association Status

Use the **Interface - Client Status** page to view clients that are authenticated to a specific interface.

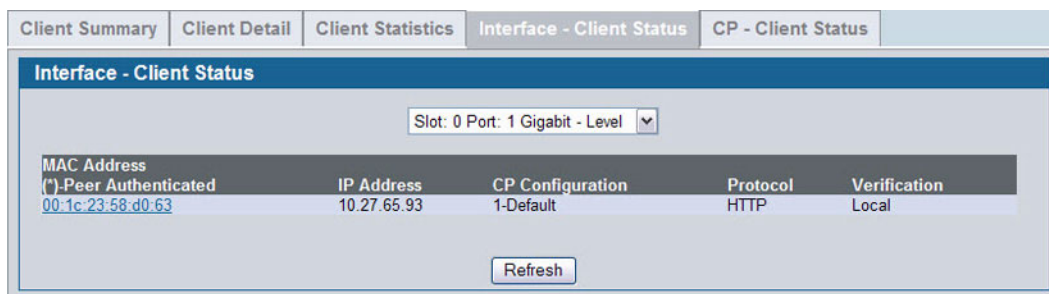


Figure 279: Interface - Client Status

The drop-down menu lists each interface on the switch. To view information about the clients connected to a CP on this interface, select it from the list.

Table 238 describes the fields on the **Interface - Client Status** page.

Table 238: Interface - Client Status

Field	Description
MAC Address	Identifies the MAC address of the wireless client. If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In order words, the cluster controller was not the authenticator.
IP Address	Identifies the IP address of the wireless client.
CP Configuration	Identifies the captive portal the client used to access the network.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.

Viewing the Client CP Association Status

Use the **CP - Client Status** page to view clients that are authenticated to a specific CP configuration.

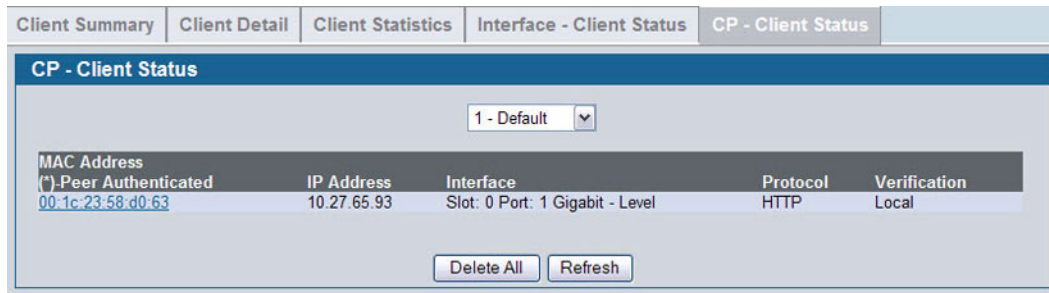


Figure 280: CP - Client Status

The drop-down menu lists each CP configured on the switch. To view information about the clients connected to the CP, select it from the list.

The following table describes the fields on the **Client CP Association Status** page.

Table 239: CP - Client Status

Field	Description
MAC Address	Identifies the MAC address of the wireless client. If the MAC address is marked with an asterisk (*), the authenticated client is authenticated by a peer switch. In order words, the cluster controller was not the authenticator.
IP Address	Identifies the IP address of the wireless client.
Interface	Identifies the interface the client used to access the network.
Protocol	Shows the current connection protocol, which is either HTTP or HTTPS.
Verification	Shows the current account type, which is Guest, Local, or RADIUS.

SNMP Trap Configuration

Use the **SNMP Trap Configuration** page to configure whether or not SNMP traps are sent from the Captive Portal and to specify captive portal events that will generate a trap.



Note: You can configure the Captive Portal traps only if the Captive Portal Trap Mode is enabled, which you configure on the LAN > Administration > SNMP Manager > Trap Flags page.

All CP SNMP traps are disabled by default.

To configure SNMP trap settings for various captive portal features, click **Security > Captive Portal > SNMP Trap Configuration**.

SNMP Trap Configuration	
Captive Portal Trap Mode	Disabled
Client Authentication Failure Traps	Disable ▾
Client Connection Traps	Disable ▾
Client Database Full Traps	Disable ▾
Client Disconnection Traps	Disable ▾

Submit Refresh

Figure 281: SNMP Trap Configuration

The traps specified in the table below are generated only by the Cluster Controller unless otherwise specified. The following table describes the events that generate SNMP traps when the status is Enabled.

Table 240: SNMP Trap Configuration

Field	Description
Captive Portal Trap Mode	Displays the captive portal trap mode status. To enable or disable the mode, use Captive Portal menu on the LAN > Administration > SNMP Manager > Trap Flags page.
Client Authentication Failure Traps	If you enable this field, the SNMP agent sends a trap when a client attempts to authenticate with a captive portal but is unsuccessful.
Client Connection Traps	If you enable this field, the SNMP agent sends a trap when a client authenticates with and connects to a captive portal.
Client Database Full Traps	If you enable this field, the SNMP agent sends a trap each time an entry cannot be added to the client database because it is full.
Client Disconnection Traps	If you enable this field, the SNMP agent sends a trap when a client disconnects from a captive portal.

RADIUS Settings

Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. The RADIUS server maintains a user database, which contains per-user authentication information. RADIUS servers provide a centralized authentication method for:

- Telnet Access
- Web Access
- Console Access
- Port Access Control (802.1X)

RADIUS Configuration

Use the **RADIUS Configuration** page to view and configure various settings for the RADIUS servers configured on the system.

To access the **RADIUS Configuration** page, click **LAN > Security > RADIUS > RADIUS Configuration** in the navigation menu.

Figure 282: RADIUS Configuration

Table 241: RADIUS Configuration Fields

Field	Description
Number of Configured Authentication Servers	The number of RADIUS authentication servers configured on the system. The value can range from 0 to 32.
Number of Configured Accounting Servers	The number of RADIUS accounting servers configured on the system. The value can range from 0 to 32.
Number of Named Authentication Server Groups	The number of authentication server groups configured on the system. An authentication server group contains one or more configured authentication servers that share the same RADIUS server name.

Table 241: RADIUS Configuration Fields (Cont.)

Field	Description
Number of Named Accounting Server Groups	The number of accounting server groups configured on the system. An accounting server group contains one or more configured authentication servers that share the same RADIUS server name.
Max Number of Retransmits	The value of the maximum number of times a request packet is retransmitted. The valid range is 1-15. Consideration to maximum delay time should be given when configuring RADIUS max retransmit and RADIUS timeout. If multiple RADIUS servers are configured, the max retransmit value on each will be exhausted before the next server is attempted. A retransmit will not occur until the configured timeout value on that server has passed without a response from the RADIUS server. Therefore, the maximum delay in receiving a response from the RADIUS application equals the sum of (retransmit times timeout) for all configured servers. If the RADIUS request was generated by a user login attempt, all user interfaces will be blocked until the RADIUS application returns a response.
Timeout Duration (secs)	The timeout value, in seconds, for request retransmissions. The valid range is 1 - 30. See the Max Number of Retransmits field description for more information about configuring the timeout duration.
Accounting Mode	Use the menu to select whether the RADIUS accounting mode is enabled or disabled on the current server.
Enable RADIUS Attribute 4 (NAS-IP Address)	To set the network access server (NAS) IP address for the RADIUS server, select the option and enter the IP address of the NAS in the available field. The address should be unique to the NAS within the scope of the RADIUS server. The NAS IP address is only used in Access-Request packets.
NAS-IP Address	Enter the IP address of the NAS. This field can be edited only when the Enable RADIUS Attribute 4 field is selected. The address should be unique to the NAS within the scope of the RADIUS server. The NAS IP address is only used in Access-Request packets.

Use the buttons at the bottom of the page to perform the following actions:

- Click **Refresh** to update the page with the most current information.
- If you make changes to the page, click **Submit** to apply the changes to the system.

RADIUS Server Configuration

From the **RADIUS Authentication Server Configuration** page, you can add a new RADIUS server, configure settings for a new or existing RADIUS server, and view RADIUS server status information. The RADIUS client on the switch supports up to 32 named authentication and accounting servers.

To access the RADIUS Server Configuration page, click **LAN > Security > RADIUS > RADIUS Authentication Server Configuration** in the navigation menu.

If there are no RADIUS servers configured on the system, or if you select Add from the RADIUS Server Host Address menu, a subset of the fields described in the following table are available. After you enter the RADIUS host address and click **Submit**, the additional configuration fields appear.

RADIUS Authentication Server Configuration	
RADIUS Server Host Address	Add ▾
Host Address	<input type="text"/>
RADIUS Server Name	Default-RADIUS-Server
Submit	

Figure 283: RADIUS Server Configuration—Add Server

If at least one RADIUS server is configured on the switch, and a host address is selected in the RADIUS Server Host Address field, then additional fields are available on the RADIUS Server Configuration page.

RADIUS Authentication Server Configuration	
RADIUS Server Host Address	10.27.65.66 ▾
Port	1812 (1 to 65535)
Secret	<input type="text"/> <input type="checkbox"/> Apply
Primary Server	No ▾
Message Authenticator	Enable ▾
Secret Configured	No
Current	Yes
RADIUS Server Name	Default-RADIUS-Server
Submit Remove Refresh	

Figure 284: RADIUS Server Configuration—Server Added

Table 242: RADIUS Server Configuration Fields

Field	Description
RADIUS Server Host Address	Use the drop-down menu to select the IP address of the RADIUS server to view or configure. Select Add to configure additional RADIUS servers.
Port	Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port, and the valid range is 1-65535. The default port for RADIUS authentication is 1812.
Secret	Shared secret text string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This secret must match the RADIUS encryption.
Apply	The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if the user has READWRITE access.
Primary Server	Sets the selected server to the Primary (Yes) or Secondary (No) server. If you configure multiple RADIUS servers with the same RAIDUS Server Name, designate one server as the primary and the other(s) as the backup server(s). The switch attempts to use the primary server first, and if the primary server does not respond, the switch attempts to use one of the backup servers with the same RADIUS Server Name.
Message Authenticator	Enable or disable the message authenticator attribute for the selected server.
Secret Configured	Indicates whether the shared secret for this server has been configured.
Current	Indicates whether the selected RADIUS server is the current server (Yes) or a backup server (No). If more than one RADIUS server is configured with the same name, the switch selects one of the servers to be the <i>current</i> server from the group of servers with the same name. When the switch sends a RADIUS request to the named server, the request is directed to the server selected as the current server. Initially the primary server is selected as the current server. If the primary server fails, one of the other servers becomes the current server. If the primary server is not configured, the current server is the most recently configured RADIUS server.
RADIUS Server Name	Shows the RADIUS server name. To change the name, enter up to 32 alphanumeric characters. Spaces, hyphens, and underscores are also permitted. If you do not assign a name, the server is assigned the default name Default-RADIUS-Server. Note: Configure at least one RADIUS server with the name Default-RADIUS-Server. Some of the switch features, such as 802.1X, expect the RADIUS server to use the default name. You can use the same name for multiple RADIUS Authentication servers. RADIUS clients can use RADIUS servers with the same name as backups for each other.

Use the buttons at the bottom of the page to perform the following actions:

- If you make changes to the page, click **Submit** to apply the changes to the system.
- To delete a configured RADIUS authentication server, select the IP address of the server from the **RADIUS Server Host Address** menu, and then click **Remove**.
- Click **Refresh** to update the page with the most current information.

Viewing Named Server Status Information

The **RADIUS Named Server Status** page shows summary information about the RADIUS servers configured on the system.

Current	RADIUS Server Host Address	RADIUS Server Name	Port Number	Server Type	Secret Configured	Message Authenticator
*	10.27.65.66	Default-RADIUS-Server	1812	Secondary	No	Enable

Figure 285: Named Server Status

Table 243: RADIUS Server Configuration Fields

Field	Description
Current	An asterisk (*) in the column indicates that the server is the current server for the authentication server group. If no asterisk is present, the server is a backup server. If more than one RADIUS server is configured with the same name, the switch selects one of the servers to be the current server from the group of servers with the same name. When the switch sends a RADIUS request to the named server, the request is directed to the server selected as the current server. Initially the primary server is selected as the current server. If the primary server fails, one of the other servers becomes the current server.
RADIUS Server Host Address	Shows the IP address of the RADIUS server.
RADIUS Server Name	Shows the RADIUS server name. Multiple RADIUS servers can have the same name. In this case, RADIUS clients can use RADIUS servers with the same name as backups for each other.
Port Number	Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.
Server Type	Shows whether the server is a Primary or Secondary server.
Secret Configured	Indicates whether the shared secret for this server has been configured.
Message Authenticator	Shows whether the message authenticator attribute for the selected server is enabled or disabled.

Click **Refresh** to update the page with the most current information.

RADIUS Server Statistics

To access the RADIUS Server Statistics page, click **LAN > Monitoring > RADIUS Statistics > Server Statistics** in the navigation menu.

RADIUS Server Statistics	
RADIUS Server Host Address	10.27.65.103
Round Trip Time (secs)	0.00
Access Requests	0
Access Retransmissions	0
Access Accepts	0
Access Rejects	0
Access Challenges	0
Malformed Access Responses	0
Bad Authenticators	0
Pending Requests	0
Timeouts	0
Unknown Types	0
Packets Dropped	0

Figure 286: RADIUS Server Statistics

RADIUS Accounting Server Configuration

From the **RADIUS Accounting Server Configuration** page, you can add a new RADIUS accounting server, configure settings for a new or existing RADIUS accounting server, and view RADIUS accounting server status information. The RADIUS client on the switch supports up to 32 named authentication and accounting servers.

If there are no RADIUS accounting servers configured on the system or if you select Add from the Accounting Server Host Address menu, a subset of the fields described in the following table are available.

Configuration | Named Accounting Server Status

RADIUS Accounting Server Configuration

Accounting Server Host Address	Add
Host Address	
RADIUS Accounting Server Name	Default-RADIUS-Server

Figure 287: Add RADIUS Accounting Server

After you enter the Accounting server host address and click **Submit**, the additional configuration fields appear.

If at least one RADIUS accounting server is configured on the switch, and a host address is selected in the Accounting Server Host Address field, then additional fields are available on the Accounting Server Configuration page.

Figure 288: RADIUS Accounting Server Configuration—Server Added

Table 244: RADIUS Accounting Server Configuration Fields

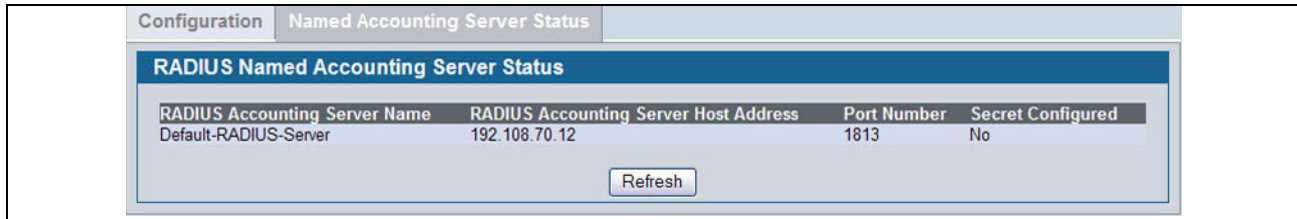
Field	Description
Accounting Server Host Address	Use the drop-down menu to select the IP address of the accounting server to view or configure. Select Add to configure additional RADIUS servers.
Port	Identifies the authentication port the server uses to verify the RADIUS accounting server authentication. The port is a UDP port, and the valid range is 1-65535. The default port for RADIUS accounting is 1813.
Secret	Specifies the shared secret to use with the specified accounting server. This field is only displayed if you are logged into the switch with READWRITE access.
Apply	The Secret will only be applied if this box is checked. If the box is not checked, anything entered in the Secret field will have no affect and will not be retained. This field is only displayed if you are logged into the switch with READWRITE access.
Secret Configured	Indicates whether the shared secret for this server has been configured.
RADIUS Accounting Server Name	Enter the name of the RADIUS accounting server. The name can contain up to 32 alphanumeric characters. Spaces, hyphens, and underscores are also permitted. If you do not assign a name, the server is assigned the default name Default-RADIUS-Server. You can use the same name for multiple RADIUS accounting servers. RADIUS clients can use accounting servers with the same name as backups for each other.

Use the buttons at the bottom of the page to perform the following actions:

- If you make changes to the page, click **Submit** to apply the changes to the system.
- To delete a configured RADIUS accounting server, select the IP address of the server from the **RADIUS Server IP Address** drop-down menu, and then click **Remove**.
- Click **Refresh** to update the page with the most current information.

Viewing Named Accounting Server Status

The RADIUS **Named Accounting Server Status** page shows summary information about the accounting servers configured on the system.



RADIUS Accounting Server Name	RADIUS Accounting Server Host Address	Port Number	Secret Configured
Default-RADIUS-Server	192.108.70.12	1813	No

Figure 289: RADIUS Server Configuration—Server Added

Table 245: Named Accounting Server Fields

Field	Description
RADIUS Accounting Server Name	Shows the RADIUS accounting server name. Multiple RADIUS accounting servers can have the same name. In this case, RADIUS clients can use RADIUS servers with the same name as backups for each other.
IP Address	Shows the IP address of the RADIUS server.
Port Number	Identifies the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.
Secret Configured	Indicates whether the shared secret for this server has been configured.

Click **Refresh** to update the page with the most current information.

RADIUS Server Statistics

To access the RADIUS Server Statistics page, click **LAN > Monitoring > RADIUS Statistics > Server Statistics** in the navigation menu.

RADIUS Accounting Server Statistics	
Accounting Server Host Address	10.27.65.104
Round Trip Time (secs)	0.00
Accounting Requests	0
Accounting Retransmissions	0
Accounting Responses	0
Malformed Access Responses	0
Bad Authenticators	0
Pending Requests	0
Timeouts	0
Unknown Types	0
Packets Dropped	0

Refresh

Figure 290: RADIUS Accounting Server Statistics

Clear Statistics

Use the RADIUS **Clear Statistics** page to reset all RADIUS authentication and accounting statistics to zero.

To access the RADIUS Clear Statistics page, click **LAN > Security > RADIUS > Clear RADIUS Statistics** in the navigation menu.

Clear RADIUS Statistics

Clear All RADIUS Statistics

Clear

Figure 291: RADIUS Clear Statistics

To clear all statistics for the RADIUS authentication and accounting server, click **Clear**.

Port Access Control

In port-based authentication mode, when 802.1X is enabled globally and on the port, successful authentication of any one supplicant attached to the port results in all users being able to use the port without restrictions. At any given time, only one supplicant is allowed to attempt authentication on a port in this mode. Ports in this mode are under bidirectional control. This is the default authentication mode.

The 802.1X network has three components:

- **Authenticators:** Specifies the port that is authenticated before permitting system access.
- **Supplicants:** Specifies host connected to the authenticated port requesting access to the system services.
- **Authentication Server:** Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

Global Port Access Control Configuration

Use the Port Based Access Control Configuration page to enable or disable port access control on the system.

To display the Port Based Authentication page, click **LAN > Security > Port Access Control > Configuration** in the navigation menu.

Figure 292: Global Port Access Control Configuration

Table 246: Global Port Access Control Configuration Fields

<i>Field</i>	<i>Description</i>
Administrative Mode	Select Enable or Disable 802.1x mode on the switch. The default is Disable. This feature permits port-based authentication on the switch.
VLAN Assignment Mode	If enabled, when a supplicant is authenticated by a authentication server, the port that the supplicant is connected to is placed in a particular VLAN specified by the RADIUS server. VLAN Assignment mode controls if the switch is allowed to place a port in a RADIUS-assigned VLAN. A port's VLAN assignment is determined by the first supplicant that is authenticated on the port.

Table 246: Global Port Access Control Configuration Fields (Cont.)

Field	Description
Dynamic VLAN Creation Mode	Select Enable to allow the switch to dynamically create a RADIUS-assigned VLAN if it does not already exist in the VLAN database.
Monitor Mode	Select Enable to permit network access even when the 802.1X authentication process fails. The switch logs the results of the authentication process for diagnostic purposes. Monitor Mode can help you troubleshoot Dot1X configuration problems without affecting network access for end users.

- If you change the mode, click **Submit** to apply the new settings to the system.

Port Configuration

Use the Port Access Control Port Configuration page to enable and configure port access control on one or more ports.

To access the Port Based Access Control Port Configuration page, click **LAN > Security > Port Access Control > Port Configuration** in the navigation menu.

Port Access Control Port Configuration

Port	0/1	
Control Mode	Auto	
Quiet Period (secs)	60	(0 to 65535)
Transmit Period (secs)	30	(1 to 65535)
Guest VLAN ID	0	(0 to 3965)
Guest VLAN Period (secs)	90	(1 to 300)
Unauthenticated VLAN ID	0	(0 to 3965)
Supplicant Timeout (secs)	30	(1 to 65535)
Server Timeout (secs)	30	(1 to 65535)
Maximum Requests	2	(1 to 10)
Reauthentication Period (secs)	3600	(1 to 65535)
Reauthentication Enabled	False	
Maximum Users	16	(1 to 16)

Submit Refresh Initialize Reauthenticate

Figure 293: Port Access Control Port Configuration

Table 247: Port Access Control Port Configuration Fields

Field	Description
Port	Selects the Port to configure.
Control Mode	<p>Defines the port authorization state. The control mode is only set if the link status of the port is link up. The possible field values are:</p> <ul style="list-style-type: none"> • Auto: Automatically detects the mode of the interface. • Force Authorized: Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication. • Force Unauthorized: Denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface.
Quiet Period (secs)	<p>Defines the amount of time that the switch remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field value is in seconds. The field default is 60 seconds.</p>
Transmit Period (secs)	<p>Defines the transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The transmit period must be a number in the range of 1 and 65535. The default value is 30.</p>
Guest VLAN ID	<p>Defines the Guest VLAN ID on the interface. The valid range is 0 to 3965. The default value is 0. Enter zero (0) to clear the Guest VLAN ID on the interface.</p>
Guest VLAN Period (secs)	<p>Defines the Guest VLAN period for the selected port. The Guest VLAN period is the value, in seconds, of the timer used by the Guest VLAN Authentication. The Guest VLAN timeout must be a value in the range of 1 to 300. The default value is 90.</p>
Unauthenticated VLAN ID	<p>Defines the Unauthenticated VLAN ID for the selected port. The valid range is 0 to 3965. The default value is zero (0). Enter zero (0) to clear the Unauthenticated VLAN ID on the interface.</p>
Supplicant Timeout (secs)	<p>Defines the amount of time that lapses before EAP requests are resent to the user. The value must be in the range of 1 to 65535 seconds. The value is 30 seconds.</p>
Server Timeout (secs)	<p>Defines the amount of time that lapses before the switch resends a request to the authentication server. The field value is in seconds. The range is 1-65535, and the field default is 30 seconds.</p>
Maximum Requests	<p>Defines the maximum number of times the switch can send an EAP request before restarting the authentication process if it does not receive a response. The possible field range is 1-10. The field default is 2 retries.</p>
Reauthentication Period (secs)	<p>Indicates the time span in which the selected port is reauthenticated. The field value is in seconds. The range is 1 - 65535, and the field default is 3600 seconds.</p>
Reauthentication Enabled	<p>Reauthenticates the selected port periodically, when enabled. The default value is False.</p>
Maximum Users	<p>Defines the maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. The range is 1 to 16. The default value is 16.</p>

- Click **Submit** to send the updated screen to the switch and cause the changes to take effect on the switch but these changes will not be retained across a power cycle unless a save is performed.
- Click **Refresh** to update the information on the screen.
- Click **Initialize** to begin the initialization sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.
- Click **Reauthenticate** to begin the reauthentication sequence on the selected port. This button is only selectable if the control mode is 'auto'. If the button is not selectable, it will be grayed out. Once this button is pressed, the action is immediate. It is not required to press the Submit button for the action to occur.

Port Access Entity Capability Configuration

Use the Port Access Entity (PAE) Capability Configuration page to configure a port as an authenticator or supplicant.

To access the PAE Capability Configuration page, click **LAN > Security > Port Access Control > PAE Capability Configuration**.

Figure 294: PAE Capability Configuration

Table 248: PAE Capability Configuration

Field	Description
Port	Select the Slot/Port to configure.
PAE Capabilities	Select authenticator or supplicant from the list.

Click **Submit** to set the PAE capability. Note that these changes will not be retained across a power cycle unless you explicitly save the changes (see [“Save All Applied Changes” on page 167](#)).

If you configured a port as a supplicant, use the [“Supplicant Port Configuration”](#) page to configure additional operational parameters for the port.

Supplicant Port Configuration

After you have configured a port as a supplicant, use this page to configure operational properties of the port.

To access the Supplicant Port Configuration page, click **LAN > Security > Port Access Control > Supplicant Port Configuration**.

Supplicant Port Configuration	
Interface	0/1
Control Mode	Auto
User Name	admin
Start Period (secs)	30 (1 to 65535)
Held Period (secs)	60 (1 to 65535)
Authentication Period (secs)	30 (1 to 65535)
Maximum Requests	3 (1 to 10)
<input type="button" value="Submit"/> <input type="button" value="Refresh"/>	

Figure 295: Port Access Control Supplicant Port Configuration

Table 249: Dot1x Supplicant Port Configuration

Field	Description
Interface	Select the port to configure.
Control Mode	Select the port authorization state. The control mode is set only if the link status of the port is link up. The possible field values are: Auto: The ports mode (Authorized, Unauthorized, etc.) is determined by 802.1X exchanges with supplicants and the authentication server. Force Authorized: Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication. Force Unauthorized: Denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to supplicants through this interface.
User Name	Select the users that will have access to the specified port. The possible values are admin and guest.
Start Period	Enter the wait interval period in seconds for the supplicant to receive the authenticator's EAP Identity request message.
Held Period	Enter the wait interval period in seconds for the supplicant to start the next authentication process after a previous authentication process failure.
Authentication Period	Enter the wait interval period for the supplicant to receive EAP challenge requests from the authenticator.
Maximum Requests	Enter the maximum number of successive EAPOL start messages that will be sent before the supplicant assumes that there is no authenticator present.

Click **Submit** to configure the supplicant. Click **Refresh** to display the page with the latest data from the switch.

Port Status

Use the Port Access Control Port Status page to view information about the port access control settings on a specific port.

To access the Port Access Control Port Status page, click **Security > Port Access Control > Port Status** in the navigation menu.

Port Access Control Status	
Interface	0/1
Protocol Version	Version1
PAE Capabilities	Authenticator
Control Mode	Auto
Authenticator PAE State	Initialize
Backend State	Initialize
Quiet Period (secs)	60
Transmit Period (secs)	30
Guest VLAN ID	0
Guest VLAN Period (secs)	90
Supplicant Timeout (secs)	30
Server Timeout (secs)	30
Maximum Requests	2
VLAN Assigned	0
VLAN Assigned Reason	Not Assigned
Reauthentication Period (secs)	3600
Reauthentication Enabled	FALSE
Key Transmission Enabled	FALSE
Control Direction	Both
Maximum Users	16
Unauthenticated VLAN ID	0
Session Timeout	0
Session Termination Action	Default

Refresh

Figure 296: Port Access Control Status

[Figure 297 on page 421](#) is an example of the fields displayed for the port when the Control mode of the port is MAC-based.

Port Access Control Status	
Interface	0/10
Protocol Version	Version 1
PAE Capabilities	Authenticator
Control Mode	MAC Based
Quiet Period (secs)	60
Transmit Period (secs)	30
Guest VLAN ID	0
Guest VLAN Period (secs)	90
Supplicant Timeout (secs)	30
Server Timeout (secs)	30
Maximum Requests	2
Reauthentication Period (secs)	3600
Reauthentication Enabled	FALSE
Key Transmission Enabled	FALSE
Control Direction	Both
Maximum Users	16
Unauthenticated VLAN ID	0

Logical Port	Supplicant MAC Address	Authenticator PAE State	Backend Authentication State	VLAN Assigned	VLAN Assigned Reason

Refresh

Figure 297: Port Access Control Status - MAC-based Control Mode

Table 250: Port Access Control Status Fields

Field	Description
Interface	Selects the Unit and Port to view.
Protocol Version	This field displays the protocol version associated with the selected port. The only possible value is 1, corresponding to the first version of the 802.1x specification. This field is not configurable.
PAE Capabilities	This field displays the port access entity (PAE) functionality of the selected port. Possible values are "Authenticator" or "Supplicant". This field is not configurable.
Control Mode	<p>Defines the port authorization state. The control mode is only set if the link status of the port is link up. The possible field values are:</p> <ul style="list-style-type: none"> • Auto: Automatically detects the mode of the interface. • Force Authorized: Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication. • Force Unauthorized: Denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface. • MAC-based: Sets the mode of the interface to authentication on a per supplicant basis.

Table 250: Port Access Control Status Fields (Cont.)

Field	Description
Authenticator PAE State	This field displays the current state of the authenticator PAE state machine. Possible values are as follows: <ul style="list-style-type: none"> • Initialize • Disconnected • Connecting • Authenticating • Authenticated • Aborting • Held • ForceAuthorized • ForceUnauthorized
Backend Authentication State	This field displays the current state of the backend authentication state machine. Possible values are as follows: <ul style="list-style-type: none"> • Request • Response • Success • Fail • Timeout • Initialize • Idle
Quiet Period	Displays the configured quiet period for the selected port. This quiet period is the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet period is the period for which the authenticator does not attempt to acquire a supplicant after a failed authentication exchange with the supplicant. The quiet period is a number in the range of 0 and 65535.
Transmit Period	Displays the configured transmit period for the selected port. The transmit period is the value, in seconds, of the timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The transmit period is a number in the range of 1 and 65535.
Guest VLAN ID	Displays the Guest VLAN ID configured on the interface. The valid range is 0 to 3965.
Guest VLAN Period (secs)	Displays the Guest VLAN period for the selected port. The Guest VLAN period is the value, in seconds, of the timer used by the Guest VLAN Authentication. The value is in the range of 1 to 300.
Supplicant Timeout	Displays the configured supplicant timeout for the selected port. The supplicant timeout is the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supplicant timeout is a value in the range of 1 and 65535.
Server Timeout	Displays the configured server timeout for the selected port. The server timeout is the value, in seconds, of the timer used by the authenticator on this port to timeout the authentication server. The server timeout is a value in the range of 1 and 65535.

Table 250: Port Access Control Status Fields (Cont.)

Field	Description
Maximum Requests	Displays the configured maximum requests for the selected port. The maximum requests value is the maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The maximum requests value is in the range of 1 and 10.
VLAN Assigned	Displays the VLAN ID assigned to the selected interface by the Authenticator. Note: This field is displayed only when the port control mode of the selected interface is not MAC-based.
VLAN Assigned Reason	Displays the reason for the VLAN ID assigned by the authenticator to the selected interface. Possible values are: <ul style="list-style-type: none"> • Radius • Unauth • Default • Not Assigned Note: This field is displayed only when the port control mode of the selected interface is not MAC-based.
Reauthentication Period	Displays the configured reauthentication period for the selected port. The reauthentication period is the value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauthentication period is a value in the range of 1 and 65535.
Reauthentication Enabled	Displays if reauthentication is enabled on the selected port. This is a configurable field. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.
Key Transmission Enabled	This field displays if key transmission is enabled on the selected port. This is not a configurable field. The possible values are 'true' and 'false'. If the value is 'false', key transmission will not occur. Otherwise, key transmission is supported on the selected port.
Control Direction	This displays the control direction for the specified port. The control direction dictates the degree to which protocol exchanges take place between Supplicant and Authenticator. This affects whether the unauthorized controlled port exerts control over communication in both directions (disabling both incoming and outgoing frames) or just in the incoming direction (disabling only the reception of incoming frames). Note: This field is not configurable on some platforms.
Maximum Users	Displays the maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This field is configurable. The maximum users value is in range of 1 to 16.
Unauthenticated VLAN ID	Displays the Unauthenticated VLAN ID for the selected port. The valid range is 0 to 3965.
Session Timeout	Displays the Session Timeout set by the RADIUS Server for the selected port. Note: This field is displayed only when the port control mode of the selected port is not MAC-based.

Table 250: Port Access Control Status Fields (Cont.)

Field	Description
Session Termination Action	<p>Displays the Termination Action set by the RADIUS Server for the selected port. Possible values are:</p> <ul style="list-style-type: none"> • Default • Reauthenticate <p>If the termination action is Default then, at the end of the session, the client details are initialized. Otherwise, re-authentication is attempted.</p> <p>Note: This field is displayed only when the port control mode of the selected port is not MAC-based.</p>
Logical Port	<p>Displays the logical port number associated with the supplicant that is connected to the port. This field is not configurable.</p> <p>Note: This field is displayed when the port control mode of the selected port is MAC-based.</p>
Supplicant MacAddress	<p>This field displays the supplicant's MAC address that is connected to the port. This field is not configurable.</p> <p>Note: This field is displayed when the port control mode of the selected port is MAC-based.</p>

Port Summary

Use the Port Access Control Port Summary page to view summary information about the port access control settings on all physical ports.

To access the Port Based Access Control Port Summary page, click **Security > Port Based Access Control > Port Summary** in the navigation menu.

Interface	Control Mode	Operating Control Mode	Re-authentication Enabled	Port Status
0/1	Auto	Auto	FALSE	Authorized
0/2	Auto	N/A	FALSE	N/A
0/3	Auto	N/A	FALSE	N/A
0/4	Auto	N/A	FALSE	N/A
0/5	Auto	N/A	FALSE	N/A
0/6	Auto	N/A	FALSE	N/A
0/7	Auto	N/A	FALSE	N/A
0/8	Auto	N/A	FALSE	N/A
0/9	Auto	N/A	FALSE	N/A
0/10	MAC Based	N/A	FALSE	N/A
0/11	Auto	N/A	FALSE	N/A

Figure 298: Port Access Control Port Summary

Table 251: Port Access Control Port Summary Fields

Field	Description
Interface	Selects the Unit and Port to view.
Control Mode	Displays the port authorization state. The possible field values are: <ul style="list-style-type: none"> • Auto: Automatically detects the mode of the interface. • Force Authorized: Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port-based authentication. • Force Unauthorized: Denies the selected interface system access by moving the interface into unauthorized state. The switch cannot provide authentication services to the client through the interface. • MAC-based: Sets the mode of the interface to authentication on a per supplicant basis.
Operating Control Mode	Indicates the control mode under which the port is actually operating. Possible values are as follows: <ul style="list-style-type: none"> • ForceUnauthorized • ForceAuthorized • Auto • MAC-based • N/A: If the port is in detached state it cannot participate in port access control.
Reauthentication Enabled	Displays whether reauthentication is enabled on the port. This is a configurable field. The possible values are as follows: <ul style="list-style-type: none"> • True: Reauthentication will occur. • False: Reauthentication will not be allowed.
Port Status	Shows the authorization status of the port, which might be Authorized, Unauthorized or N/A. The value is N/A if the port is in detached state and cannot participate in port access control.

- Click **Refresh** to update the information on the screen.

Port Access Control Statistics

Use the Port Access Control Statistics page to view EAP and EAPOL information on a specific port.

To access the Port Based Access Control Statistics page, click **Security > Port Based Access Control > Statistics** in the navigation menu.

Authenticator Port Access Control Statistics	
EAPOL Frames Received	0
EAPOL Frames Transmitted	0
EAPOL Start Frames Received	0
EAPOL Logoff Frames Received	0
Last EAPOL Frame Version	0
Last EAPOL Frame Source	00:00:00:00:00:00
EAP Response/ID Frames Received	0
EAP Response Frames Received	0
EAP Request/ID Frames Transmitted	0
EAP Request Frames Transmitted	0
Invalid EAPOL Frames Received	0
EAPOL Length Error Frames Received	0

Figure 299: Port Access Control Statistics

Table 252: Port Access Control Statistics Fields

Field	Description
Interface	Selects the port to be displayed. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected port. All physical interfaces are valid.
EAPOL Frames Received	Displays the number of valid EAPOL frames received on the port.
EAPOL Frames Transmitted	Displays the number of EAPOL frames transmitted via the port.
EAPOL Start Frames Received	Displays the number of EAPOL Start frames received on the port.
EAPOL Logoff Frames Received	Displays the number of EAPOL Log off frames that have been received on the port.
Last EAPOL Frames Version	Displays the protocol version number attached to the most recently received EAPOL frame.
Last EAPOL Frames Source	Displays the source MAC Address attached to the most recently received EAPOL frame.
EAP Response/ID Frames Received	Displays the number of EAP Respond ID frames that have been received on the port.
EAP Response Frames Received	Displays the number of valid EAP Respond frames received on the port.

Table 252: Port Access Control Statistics Fields (Cont.)

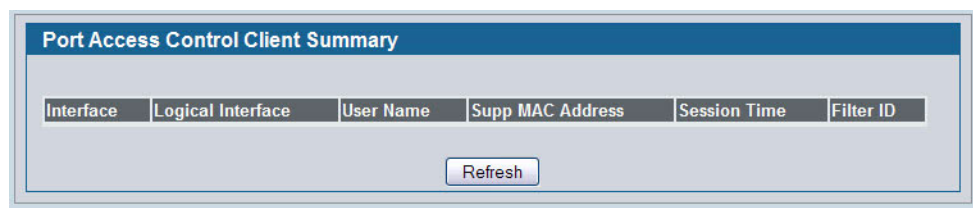
Field	Description
EAP Request/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted via the port.
EAP Request Frames Transmitted	Displays the number of EAP Request frames transmitted via the port.
Invalid EAPOL Frames Received	Displays the number of unrecognized EAPOL frames received on this port.
EAPOL Length Error Frames Received	Displays the number of EAPOL frames with an invalid Packet Body Length received on this port.

- Click **Refresh** to update the information on the page.
- Click **Clear All** to reset all statistics for all ports to 0. There is no confirmation prompt. When you click this button, the statistics are immediately cleared.
- Click **Clear** to reset the statistics for the selected port. There is no confirmation prompt. When you click this button, the statistics are immediately cleared.

Client Summary

Use the Port Access Control Client Summary page to view summary information about the supplicant device.

To access the Port Access Control Client Summary page, click **Security > Port Access Control > Client Summary** in the navigation menu.

**Figure 300: Port Access Control Client Summary****Table 253: Port Access Control Client Summary Fields**

Field	Description
Interface	Displays the interface address of the supplicant device.
User Name	Displays the user name representing the supplicant device.
Supp Mac Address	Displays the supplicant device's MAC address.
Session Time	Displays the time since the supplicant logged in. The value is in seconds.
Filter ID	The policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID	The VLAN ID assigned by the authenticator to the supplicant device.

- Click **Refresh** to refresh the page with the most current data from the switch.

Port Access Privileges

Use the Port Access Control Privileges page to grant or deny port access to users configured on the system.

To access the Port Based Access Control Privileges page, click **LAN > Security > Port Access Control > Port Access Privileges** in the navigation menu.

Figure 301: Port Access Privileges

Table 254: Port Access Privileges Fields

Field	Description
Port	Selects the port to grant or deny access. To grant or deny port access privileges to a user on all ports, select All from the drop-down menu.
Users	Lists the users configured on the system. The users that are highlighted have access to the selected port. By default, all users have access to all ports. To deny access to a port, Shift + click to select only the users to allow access. Make sure the username to deny port access is not selected, and then click Submit .

TACACS+ Settings

D-Link DWS-4000 Series switch provides Terminal Access Controller Access Control System (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication:** Provides authentication during login and via user names and user-defined passwords.
- **Authorization:** Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS+ server checks the user privileges.

The TACACS+ protocol ensures network security through encrypted protocol exchanges between the device and TACACS+ server.

TACACS+ Configuration

The TACACS+ Configuration page contains the TACACS+ settings for communication between the switch and the TACACS+ server you configure.

To display the TACACS+ Configuration page, click **LAN > Security > TACACS+ > Configuration** in the navigation menu.

Figure 302: TACACS+ Configuration

Table 255: TACACS+ Configuration Fields

Field	Description
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The valid range is 0-128 characters. The key must match the key configured on the TACACS+ server.
Connection Timeout	The maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server.

- If you make any changes to the page, click **Submit** to apply the new settings to the system.

TACACS+ Server Configuration

Use the TACACS+ Server Configuration page to configure up to five TACACS+ servers with which the switch can communicate.

To display the TACACS+ Server Configuration page, click **LAN > Security > TACACS+ > Server Configuration** in the navigation menu.

Figure 303 shows the TACACS+ Accounting Server Configuration page when no TACACS+ servers are configured or when you select **Add** from the **TACACS+ Server** field.

The screenshot shows a web interface titled "TACACS+ Server Configuration". It features a dropdown menu labeled "TACACS+ Server" with "Add" selected. Below it is a text input field labeled "Server Address" which is currently empty. At the bottom of the configuration area is a "Submit" button.

Figure 303: TACACS+ Configuration—No Server

After you add one or more TACACS+ servers, additional fields appear on the TACACS+ Server Configuration page.

Table 256: TACACS+ Configuration Fields

Field	Description
TACACS+ Server	Use the drop-down menu to select the IP address of the TACACS+ server to view or configure. If fewer than five TACACS+ servers are configured on the system, the Add option is also available. Select Add to configure additional TACACS+ servers.
IP Address	Enter the IP address of the TACACS+ server to add. This field is only available when Add is selected in the TACACS+ Server field.
Port	The authentication port number through which the TACACS+ session occurs. The default is port 49, and the range is 0-65535.
Key String	Defines the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ server. The valid range is 0-128 characters.
Connection Timeout	The amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is from 1 to 30 seconds.

- Click **Refresh** to update the page with the most current information.
- If you make changes to the page, click **Submit** to apply the changes to the system.
- To delete a configured TACACS+ server, select the IP address of the server from the **RADIUS Server IP Address** drop-down menu, and then click **Remove**.

Section 9: Configuring the Wireless Features

The D-Link Unified Switch is a wireless local area network (WLAN) solution that enables WLAN deployment while providing state-of-the-art wireless networking features. It is a scalable solution that provides secure wireless connectivity and seamless layer 2 and layer 3 fast roaming for end users.

This section contains information about the features available in the WLAN folder, which includes the following:

- [Unified Wired and Wireless Access System Components](#)
- [Monitoring Status and Statistics](#)
- [Basic Setup](#)
- [AP Management](#)
- [Configuring Advanced Settings](#)
- [Configuring the Wireless Distribution System](#)
- [Locating WLAN Devices](#)
- [Visualizing the Wireless Network](#)

Unified Wired and Wireless Access System Components

The Unified Wired and Wireless Access System components include:

- D-Link DWS-4000 Series Unified Wireless Switch (UWS)
- DWL-8600AP Unified Access Point (UAP)
- DWL-6600AP UAP
- DWL-3600AP UAP

Each DWS-4000 Series switch can manage up to 64 UAPs. Each access point radio can handle up to 200 associated wireless clients, so a dual-radio AP can handle up to 400 wireless clients. The switch tracks the status and statistics for all associated WLAN traffic and devices.

To support larger networks wireless switches can be configured to belong to a cluster (peer group). Clusters can contain up to 8 switches that share various information about UAPs and their associated wireless clients. Each cluster can support up to 256 APs and a total of 8000 wireless clients. Switches within the cluster enable L3 roaming between managed APs in a routing configuration. This means that wireless clients can roam among the access points within the cluster without losing network connections. Additionally, you can push portions of the wireless configuration to one or more switches within the cluster.

One switch in the cluster is automatically elected or configured to be the Cluster Controller. The Cluster Controller gathers status and statistics about all APs and clients in the cluster so you can view network status information and manage all devices in the cluster from a single switch.

Devices in the wireless system can be directly connected to each other, separated by layer 2 bridges, or located in different IP subnets. Whether or not you have a cluster, the DWS-4000 Series switch can support a total of 8000 wireless clients.

D-Link DWS-4000 Series Unified Wireless Switch

The DWS-4000 Series switch handles Layer 2, 3, and 4 switching and routing functions for traffic on the wired and wireless LAN and manages up to 64 APs, based on the existing reference design. The DWS-4000 Series switch user interface allows you to configure and monitor all AP settings and maintain a consistent configuration among all APs in the network.

The DWS-4000 Series switch supports advanced data path connectivity, mobility control, security safeguards, control over radio and power parameters, and management features for both network and element control. The DWS-4000 Series switch allows you to control the discovery, validation, authentication, and monitoring of peer wireless switches, APs, and clients on the WLAN, including discovery and status of rogue APs and clients.

DWL-X600AP Unified Access Points

There are three access point models in the DWL-X600AP family of Unified Access Points (UAPs):

- The DWL-8600AP UAP is a dual-radio access point.
- The DWL-6600AP UAP is a dual-radio access point.
- The DWL-3600AP is a single-radio access point.

The DWL-X600AP models include the same set of software features. Any reference to the DWL-X600AP or UAP includes all three models.

The UAP can operate in one of two modes: Standalone Mode or Managed Mode. In Standalone Mode, the UAP acts as an individual access point in the network, and you manage it by connecting to the UAP and using the Administrator Web User Interface (UI), command-line interface (CLI) or SNMP. In Managed Mode, the UAP is part of the Unified Wired and Wireless Access System, and you manage it by using the DWS-4000 Series switch. If a UAP is in Managed Mode, the Administrator Web UI and SNMP services on the UAP are disabled. Access is limited to the CLI through a serial-cable connection.

The Standalone Mode is appropriate for small networks with only a few APs. The Managed Mode is useful for any size network. If you start out with APs in Standalone Mode, you can easily transition the APs to Managed Mode when you add a DWS-4000 Series switch to the network. By using the AP in Managed Mode, you can centralize AP management and streamline the AP upgrade process by pushing configuration profiles and software upgrades from the DWS-4000 Series switch to the managed APs.

The DWL-8600AP and DWL-6600AP each have two radios and are capable of broadcasting in the following wireless modes:

- IEEE 802.11b mode
- IEEE 802.11g mode
- IEEE 802.11a mode
- IEEE 802.11n mode (2.4 GHz and 5 GHz)

The DWL-3600AP has one radio and is capable of broadcasting in the following wireless modes:

- IEEE 802.11b mode
- IEEE 802.11g mode
- IEEE 802.11n mode (2.4 GHz)

The DWL-X600AP access points support up to 16 virtual access points (VAPs) per radio. The VAP feature allows you to segment each physical access point into multiple logical access points that each support a unique SSID, VLAN ID, and security policy.

DWS-4000 Series Switch and AP Discovery Methods

The DWS-4000 Series switch and AP can use the following methods to discover each other:

- [L2 Discovery](#)
- [IP Address of AP Configured in the Switch](#)
- [IP Address of Switch Configured in the AP](#)



Note: For an AP to be managed by a switch, the managed mode on the AP must be enabled. To enable managed mode on the AP, log on to the AP CLI and use the `set managed-mode up` command or access the Administration Web UI and go to the Managed Access Point page and enable the Managed Mode option.



Note: The AP and the switch that should manage the AP cannot be separated by a Network Address Translation (NAT) device. The AP and switch exchange each other's IP addresses in the payload of the discovery and other messages. These addresses are then used for the subsequent communication between the switch and the AP. As those addresses do not undergo translation, the switch and AP will fail to communicate. However, the switch and the AP will have no such communication issues for remote sites or branch offices that are connected by Virtual Private Network (VPN). VPN functionality is already commonly found on firewalls. This issue can be resolved by setting up VPN access between the networks that use NAT.

L2 Discovery

When the AP and DWS-4000 Series switch are directly connected or in the same layer 2 broadcast domain and use the default VLAN settings, the DWS-4000 Series switch automatically discovers the AP through its broadcast of a L2 discovery message. The L2 discovery works automatically when the devices are directly connected or connected by using a layer 2 bridge.

For more information about L2 Discovery, see [“L2/VLAN Discovery” on page 536](#).

IP Address of AP Configured in the Switch

If APs are in a different broadcast domain than the DWS-4000 Series switch or use different management VLANs, You can add the IP addresses of the APs to the L3 Discovery list on the switch. The DWS-4000 Series switch sends UDP discovery messages to the IP addresses in its list. When the AP receives the messages and decides that it can connect to the switch, it initiates an SSL TCP connection to the switch.

For more information about configuring the IP address of the AP in the switch, see [“L3/IP Discovery” on page 535](#).

IP Address of Switch Configured in the AP

You can connect to the access point in Standalone mode and statically configure the IP addresses or DNS name of up to four switches that are allowed to manage the AP.

The AP sends a UDP discovery message to the first IP address configured in its list. When the switch receives the message, it verifies that the vendor ID on the AP is valid, there is no existing SSL TCP connection to the access point, and the maximum number of managed APs has not been reached. If all these conditions are met then the switch sends an invitation message to the AP to start the SSL TCP connection.

If the AP does not receive an invitation from the first DWS-4000 Series switch configured in its list, it sends a UDP discovery message to the second DWS-4000 Series switch configured in the list five seconds after sending the message to the first DWS-4000 Series switch.

When an IP address of a DWS-4000 Series switch is configured on the AP, the AP only associates with that switch even if other switches discover the AP by using other mechanisms.



Note: For this method to work, the AP must be able to find a route to the Unified Switch.

To use the access point Web interface to configure the switch IP address information, use a Web browser to log onto the AP and go to the **Managed Access Point** page. Enter the information into the available fields and click **Update**.

To use the CLI to configure the switch IP address information in the AP, use the following procedures:

1. Use a serial or Telnet connection to log on to the access point.
2. Use the `set managed-ap switch-address-<1-4>` to enter the IP address of up to four switches that are permitted to manage the AP.

For example, to enter a switch with an IP address of 192.168.66.202 and a switch with an IP address of 192.168.19.242, use the following commands:

```
WLAN-AP# set managed-ap switch-address-1 192.168.66.202
WLAN-AP# set managed-ap switch-address-2 192.168.19.242
```

3. Use the `get managed-ap` command to verify that the information you entered is correct.

```
WLAN-AP# get managed-ap
Property                               Value
-----
mode                                    up
ap-state                                down
switch-address-1                        192.168.66.202
```



```

switch-address-2      192.168.19.242
switch-address-3
switch-address-4
dhcp-switch-address-1
dhcp-switch-address-2
dhcp-switch-address-3
dhcp-switch-address-4
managed-mode-watchdog 0

```

Configuring the DHCP Option

You can configure the IP address of the DWS-4000 Series switch as an option in the DHCP response to the DHCP request that the AP sends the DHCP server.

The AP can learn up to four switch IP addresses or DNS names through DHCP option 43 (the Vendor Information option) in the DHCP response. If you configured a static IP address in the AP, the AP ignores DHCP option 43.

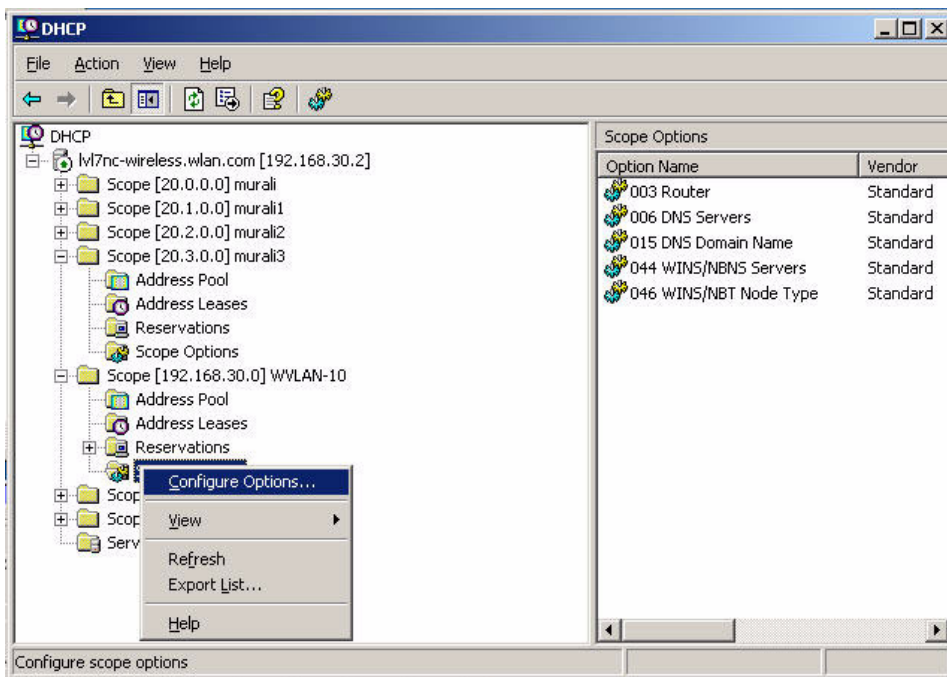


Note: This discovery method only works if you configure the DHCP option before the AP receives its network information from the DHCP server.

The format for DHCP option 43 values are defined by RFC 2132.

The procedures to add the DHCP option to the DHCP server depend on the type of DHCP server you use on your network. If you use a Microsoft Windows 2000 or Microsoft Windows 2003 DHCP Server, you configure the scope you use with the access points with DHCP Option 43, as the following procedures describe.

1. From the DHCP manager, right-click the applicable scope and select **Configure Options...**



2. From the Available Options list, scroll to Option 43 and select the **043 Vendor Specific Info** check box.

3. Enter the Option 43 data into the Data Entry field.

The format for DHCP option 43 values are defined by RFC 2132. To enter an IP address of 192.168.1.10 into the Binary column, you enter the data type code (01) and the address length (04), followed by the IP address in hexadecimal format. You repeat the data type and address length codes for each address you enter.

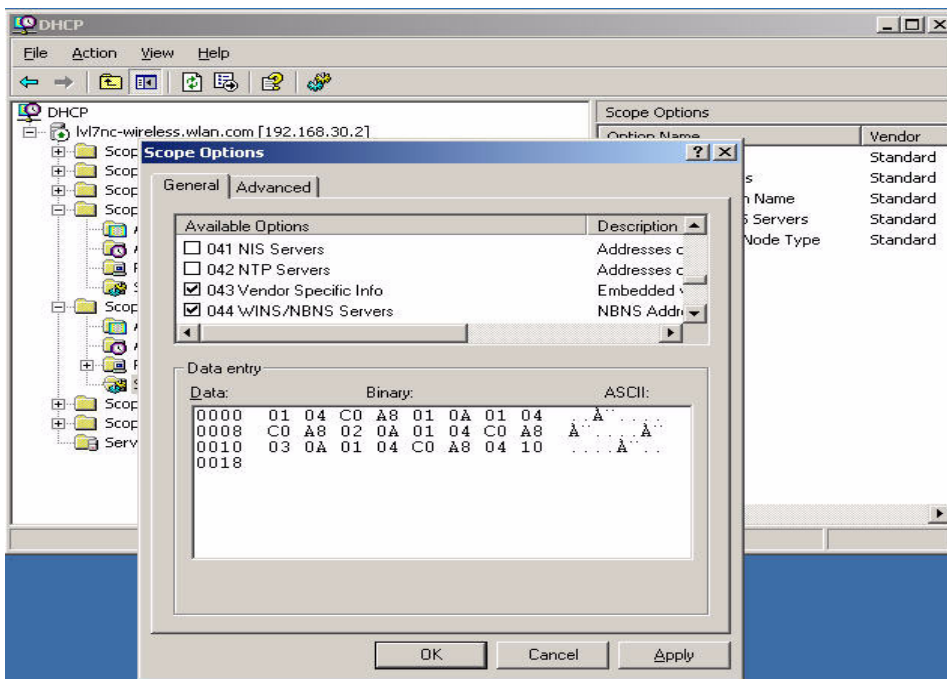


Note: If you do not know the hexadecimal format for a specific IP address, use an IP address converter (dotted decimal-to-hex) available on the Internet.

For example, to add the four switch IP addresses 192.168.1.10, 192.168.2.10, 192.168.3.10, and 192.168.4.16 to Option 43, you enter the following hexadecimal numbers into the Data Entry field:

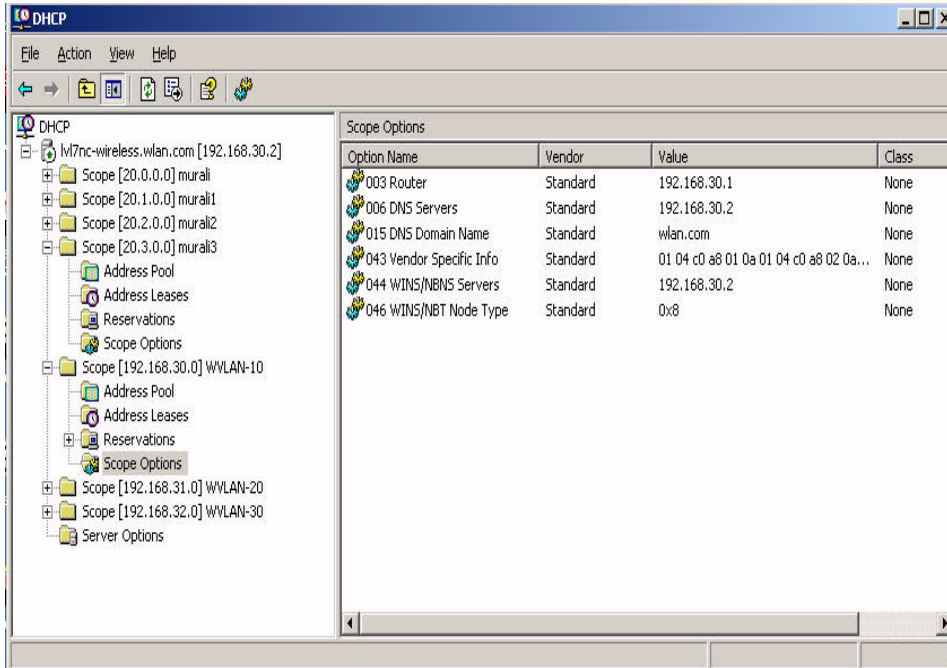
01 04 0C A8 01 0A 01 04 0C A8 02 0A 01 04 0C A8 03 0A 01 04 0C A8 04 10

The following image shows the four IP addresses entered into the Data Entry field on the Windows DHCP server.



4. Click OK.

The following figure shows a scope with Option 43 configured.



Discovery and Peer Switches

When multiple peer switches are present in the network, you can control which switch or switches are allowed to discover a particular AP by the discovery method you use.

If you want to make sure that an AP is discovered by one specific switch, use one of the following methods:

- Disable L2 Discovery on all switches and configure the IP address of the AP in only one DWS-4000 Series switch.
- Configure the IP address of one DWS-4000 Series switch in the AP.
- Configure the DHCP option 43 with the IP address of only one DWS-4000 Series switch.

An alternative approach is to configure the RADIUS server to return a switch IP address during AP MAC address checking in the AP authentication process. If the RADIUS server indicates that the AP is a valid managed AP and returns an IP address of a switch that is not the same as this switch, then the switch sends a re-link message to the access point with the IP address of the wireless switch to which the AP should be talking to. When the AP gets the re-link message it modifies or sets the wireless switch IP address, breaks the TCP connection with the current switch and starts a new discovery process.

You can configure the DWS-4000 Series switch so that each AP is allowed to be managed by any switch in a cluster. If the DWS-4000 Series switch that manages an AP goes down, one of the backup switches takes over the management responsibilities.

To use one or more switches as a backup for an AP, use one of the following discovery methods:

- If the AP and any of the peer switches are in the same L2 broadcast domain, L2 Discovery is enabled, and all the devices use the default VLAN settings, a peer switch will automatically discover the AP if the primary DWS-4000 Series switch becomes unavailable.
- Configure the IP address of the AP in multiple switches.
- Configure the IP address of up to four switches in the AP while it is in Standalone Mode.
- Configure the DHCP option 43 with the IP addresses of additional switches in the cluster.

Monitoring Status and Statistics

The Status/Statistics folder contains links to the following pages that help you monitor the status and statistics for your D-Link Unified Switch network:

- [Monitoring Status and Statistics](#)
- [Managed AP Status](#)
- [Associated Client Status/Statistics](#)
- [Peer Switch Status](#)
- [Radio Resource Measurement Status Information](#)

Wireless Global Status/Statistics

The DWS-4000 Series switch periodically collects information from the APs it manages and from associated peer switches. The information on the Global page shows status and statistics about the switch and all of the objects associated with it. You can access the global WLAN statistics by clicking **WLAN > Monitoring > Global**.

Global				Switch Status	IP Discovery	Configuration Received	AP Hardware Capability
Wireless Global Status/Statistics							
WLAN Switch Operational Status	Enabled	IP Address	10.27.65.126				
Peer Switches	1						
Cluster Controller	Yes	Cluster Controller IP Address	10.27.65.126				
Total Access Points	2	Managed Access Points	2				
Standalone Access Points	0	Rogue Access Points	5				
Discovered Access Points	0	Connection Failed Access Points	0				
Authentication Failed Access Points	4	Unknown Access Points	45				
Rogue AP Mitigation Limit	16	Rogue AP Mitigation Count	0				
Maximum Managed APs in Peer Group	256	WLAN Utilization	1 %				
Total Clients	1	Authenticated Clients	1				
802.11a Clients	0	802.11b/g Clients	0				
802.11n Clients	1	Maximum Associated Clients	8000				
Detected Clients	60	Maximum Detected Clients	16000				
Maximum Pre-authentication History Entries	500	Total Pre-authentication History Entries	0				
Maximum Roam History Entries	500	Total Roam History Entries	0				
AP Provisioning Count	6	Maximum AP Provisioning Entries	512				
RRM Channel Load History Entries	0	Maximum Channel Load History Entries	100				
WLAN Bytes Transmitted	78326494	WLAN Packets Transmitted	704014				
WLAN Bytes Received	9071542	WLAN Packets Received	82593				
WLAN Bytes Transmit Dropped	0	WLAN Packets Transmit Dropped	0				
WLAN Bytes Receive Dropped	0	WLAN Packets Receive Dropped	0				
Distributed Tunnel Packets Transmitted	0	Distributed Tunnel Roamed Clients	0				
Distributed Tunnel Clients	0	Distributed Tunnel Client Denials	0				
Total Voice Traffic Streams	0	Total Traffic Stream Clients	0				
Total Video Traffic Streams	0	Total Traffic Stream Roaming Clients	0				
TSPEC Statistics							
Access Category	Voice	Video					
Total TSPEC Packets Received	0	0					
Total TSPEC Packets Transmitted	0	0					
Total TSPEC Bytes Received	0	0					
Total TSPEC Bytes Transmitted	0	0					
Total TSPECs Accepted	0	0					
Total TSPECs Rejected	0	0					
Total Roaming TSPECs Accepted	0	0					
Total Roaming TSPECs Rejected	0	0					
<input type="button" value="Refresh"/> <input type="button" value="Clear Statistics"/>							

Figure 304: Global WLAN Status/Statistics

Table 257 on page 440 describes the fields on the **Wireless Global Status/Statistics** page.

Table 257: Global WLAN Status/Statistics

Field	Description
WLAN Switch Operational Status	<p>This status field displays the operational status of the WLAN Switch. The WLAN Switch may be configured as enabled, but is operationally disabled due to configuration dependencies. If the operational status is disabled, the reason will be displayed in the following status field.</p> <p>The WLAN Switch is composed of multiple components, and each component in the system must acknowledge an enable or disable of the WLAN Switch. During a transition the operational status might temporarily show a pending status.</p>
WLAN Switch Disable Reason	<p>If the status is disabled, this field appears and one of the following reasons is listed:</p> <ul style="list-style-type: none"> • None: The cause for the disabled status is unknown. • Administrator disabled: The Enable WLAN Switch option on the global configuration page has been cleared. • No IP Address: The WLAN interface does not have an IP address. • No SSL Files: The DWS-4000 Series switch communicates with the APs it manages by using Secure Sockets Layer (SSL) connections. The first time you power on the DWS-4000 Series switch, it automatically generates a server certificate that will be used to set up the SSL connections. The SSL certificate and key generation can take up to an hour to complete. <p>If routing is enabled on the switch, the operational status might be disabled due to one of the following reasons:</p> <ul style="list-style-type: none"> • No Loopback Interface: The switch does not have a loopback interface. • Global Routing Disabled: Even if the routing mode is enabled on the WLAN switch interface, it must also be enabled globally for the operational status to be enabled.
IP Address	IP address of the switch.
Peer Switches	Number of peer WLAN switches detected on the network.
Cluster Controller	<p>Indicates whether this switch is the Cluster Controller for the cluster.</p> <p>Among a group of peer switches, one of the switches is automatically elected or configured to be the Cluster Controller. The Cluster Controller gathers status and statistics about all APs and clients in the peer group.</p> <p>Note: Only the Cluster Controller switch can display managed APs, clients, statistics, and RF Scan databases for the whole cluster. The switches that are not Cluster Controllers can display information only about locally attached devices.</p>
Cluster Controller IP Address	The IP address of the peer switch that is the Cluster Controller.
Total Access Points	Total number of Managed APs in the database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.
Managed Access Points	Number of APs in the managed AP database that are authenticated, configured, and have an active connection with the Unified Switch.
Standalone Access Points	Number of trusted APs in Standalone mode. APs in Standalone mode are not managed by a switch.
Rogue Access Points	Number of Rogue APs currently detected on the WLAN. When an AP performs an RF scan, it might detect access points that have not been validated. It reports these APs as rogues.

Table 257: Global WLAN Status/Statistics (Cont.)

Field	Description
Discovered Access Points	APs that have a connection with the switch, but haven't been completely configured. This value includes all managed APs with a Discovered or Authenticated status.
Connection Failed Access Points	Number of APs that were previously authenticated and managed, but currently don't have connection with the Unified Switch.
Authentication Failed Access Points	Number of APs that failed to establish communication with the Unified Switch.
Unknown Access Points	Number of Unknown APs currently detected on the WLAN. If an AP configured to be managed by the Unified Switch is detected through an RF scan at any time that it is not actively managed it is classified as an Unknown AP.
Rogue AP Mitigation Limit	Maximum number of APs for which the system can send de-authentication frames.
Rogue AP Mitigation Count	Number of APs to which the wireless system is currently sending de-authentication messages to mitigate against rogue APs. A value of 0 indicates that mitigation is not in progress.
Maximum Managed APs in Peer Group	Maximum number of access points that can be managed by the cluster.
WLAN Utilization	Total network utilization across all APs managed by this switch. This is based on global statistics.
Total Clients	Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status.
Authenticated Clients	Total number of clients in the associated client database with an Authenticated status.
802.11a Clients	Total number of IEEE 802.11a only clients that are authenticated.
802.11b/g Clients	Total number of IEEE 802.11b/g only clients that are authenticated.
802.11n Clients	Total number of clients that are IEEE 802.11n capable and are authenticated. These include IEEE 802.11a/n, IEEE 802.11b/g/n, 5 GHz IEEE 802.11n, 2.4GHz IEEE 802.11n.
Maximum Associated Clients	Maximum number of clients that can associate with the wireless system. This is the maximum number of entries allowed in the Associated Client database.
Detected Clients	Number of wireless clients detected in the WLAN.
Maximum Detected Clients	Maximum number of clients that can be detected by the switch. The number is limited by the size of the Detected Client Database.
Maximum Pre-authentication History Entries	Maximum number of Client Pre-Authentication events that can be recorded by the system.
Total Pre-authentication History Entries	Current number of pre-authentication history entries in use by the system.
Maximum Roam History Entries	Maximum number of entries that can be recorded in the roam history for all detected clients.
Total Roam History Entries	Current number of roam history entries in use by the system.
AP Provisioning Count	Current number of AP provisioning entries configured on the system.

Table 257: Global WLAN Status/Statistics (Cont.)

Field	Description
Maximum AP Provisioning Entries	Number of AP provisioning entries that can be stored by the system.
RRM Channel Load History Entries	Current number of RRM channel load history entries in use by the system.
Maximum Channel Load History Entries	Number of channel load history entries that can be stored by the system.
WLAN Bytes Transmitted	Total bytes transmitted across all APs managed by the switch.
WLAN Packets Transmitted	Total packets transmitted across all APs managed by the switch.
WLAN Bytes Received	Total bytes received across all APs managed by the switch.
WLAN Packets Received	Total packets received across all APs managed by the switch.
WLAN Bytes Transmit Dropped	Total bytes transmitted across all APs managed by the switch that were dropped.
WLAN Packets Transmit Dropped	Total packets transmitted across all APs managed by the switch that were dropped.
WLAN Bytes Receive Dropped	Total bytes received across all APs managed by the switch that were dropped.
WLAN Packets Receive Dropped	Total packets received across all APs managed by the switch that were dropped.
Distributed Tunnel Packets Transmitted	Total number of packets sent by all APs via distributed tunnels.
Distributed Tunnel Roamed Clients	Total number of clients that successfully roamed away from Home AP using distributed tunneling.
Distributed Tunnel Clients	Total number of clients that are associated with an AP that are using distributed tunneling.
Distributed Tunnel Client Denials	Total number of clients for which the system was unable to set up a distributed tunnel when client roamed.
Total Voice Traffic Streams	Shows the number of voice traffic streams being transmitted by wireless clients that are connected to the network through APs managed by this switch. Note: A traffic stream is a collection of data packets identified by the AP as belonging to a particular user priority.
Total Video Traffic Streams	Shows the number of video traffic streams being transmitted by wireless clients that are connected to the network through APs managed by this switch.
Total Traffic Stream Clients	Shows the number of wireless clients currently transmitting traffic streams.
Total Traffic Stream Roaming Clients	Shows the number of wireless clients with a roaming status that are currently transmitting traffic streams.

Table 257: Global WLAN Status/Statistics (Cont.)

Field	Description
TSPEC Statistics (Voice and Video)	
Total TSPEC Packets Received	The number of TSPEC packets sent from the wireless client to the AP. The number is a total for all APs managed by the switch.
Total TSPEC Packets Transmitted	The number of TSPEC packets sent from the AP to the wireless client. The number is a total for all APs managed by the switch.
Total TSPEC Bytes Received	The number of TSPEC bytes sent from the wireless client to the AP. The number is a total for all APs managed by the switch.
Total TSPEC Bytes Transmitted	The number of TSPEC bytes sent from the AP to the wireless client. The number is a total for all APs managed by the switch.
Total TSPECs Accepted	The number of TSPEC packets that were accepted by all APs that the switch manages.
Total TSPECs Rejected	The number of TSPEC packets that were rejected by all APs that the switch manages.
Total Roaming TSPECs Accepted	The total number of TSPEC packets transmitted by roaming clients that were accepted by all APs that the switch manages.
Total Roaming TSPECs Rejected	The total number of TSPEC packets transmitted by roaming clients that were rejected by all APs that the switch manages.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Clear Statistics**—Reset all counters on the page to zero.

Viewing Switch Status and Statistics Information

The **Switch Status/Statistics** page for each switch provides information about the access points it manages and their associated clients. If the switch is the Cluster Controller, it provides the switch status and statics information about each switch in its group.



Note: Only the Cluster Controller switch can display managed APs, clients, statistics, and RF Scan database information for the whole cluster. The switches that are not Cluster Controllers can display information about locally attached devices.

Use the drop-down menu to select the switch with the information to display. If the local switch is the only available option, then it is the only switch in the cluster, or it is not a Cluster Controller.

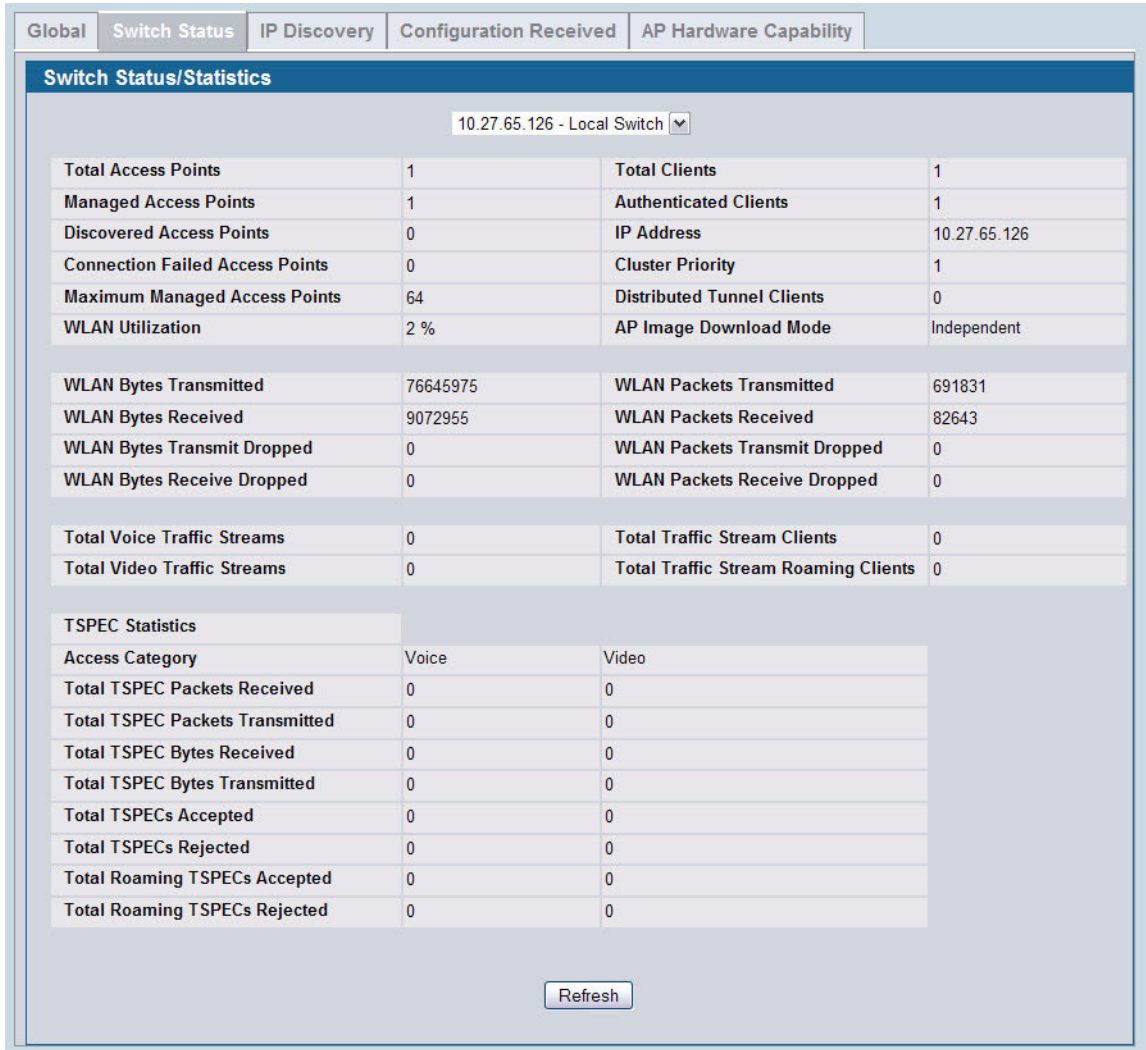


Figure 305: Switch Status/Statistics

Table 257 on page 440 describes the fields on the **Wireless Global Status** page.

Table 258: Switch Status/Statistics

Field	Description
Total Access Points	Total number of Managed APs in the database. This value is always equal to the sum of Managed Access Points, Connection Failed Access Points, and Discovered Access Points.
Managed Access Points	Number of APs in the managed AP database that are authenticated, configured, and have an active connection with the wireless switch.
Discovered Access Points	APs that have a connection with the switch, but haven't been completely configured. This value includes all managed APs with a Discovered or Authenticated status.
Connection Failed Access Points	Number of APs that were previously authenticated and managed, but currently don't have connection with the wireless switch.

Table 258: Switch Status/Statistics

Field	Description
Maximum Managed Access Points	Maximum number of access points that can be managed by the switch.
WLAN Utilization	Total network utilization across all APs managed by this switch. This is based on global statistics.
Total Clients	Total number of clients in the database. This total includes clients with an Associated, Authenticated, or Disassociated status.
Authenticated Clients	Total number of clients in the associated client database with an Authenticated status.
IP Address	IP address of the switch.
Cluster Priority	Cluster priority value of the switch. The switch with highest priority in a cluster becomes the Cluster Controller. If the priority is the same then the switch with lowest IP address becomes the Cluster Controller. A priority of 0 means that the switch cannot become the Cluster Controller.
Distributed Tunnel Clients	Total number of clients that are associated with an AP that are using distributed tunneling.
WLAN Bytes Transmitted	Total bytes transmitted across all APs managed by the switch.
WLAN Bytes Received	Total bytes received across all APs managed by the switch.
WLAN Bytes Transmit Dropped	Total bytes transmitted across all APs managed by the switch that were dropped.
WLAN Bytes Received Dropped	Total bytes received across all APs managed by the switch that were dropped.
WLAN Packets Transmitted	Total packets transmitted across all APs managed by the switch.
WLAN Packets Received	Total packets received across all APs managed by the switch.
WLAN Packets Transmit Dropped	Total packets transmitted across all APs managed by the switch that were dropped.
WLAN Packets Receive Dropped	Total packets received across all APs managed by the switch that were dropped.
Total Voice Traffic Streams	Shows the number of voice traffic streams being transmitted by wireless clients that are connected to the network through APs managed by this switch. Note: A traffic stream is a collection of data packets identified by the AP as belonging to a particular user priority.
Total Video Traffic Streams	Shows the number of video traffic streams being transmitted by wireless clients that are connected to the network through APs managed by this switch.
Total Traffic Stream Clients	Shows the number of wireless clients currently transmitting traffic streams.
Total Traffic Stream Roaming Clients	Shows the number of wireless clients with a roaming status that are currently transmitting traffic streams.

Table 258: Switch Status/Statistics

Field	Description
TSPEC Statistics (Voice and Video)	
Total TSPEC Packets Received	The number of TSPEC packets sent from the wireless client to the AP. The number is a total for all APs managed by the switch.
Total TSPEC Packets Transmitted	The number of TSPEC packets sent from the AP to the wireless client. The number is a total for all APs managed by the switch.
Total TSPEC Bytes Received	The number of TSPEC bytes sent from the wireless client to the AP. The number is a total for all APs managed by the switch.
Total TSPEC Bytes Transmitted	The number of TSPEC bytes sent from the AP to the wireless client. The number is a total for all APs managed by the switch.
Total TSPECs Accepted	The number of TSPEC packets that were accepted by all APs that the switch manages.
Total TSPECs Rejected	The number of TSPEC packets that were rejected by all APs that the switch manages.
Total Roaming TSPECs Accepted	The total number of TSPEC packets transmitted by roaming clients that were accepted by all APs that the switch manages.
Total Roaming TSPECs Rejected	The total number of TSPEC packets transmitted by roaming clients that were rejected by all APs that the switch manages.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing IP Discovery Status

From the **WLAN > Monitoring > Global > IP Discovery** tab, you can view information about communication with the devices in the IP discovery list on the **WLAN > Administration > Basic Setup > Discovery** page.

The IP Discovery list can contain the IP addresses of peer switches and APs for the UWS to discover and associate with as part of the WLAN.

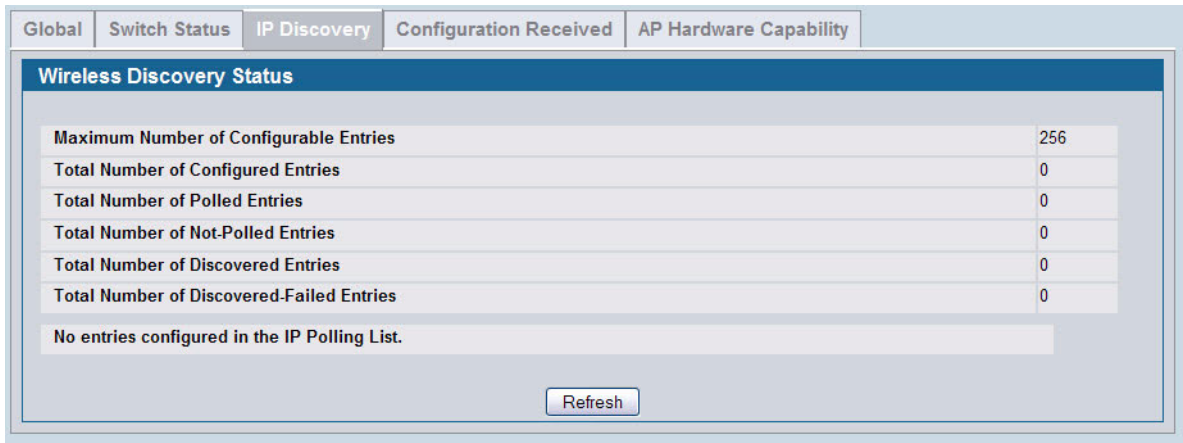


Figure 306: Wireless Discovery Status

Table 259: AP Hardware Capability Radio Detail

Field	Description
Maximum Number of Configurable Entries	Shows the maximum number of IP addresses that can be configured in the IP Discovery list.
Total Number of Configured Entries	Shows the number of IP addresses that have been configured in the IP Discovery list.
Total Number of Polled Entries	Identifies how many of the IP addresses in the IP Discovery list the switch has attempted to contact.
Total Number of Not-Polled Entries	Identifies how many of the IP addresses in the IP Discovery list the switch has not attempted to contact.
Total Number of Discovered Entries	Identifies how many devices (peer switches or APs) the switch has successfully discovered, authenticated, and validated by polling the IP address configured in the IP Discovery list.
Total Number of Discovered-Failed Entries	Identifies how many devices that have an IP address configured in the IP Discovery list that the switch has attempted to contact and failed to authenticate or validate.

Table 259: AP Hardware Capability Radio Detail (Cont.)

Field	Description
IP Address	Shows the IP address of the device configured in the IP Discovery list.
Status	<p>The status is in one of the following states:</p> <ul style="list-style-type: none">• Not Polled: The switch has not attempted to contact the IP address in the L3/IP Discovery list.• Polled: The switch has attempted to contact the IP address.• Discovered: The switch contacted the peer switch or the AP in the L3/IP Discovery list and has authenticated or validated the device.• Discovered - Failed: The switch contacted the peer switch or the AP with IP address in the L3/IP Discovery list and was unable to authenticate or validate the device. <p>If the device is an access point, an entry appears in the AP failure list with a failure reason.</p>

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing the Peer Switch Configuration Received Status

The Peer Switch Configuration feature allows you to send the critical wireless configuration from one switch to all other switches. In addition to keeping the switches synchronized, this function enables the administrator to manage all wireless switches in the cluster from one switch. The **Peer Switch Configuration Received Status** page provides information about the configuration a switch has received from one of its peers.

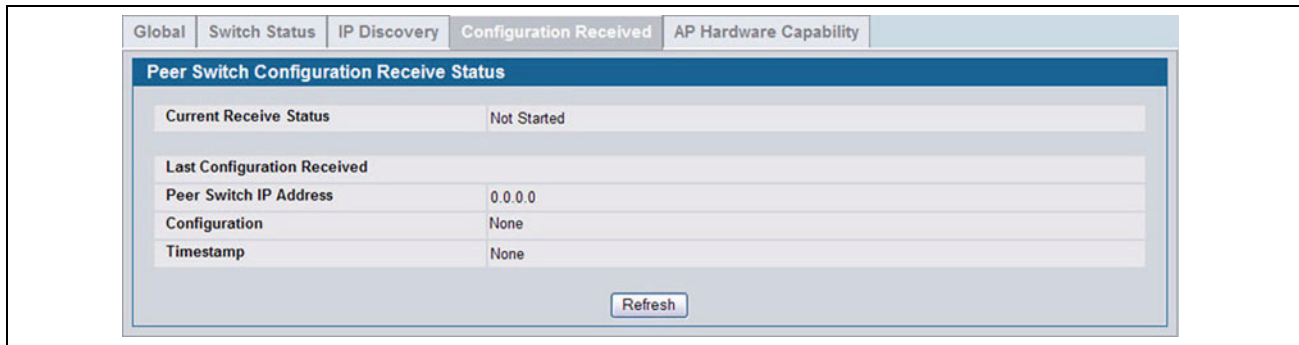


Figure 307: Configuration Received

[Table 257](#) describes the fields on the **Wireless Global Status** page.

Table 260: Peer Switch Configuration

Field	Description
Current Receive Status	Indicates the global status when wireless configuration is received from a peer switch. The possible status values are as follows: <ul style="list-style-type: none"> • Not Started • Receiving Configuration • Saving Configuration, • Applying AP Profile Configuration • Success • Failure - Invalid Code Version • Failure - Invalid Hardware Version • Failure - Invalid Configuration
Last Configuration Received	
Peer Switch IP Address	Indicates the last switch from which this switch received any wireless configuration data.

Table 260: Peer Switch Configuration (Cont.)

Field	Description
Configuration	<p>Indicates which portions of configuration were last received from a peer switch, which can be one or more of the following:</p> <ul style="list-style-type: none"> • Global • Discovery • Channel/Power • AP Database • AP Profiles • Known Client • Captive Portal • RADIUS Client • QoS ACL • QoS DiffServ <p>If the switch has not received any configuration for another switch, the value is None.</p>
Timestamp	Indicates the last time this switch received any configuration data from a peer switch.

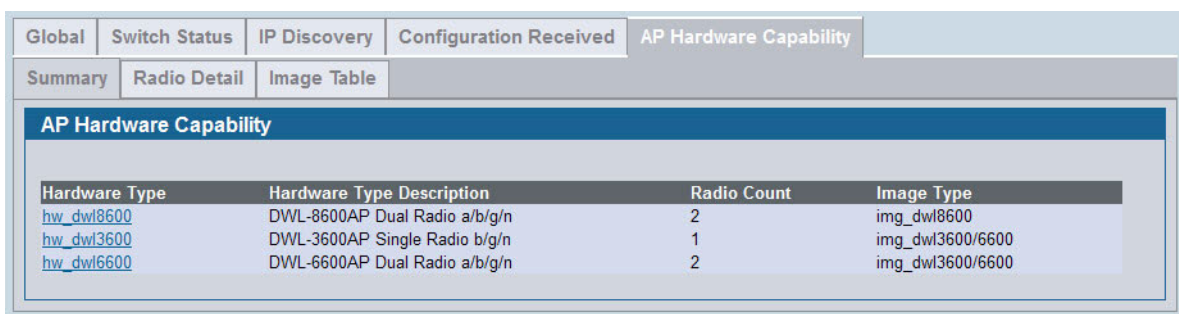
Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing the AP Hardware Capability List

The switch can support APs that have different hardware capabilities, such as the supported number of radios, the supported IEEE 802.11 modes, and the software image required by the AP. From the AP Hardware Capability tab, you can access summary information about the AP Hardware support, the radios and IEEE modes supported by the hardware, and the software images that are available for download to the APs.



Hardware Type	Hardware Type Description	Radio Count	Image Type
hw_dw18600	DWL-8600AP Dual Radio a/b/g/n	2	img_dw18600
hw_dw3600	DWL-3600AP Single Radio b/g/n	1	img_dw3600/6600
hw_dw6600	DWL-6600AP Dual Radio a/b/g/n	2	img_dw3600/6600

Figure 308: AP Hardware Capability Information

Table 261 describes the fields available on the AP Hardware Capabilities page.

Table 261: AP Hardware Capability Summary

Field	Description
Hardware Type	Identifies the ID number assigned to each AP hardware type. The switch supports up to six different AP hardware types.
Hardware Type Description	Includes a description of the platform and the supported IEEE 802.11 modes.
Radio Count	Specifies whether the hardware supports one radio or two radios.
Image Type	Specifies the type of software the hardware requires.

AP Hardware Radio Capability

Use the **Radio Detail** tab under the **Hardware Capabilities** tab to view radio details.

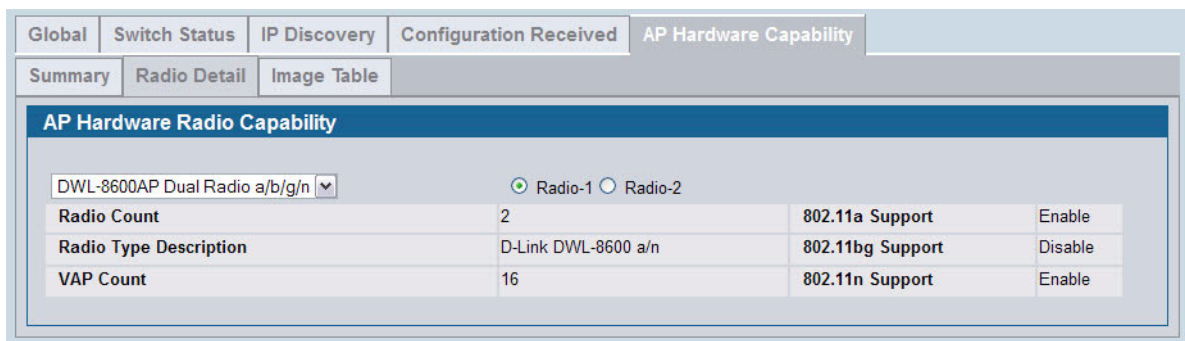


Figure 309: Radio Detail

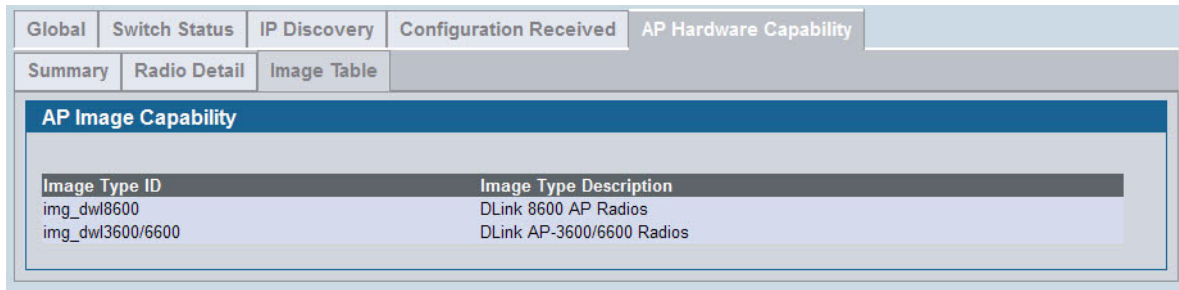
Table 262 on page 451 describes the fields available on the AP Hardware Radio Capability page.

Table 262: AP Hardware Capability Radio Detail

Field	Description
AP Selector	Use the drop-down menu to select the AP model.
Radio Selector	If the selected AP is a dual-radio AP, select Radio-1 or Radio-2 to view information about the selected radio.
Radio Count	Displays the number of radios supported on the hardware platform, which is either 1 or 2.
Radio Type Description	Displays the type of radio, which might contain information such as the manufacturer name and supported IEEE 802.11 modes.
VAP Count	Displays the number of VAPs the radio supports.
802.11a Support	Shows whether support for IEEE 802.11a mode is enabled.
802.11bg Support	Shows whether support for IEEE 802.11bg mode is enabled.
802.11n Support	Shows whether support for IEEE 802.11n mode is enabled.

AP Image Capability

The switch is able to update software on the access points that it manages. To update the AP with the correct software, the UWS can store up to three AP software images to support different AP hardware types. This page displays the image ID-to-hardware type mapping.



AP Image Capability	
Image Type ID	Image Type Description
img_dw18600	DLink 8600 AP Radios
img_dw3600/6600	DLink AP-3600/6600 Radios

Figure 310: Image Table

Table 263: AP Image Capability

Field	Description
Image Type ID	Shows the ID number assigned to the image.
Image Type Description	Provides a basic description of the image.

Peer Switch Status

The **Peer Switch Status** page provides information about other Unified Wireless Switches in the network. To access the peer switch information, click **WLAN > Monitoring > Peer Switch**.

Peer wireless switches within the same cluster exchange data about themselves, their managed APs, and clients. The switch maintains a database with this data so you can view information about a peer, such as its IP address and software version. If the switch loses contact with a peer, all of the data for that peer is deleted.

One switch in a cluster is elected as a Cluster Controller. The Cluster Controller collects status and statistics from all the other switches in the cluster, including information about the APs peer switches manage and the clients associated to those APs.

Peer Switch Status						
Cluster Controller IP Address	10.27.65.126					
Peer Switches	1					
IP Address	Vendor ID	Software Version	Protocol Version	Discovery Reason	Managed AP Count	Age
10.27.65.136	D-Link	D.6.27.1	2	L2 Poll	1	0d:00:01:11

Figure 311: Peer Switch Status

Table 264: Peer Switch Status

Field	Description
Cluster Controller IP Address	IP address of the switch that controls the cluster.
Peer Switches	Displays the number of peer switches in the cluster.
IP Address	IP address of the peer wireless switch in the cluster.
Vendor ID	Vendor ID of the peer switch software.
Software Version	The software version for the given peer switch.
Protocol Version	Indicates the protocol version supported by the software on the peer switch.
Discovery Reason	The discovery method of the given peer switch, which can be through an L2 Poll or IP Poll
Managed AP Count	Shows the number of APs that the switch currently manages.
Age	Time since last communication with the switch in Hours, Minutes, and Seconds.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Peer Switch Configuration Status

You can push portions of the switch configuration from one switch to another switch in the cluster. The **Peer Switch Configuration Status** page displays information about the configuration sent by a peer switch in the cluster. It also identifies the IP address of each peer switch that received the configuration information.



Note: To view information about the configuration received by the local switch, go to the **WLAN > Monitoring > Global** page and click the Configuration Received tab.

Peer IP Address	Configuration Switch IP Address	Configuration	Timestamp
10.27.65.76	0.0.0.0	None	JAN 01 00:00:00 1970

Figure 312: Peer Switch Configuration Status

Table 265 describes the fields available on the **Peer Switch Status** page.

Table 265: Peer Switch Configuration Status

Field	Description
Peer IP Address	Shows the IP address of each peer wireless switch in the cluster that received configuration information.
Configuration Switch IP Address	Shows the IP Address of the switch that sent the configuration information.
Configuration	Identifies which parts of the configuration the switch received from the peer switch. The possible configuration elements can be one or more of the following: <ul style="list-style-type: none"> • Global • Discovery • Channel/Power • AP Database • Channel/Power • AP Profiles • Known Client • Captive Portal • RADIUS Client • QoS ACL • QoS DiffServ If the switch has not received any configuration for another switch, the value is None.
Timestamp	Shows when the configuration was applied to the switch. The time is displayed as UTC time and therefore only useful if the administrator has configured each peer switch to use NTP

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Peer Switch Managed AP Status

The **Peer Switch Managed AP Status** page displays information about the APs that each peer switch in the cluster manages. Use the menu above the table to select the peer switch with the AP information to display. Each peer switch is identified by its IP address.

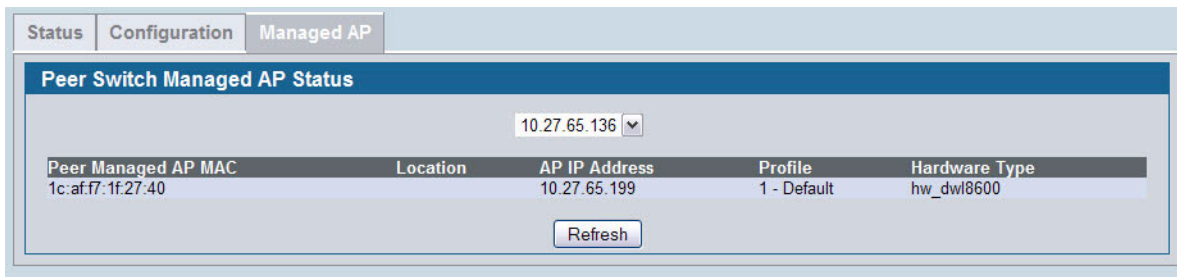


Figure 313: Peer Switch Managed AP Status

[Table 266](#) describes the fields available on the **Peer Switch Managed AP Status** page.

Table 266: Peer Switch Managed AP Status

Field	Description
Switch Selector	Select the IP address of the peer switch with the information to view or select All to view information about all APs managed by peer switches in the cluster.
Peer Managed AP MAC	Shows the MAC address of each AP managed by the peer switch.
Peer Switch IP Address	Shows the IP address of the peer switch that manages the AP. This field displays when All is selected from the drop-down menu.
Location	The descriptive location configured for the managed AP.
AP IP Address	The IP address of the AP.
Profile	The AP profile applied to the AP by the switch.
Hardware Type	The Hardware ID associated with the AP hardware platform .

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

All AP Status

The **All AP Status** page shows summary information about managed, failed, and rogue access points the switch has discovered or detected.

MAC address	Location	Switch Port	IP Address	Software Version	Age	Status	Profile	Radio	Channel	Authenticated Clients
00:22:b0:3a:c1:80		0/5	10.27.65.132	D.08.03.1	0h:0m:3s	Managed	1-Default	1-802.11a/n 2-802.11b/g/n	149 6	0 0
00:22:b0:3a:c9:80		0/7	10.27.65.192	D.08.03.1	0h:0m:2s	Managed	1-Default	1-802.11a/n 2-802.11b/g/n	124 6	0 0
00:02:bc:00:17:d0	N/A	N/A	N/A	N/A	0h:50m:3s	None	N/A	802.11b	6	N/A
00:02:bc:00:17:e0	N/A	N/A	N/A	N/A	0h:35m:38s	None	N/A	802.11a	149	N/A
00:0e:84:f5:f2:d0	N/A	N/A	N/A	N/A	0h:50m:3s	None	N/A	802.11b	6	N/A
00:11:22:44:55:70	N/A	N/A	N/A	N/A	0h:50m:3s	None	N/A	802.11b	6	N/A
00:17:9a:d2:02:10	N/A	N/A	N/A	N/A	0h:33m:38s	Rogue	N/A	802.11a	153	N/A
00:17:9a:d2:02:18	N/A	N/A	N/A	N/A	0h:19m:38s	Rogue	N/A	802.11b	11	N/A
00:1b:2f:30:02:50	N/A	N/A	N/A	N/A	0h:42m:38s	Rogue	N/A	802.11b	11	N/A

Figure 314: All Access Points

The font color for the AP listing indicates that the AP is one of the following types:

- Green—Managed AP
- Orange—Peer Managed AP
- Red—Failed or Rogue AP
- Gray—Unknown AP

To view additional information about the detected AP, click the MAC address of the AP.

Table 267: Monitoring All Access Points

Field	Description
MAC Address	Shows the MAC address of the access point.
Location	A location description for the AP. This is the value configured in the valid AP database (either locally or on the RADIUS server).
Switch Port	The physical port (in the slot/port format) on the switch that the AP is connected to either directly or indirectly in the same L3 domain. If the AP is beyond the L3 network boundary, then 'Unknown' is displayed.
IP Address	The network address of the access point.
Software Version	Shows the version of D-Link Access Point software that the AP is running.
Age	Shows how much time has passed since the AP was last detected and the information was last updated.

Table 267: Monitoring All Access Points (Cont.)

Field	Description
Status	<p>Shows the access point status:</p> <ul style="list-style-type: none"> • Managed—The AP profile configuration has been applied to the AP and it's operating in managed mode. • No Database Entry—The AP has attempted to become managed by the switch, but the MAC address of the AP does not appear in the local or RADIUS Valid AP database. • Authenticated—The AP has been authenticated by the switch and is in the process of becoming managed. • Local Authentication — The authentication password configured in the AP did not match the password configured in the local database. • Not Managed — The AP is in the Valid AP database, but the AP Mode in the local database is not set to Managed. • RADIUS Authentication — The password configured in the RADIUS client for the RADIUS server was rejected by the server. • RADIUS Challenged — The RADIUS server is configured to use the Challenge-Response authentication mode, which is incompatible with the AP. • RADIUS Unreachable — The RADIUS server that the AP is configured to use is unreachable. • Invalid RADIUS Response — The AP received a response packet from the RADIUS server that was not recognized or invalid. • Invalid Profile ID — The profile ID specified in the RADIUS database may not exist on the switch. This can also happen with the local database when the configuration has been received from a peer switch. • Profile Mismatch-Hardware Type — The AP hardware type specified in the AP Profile is not compatible with the actual AP hardware. • Connection Failed—The AP was previously authenticated and managed, but currently does not have connection with the wireless switch. A connection failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reset. • Rogue—The AP is detected in the network and is classified as a threat by one of the threat detection algorithms. • Unknown—The AP is detected in the network but it is not classified as a threat by the threat detection algorithms.
Profile	<p>The AP profile configuration currently applied to the managed AP. The profile is assigned to the AP in the valid AP database.</p> <p>Note: Once an AP is discovered and managed by the Unified Switch, if the profile is changed in the valid AP database (either locally or on the RADIUS server) the AP is automatically reset when a new profile is assigned.</p>
Radio	Shows the wireless radio mode the AP is using.
Channel	Shows the operating channel for the radio.
Authenticated Clients	Shows the number of wireless clients that are associated and authenticated with the access point per radio.



Note: Some status values for some APs in the All Access Points list are not available. Those are listed as N/A.



Note: You can sort the list of APs by any of the column heading except for Radio, Channel, and Authenticated Clients. For example, to sort the APs by the profile they use, click Profile.

Command Buttons

The page includes the following button:

- **Delete All** —Manually clear all APs from the All Access Points status page except Managed Access Points.
- **Manage** — Configure an Authentication Failed AP to be managed by the switch the next time it is discovered. Select the check box next to the MAC address of the AP before you click **Manage**. You will be presented with the Valid Access Point Configuration page. You can then configure the AP and click **Submit** to save the AP in the local Valid AP database. If you use a RADIUS server for AP validation, you must add the MAC address of the AP to the AP database on the RADIUS server.
- **Acknowledge** — Identify an AP as an Acknowledged Rogue. Select the check box next to the MAC address of the AP before you click **Acknowledge**. The switch adds the AP to the Valid AP database as an Acknowledged Rogue.
- **Refresh**—Updates the page with the latest information.

Managed AP Status

From the **WLAN > Monitoring > Access Point > Managed AP Status** page, you can access a variety of information about each AP that the switch manages. The pages you access from the **Status** tab provide configuration and association information about managed APs and their neighbors. The pages you access from the **Statistics** tab display information about the number of packets and bytes transmitted and received on various interfaces.

Monitoring AP Status

The following figure shows the **Managed Access Point Status** page with two managed APs.

MAC Address (*).Peer Managed	Location	Switch Port	IP Address	Software Version	Age	Status	Configuration Status	Profile	Radio	Channel	Authenticated Clients
* 1c:af:f7:1f:27:40		0/6	10.27.65.199	D.6.27.1	0d:00:00:03	Managed	Failure	1-Default	1-802.11a/n 2-802.11b/g/n	0 0	0 0
1c:af:f7:1f:27:80		0/6	10.27.64.137	D.6.27.1	0d:00:00:04	Managed	Success	1-Default	1-802.11a/n 2-802.11b/g/n	157 1	0 0

Figure 315: Managed AP Status

The following tabs are available from the **Managed AP Status** page:

- **Summary:** Lists the APs managed by the switch and provides summary information about them.
- **Detail:** Shows detailed status information collected from the AP.
- **Radio Summary:** Shows the channel, transmit power, and number of associated wireless clients for all managed APs.
- **Radio Detail:** Shows detailed status for a radio interface. Use the radio button to navigate between the two radio interfaces.
- **Neighbor APs:** Shows the neighbor APs that the specified AP has discovered through periodic RF scans on the selected radio interface.
- **Neighbor Clients:** Shows information about wireless clients associated with an AP or detected by the AP radio.
- **VAP:** Shows summary information about the virtual access points (VAPs) for the selected AP and radio interface on the APs that the switch manages.
- **Distributed Tunneling:** Shows information about the L2 tunnels currently in use on the AP.

The following table provides summary information about the APs that the switch manages. If the switch is the Cluster Controller, the page provides information about the APs managed by all switches in the cluster.

Table 268: Managed Access Point Status

Field	Description
MAC Address	The Ethernet address of the DWS-4000 Series switch- managed AP. If the MAC address of the AP is followed by an asterisk (*), it is managed by a peer switch.
Location	A location description for the AP. This is the value configured in the valid AP database (either locally or on the RADIUS server).
Switch Port	The physical port (in the slot/port format) on the switch that the AP is connected to either directly or indirectly in the same L3 domain. If the AP is beyond the L3 network boundary, then 'Unknown' is displayed.

Table 268: Managed Access Point Status (Cont.)

Field	Description
IP Address	The network IP address of the managed AP.
Software Version	The software version the AP is currently running.
Age	Time since last communication between the DWS-4000 Series switch and the AP.
Status	<p>The current managed state of the AP. The possible values are:</p> <ul style="list-style-type: none"> • Discovered: The AP is discovered and by the switch, but is not yet authenticated. • Authenticated: The AP has been validated and authenticated (if authentication is enabled), but it is not configured. • Managed: The AP profile configuration has been applied to the AP and it's operating in managed mode. • Failed: The DWS-4000 Series switch lost contact with the AP, a failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reset. <p>Note: When management connectivity is lost for a managed AP, then both radios of the AP are turned down. All the clients associated with the AP get disassociated. The radios become operational if and when that AP is managed again by a switch.</p>
Configuration Status	<p>This status indicates if the AP is configured successfully with the assigned profile. The status is one of the following:</p> <ul style="list-style-type: none"> • Not Configured: The profile has not been sent to the AP yet, the AP may be discovered but not yet authenticated. • In Progress: The switch is currently sending the AP profile configuration packet to the AP. • Success: The entire profile has been sent to the AP and there were no configuration errors. • Partial Success: The entire profile has been sent to the AP and there were configuration errors (for example, some configuration parameters were not accepted), but the AP is operational. • Failure: The profile has been sent to the AP and there were configuration errors, the AP is not operational.
Profile	<p>The AP profile configuration currently applied to the managed AP. The profile is assigned to the AP in the valid AP database.</p> <p>Note: Once an AP is discovered and managed by the DWS-4000 Series switch, if the profile is changed in the valid AP database (either locally or on the RADIUS server) the AP must be reset to configure with the new profile.</p>
Radio	Shows the wireless radio mode that each radio on the AP is using.
Channel	Shows the operating channel for the radio.
Authenticated Clients	Shows the number of wireless clients associated and authenticated with the access point per radio.



Note: You can sort the list of APs by clicking any of the column headings. For example, to sort the APs by the profile they use, click **Profile**.

Command Buttons

The page includes the following buttons:

- **Delete**—Clears the selected entry from the current list. Only APs with a Configuration Status of Failed can be removed from the list.
- **Delete All**—Clears all APs with a Configuration Status of Failed from the current list.
- **Refresh**—Updates the page with the latest information.

Viewing Detailed Managed Access Point Status

To view detailed information about an AP that the switch manages, click the MAC address of the AP from the **Summary** page or select the MAC address of the AP from the drop-down menu on the **Detail** page.

[Table 269](#) describes the fields you see on the **Detail** page for the managed access point status. The label at the top of the table shows the MAC address and location of the AP to which the values on the page apply. To view details about a different AP, select its MAC address from the drop-down menu.

Click the **Reset** button to reset the managed AP. A pop-up message asks you to confirm that you want to reset the AP. Any wireless clients associated with the access point will be disassociated. To refresh the status information for the AP, click **Refresh**.

Table 269: Detailed Managed Access Point Status

<i>Field</i>	<i>Description</i>
IP Address	The IP address of the managed AP.
IP Subnet Mask	The subnet mask of the managed AP
Status	<p>The current managed state of the AP. The possible values are:</p> <ul style="list-style-type: none"> • Discovered: The AP is discovered and by the switch, but is not yet authenticated. • Authenticated: The AP has been validated and authenticated (if authentication is enabled), but it is not configured. • Managed: The AP profile configuration has been applied to the AP and it's operating in managed mode. • Connection Failed: The DWS-4000 Series switch lost contact with the AP, a failed entry will remain in the managed AP database unless you remove it. Note that a managed AP will temporarily show a failed status during a reset. <p>Note: When management connectivity is lost for a managed AP, then both radios of the AP are turned down. All the clients associated with the AP get disassociated. The radios become operational if and when that AP is managed again by a switch.</p>
Software Version	Indicates the version of software on the AP, this is learned from the AP during discovery.

Table 269: Detailed Managed Access Point Status (Cont.)

Field	Description
Code Download Status	<p>Indicates the current status of a code download request for this AP. The possible values include the following:</p> <ul style="list-style-type: none"> • Not Started: No download has begun. • Requested: A download is planned for this AP, but the AP is not in the current download group, so it hasn't been told to start the download yet. • Code-Transfer-In-Progress: The AP has been told to download the code. • Failure: The AP reported a failing code download. • Aborted: The download was aborted before the AP loaded code from the TFTP server. • Waiting-For-APs-To-Download: A download finished on this AP, and it is waiting for other APs to finish download. Reset command is not sent to the AP in this state. • NVRAM-Update-In-Progress: Download completed successfully. The reset command sent to the AP. • Timed-Out: The AP did not reconnect to the DWS-4000 Series switch in the fixed time interval.
Configuration Status	<p>Indicates whether the AP is configured successfully with the assigned profile. The status is one of the following:</p> <ul style="list-style-type: none"> • Not Configured: The profile has not been sent to the AP yet, the AP may be discovered but not yet authenticated. • In Progress: The switch is currently sending the AP profile configuration packet to the AP. • Success: The entire profile has been sent to the AP and there were no configuration errors. • Partial Success: The entire profile has been sent to the AP and there were configuration errors, but the AP is operational. • Failure: The profile has been sent to the AP and there were configuration errors, the AP is not operational.
Configuration Failure Error Message	<p>This field appears if the configuration status indicates a partial or complete failure. The field provides information about the last element that failed during configuration. The field shows an ASCII string filled in by the AP containing the error message for the last failing configuration element. </p>
Configuration Failure Element	<p>This field appears if the configuration status indicates a partial success or failure. It shows the element ID of the last failing configuration element.</p>
Vendor ID	Vendor of the AP software, this is learned from the AP during discovery.
Part Number	Hardware part number for the AP, which is learned from the AP during discovery.
Hardware Type	Hardware platform for the AP, which is learned from the AP during discovery.
Managing Switch	Indicates whether the AP is managed by the local switch or a peer switch.
Switch MAC Address	Identifies the MAC address of the switch that is managing the AP.
Switch IP Address	Identifies the IP address of the switch that is managing the AP.
Profile	<p>The AP profile configuration currently applied to the managed AP, the profile is assigned to the AP in the valid AP database.</p> <p>Note: Once an AP is discovered and managed by the DWS-4000 Series switch, if the profile is changed in the valid AP database (either locally or on the RADIUS server) the AP must be reset to configure with the new profile.</p>

Table 269: Detailed Managed Access Point Status (Cont.)

Field	Description
Discovery Reason	This status value indicates how the managed AP was discovered, the status is one of the following values: <ul style="list-style-type: none"> • IP Poll Received: The AP was discovered via an IP poll from the DWS-4000 Series switch, its IP address is configured in the IP polling list. • Peer Redirect: The AP was discovered through a peer switch redirect, the AP tried to associate with another peer switch and learned the current DWS-4000 Series switch IP address from the peer (peer learned DWS-4000 Series switch IP address in RADIUS server response when validating the AP). • Switch IP Configured: The managed AP is configured with the DWS-4000 Series switch IP address. • Switch IP DHCP: The managed AP learned the current DWL-X600AP IP address through DHCP option 43. • L2 Poll Received: The AP was discovered through the D-Link Wireless Device Discovery protocol.
Protocol Version	Indicates the protocol version supported by the software on the AP, which is learned from the AP during discovery.
Authenticated Clients	Total number of clients currently associated to the AP that have been authenticated. This is the sum of all authenticated clients for all the VAPs enabled on the AP.
System Up Time	Time in seconds since last power-on reset of the managed AP.
Age	Time since last communication between the DWS-4000 Series switch and the AP.

Command Buttons

The page includes the following buttons:

- **Reset**— Resets the managed AP. A pop-up message asks you to confirm that you want to reset the AP.
- **Disassociate Clients**— Disconnects all associated clients from the AP.
- **Refresh**— Updates the page with the latest information.
- **Back**— Returns to the Managed AP Status page.

Viewing Managed Access Point Radio Summary Information

You can view general information about each operational radio on all APs managed by the switch. The **Managed Access Point Radio Summary** page shows the channel, transmit power, and number of associated wireless clients for all managed APs. For more information about a specific radio on an AP, click the radio.

[Table 270](#) describes the fields you see on the **Radio Summary** page for the managed access point status.

Table 270: Managed AP Radio Summary

<i>Field</i>	<i>Description</i>
MAC Address	The Ethernet address of the DWS-4000 Series switch managed AP. If the MAC address of the AP is followed by an asterisk (*), it is managed by a peer switch.
Location	A location description for the AP, this is the value configured in the valid AP database (either locally or on the RADIUS server).
Radio	Indicates the radio interface and configured mode of the radio, if the radio is disabled the radio mode will be displayed as Off instead of showing the configured mode.
Channel	If radio is operational, the current operating channel for the radio.
Transmit Power	If radio is operational, the current transmit power for the radio.
Authenticated Clients	Total count of clients authenticated by the AP on the physical radio. This is a sum of all the clients authenticated by each VAP enabled on the radio.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Back**—Returns to the Managed AP Status page.

Viewing Detailed Managed Access Point Radio Information

You can view detailed information about each radio on the APs that the DWS-4000 Series switch manages on the **Radio Detail** page for the managed access point radio status. Use the options above the table to select the AP and radio with the settings to view. The AP is identified by its MAC address and location. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off. [Table 271](#) describes the fields you see on the **Radio Detail** page for the managed access point status.

Table 271: Managed AP Radio Detail

<i>Field</i>	<i>Description</i>
Supported Channels	The list of eligible channels the AP reported to the switch for channel assignment. The list is based on country code, hardware capabilities, and any configured channel limitations.
Channel	If radio is operational, the current operating channel for the radio.
Channel Bandwidth	Indicates whether the channel bandwidth is 20 MHz or 40 MHz.
Fixed Channel Indicator	This flag indicates if a fixed channel is configured and assigned to the radio, a fixed channel can be configured in the valid AP database (locally or on a RADIUS server).

Table 271: Managed AP Radio Detail (Cont.)

Field	Description
Manual Channel Adjustment Status	Indicates the current state of a manual request to change the channel on this radio. The valid values are: <ul style="list-style-type: none"> • Not Started: No request has been made to change the channel. • Requested: A channel change has been requested by the user but has not been processed by the switch. • In Progress: The switch is processing a channel change request for this radio. • Success: A channel change request is complete. • Failure: A channel change request failed.
WLAN Utilization	Total network utilization for the physical radio. This value is based on radio statistics.
Authenticated Clients	Total count of clients authenticated with the AP on the physical radio. This is a sum of all the clients authenticated with the AP for each VAP enabled on the radio.
Transmit Power	If radio is operational, the current transmit power for the radio.
Fixed Power Indicator	This flag indicates if a fixed power setting is configured and assigned to the radio, a fixed transmit power can be configured in the valid AP database (locally or on a RADIUS server).
Manual Power Adjustment Status	Indicates the current state of a manual request to change the power setting on this radio. The valid values are: <ul style="list-style-type: none"> • None: No request has been made to change the power. • Requested: A power adjustment has been requested by the user but has not been processed by the switch. • In Progress: The switch is processing a power adjustment request for this radio. • Success: A power adjustment request is complete. • Failure: A power adjustment request failed.
Total Neighbors	Total number of neighbors (both APs and clients) that can be seen by this radio in its RF area.

For radios that include IEEE 802.11a, IEEE 802.11a/n, or 5-GHz 802.11n support, the page displays an additional table with radar detection information.

Table 272: Radio Detail Regulatory Domain

Field	Description
Supported Channel	Lists the radio channel used for transmitting and receiving wireless traffic.
Radar Detection Required	In some regulatory domains, radar detection is required on some channels in the 5-GHz band. If radar detection is required on the channel, the AP uses the 802.11h specification to avoid interference with other wireless devices.
Radar Detected	Indicates whether another 802.11 device was detected on the channel.
Time Since Radar Last Detected	Shows the amount of time that has passed since the device was last detected on the channel.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Back**—Returns to the Managed AP Status page.

Viewing Managed Access Point Neighbor APs

During the RF scan, an access point collects and stores beacon information visible from neighboring access points. Access points can store the neighbor information for up to 64 neighbor APs. If the neighbor scan information exceeds the capacity, the oldest data in the neighbor list is overwritten.

Use the menu above the table to select the AP with the Neighbor AP information to view. The AP is identified by its MAC address and location. If the AP has two radios, select a radio to view the neighbor APs detected by using an RF scan on that radio. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off.

[Table 273 on page 466](#) describes the fields you see on the **Neighbor APs** page for the managed access point status.

Table 273: Managed AP Neighbor Status

Field	Description
Neighbor AP MAC	The Ethernet MAC address of the neighbor AP network, this could be a physical radio interface or VAP MAC address. For D-Link APs this is always a VAP MAC address. The neighbor AP MAC address may be cross-referenced in the RF Scan status.
SSID	Service Set ID of the neighbor AP network.
RSSI	Received Signal Strength Indication, this is an indicator of the signal strength relative to the neighbor and may give an idea of the neighbor's distance from the managed AP. The range is 1–100, where 1 is the weakest signal strength.
Status	Indicates the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. The valid values are: <ul style="list-style-type: none"> • Managed: The neighbor AP is managed by the wireless system. • Standalone: The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS). • Rogue: The AP is classified as a threat by one of the threat detection algorithms. • Unknown: The AP is detected in the network but is not classified as a threat by the threat detection algorithms.
Age	Indicates the time since this AP was last reported from an RF scan on the radio.

Command Buttons

The page includes the following buttons:

- **Delete All Neighbors**—Clears all entries from the Neighbor APs and Neighbor Clients list. This deletes all neighbors for all radios on all APs — not only for the currently selected AP and radio. The list is repopulated as neighbors are discovered.
- **Refresh**—Updates the page with the latest information.

Viewing Clients Associated with Neighbor Access Points

The **Neighbor Clients** page shows information about wireless clients that have been discovered by the selected AP. APs can store information for up to 512 wireless clients. If the information exceeds the capacity, the oldest data in the neighbor client list is overwritten.

Use the menu above the table to select the AP with the neighbor client information to view. The AP is identified by its MAC address and location. If the AP has two radios, select a radio to view the neighbor clients detected via an RF scan on that radio. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off.

The **Delete All Neighbors** button clears the Neighbor AP and Neighbor Clients lists. The list is repopulated as neighbors and associated clients are discovered.

[Table 274](#) describes the fields you see on the **Neighbor Clients** page for the managed access point status.

Table 274: Neighbor AP Clients

<i>Field</i>	<i>Description</i>
Neighbor Client MAC	The Ethernet address of client station.
RSSI	Received Signal Strength Indication, this is an indicator of the signal strength relative to the neighbor and may give an idea of the neighbor's distance from the managed AP. The range is 1–100, where 1 is the weakest signal strength.
Channel	The managed AP channel the client frame was received on, which may be different than the operating channel for this radio.
Discovery Reason	Indicates one or more discovery methods for the neighbor client. One or more of the following values may be displayed: <ul style="list-style-type: none"> RF Scan Discovered: The client was reported from an RF scan on the radio. Note that client stations are difficult to detect via RF scan, the other methods are more common for client neighbor detection. Probe Request: The managed AP received a probe request from the client. Associated to Managed AP: This neighbor client is associated to another managed AP. Associated to this AP: The client is associated to this managed AP on the displayed radio. Associated to Peer AP: The client is associated to an AP managed by a peer switch. Ad Hoc Rogue: The client was detected as part of an Ad Hoc network.
Age	Indicates the time since this client was last reported from an RF scan on the radio.

Command Buttons

The page includes the following buttons:

- **Delete All Neighbors**—Clears all entries from the Neighbor APs and Neighbor Clients list. The list is repopulated as neighbors are discovered.
- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point VAPs

There are 16 virtual access points (VAPs) available on each radio of an AP. For each radio of an access point managed by the switch, you can view a summary of the VAP configuration and the number of wireless clients associated with a particular VAP.

Use the menu above the table to select the AP with the VAP information to view. The AP is identified by its MAC address and location. If the AP has two radios, select a radio to view details about VAPs on that radio. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off.

[Table 275](#) describes the fields you see on the **VAPs** page for the managed access point status.

Table 275: Managed Access Point VAP Status

Field	Description
VAP ID	The integer ID used to identify the VAP (0-7), this is used to uniquely identify the VAP for configuration via CLI/SNMP.
VAP Mode	Indicates whether or not the VAP is enabled or disabled. VAPs are always configured, but are only sending beacons and accepting clients when they are Enabled.
BSSID	The Ethernet address of the VAP.
SSID	Indicates the network assigned to the VAP. The network for each VAP is configured within the AP profile and the SSID is based on the network configuration.
Client Associations	Indicates the total number of clients currently associated to the VAP.
Client Authentications	Indicates the total number of clients currently authenticated with the VAP.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point VAP TSPEC Status

There are 16 virtual access points (VAPs) available on each radio of an AP. For each VAP on each radio of an AP managed by the switch, you can view information about the traffic that uses a traffic specification (TSPEC). A TSPEC is a set of parameters that define Quality of Service (QoS) characteristics of a traffic flow. A QoS-capable wireless client sends a TSPEC request to the AP to enable the AP to prioritize traffic streams and deliver appropriate resources to time- and delay-sensitive network traffic. TSPECs are commonly used with video and voice traffic.

To view TSPEC data for a VAP, you select the AP, radio interface, and VAP. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off. The VAP is identified by the VAP ID.

The following table describes the fields you see on the **VAP TSPEC** page.

Table 276: Managed Access Point VAP TSPEC Status

Field	Description
VAP ID	The integer ID used to identify the VAP (0-15), this is used to uniquely identify the VAP for configuration via CLI/SNMP.
Access Category	Indicates whether the TSPEC data is for voice traffic or video traffic. The VAP maintains separate counters for the voice and video categories.
Operational Status	Indicates the current operational mode for the category. The operational mode is influenced by both the individual Admission Control Mandatory (ACM) mode and overall TSPEC mode.
Number of Active Traffic Streams	Shows the number of active traffic streams on the selected VAP. A traffic stream is a collection of data packets identified by the wireless client as belonging to a particular user priority. An example of a voice traffic stream is a Wi-Fi Certified telephone handset that marks its codec-generated data packets as voice priority traffic. An example of a video traffic stream is a video player application on a wireless laptop that prioritizes a video conference feed from a corporate server.
Number of Traffic Stream Clients	Shows the number of clients with an active traffic stream on the selected VAP.
Number of Traffic Stream Roaming Clients	Shows the number of clients in roaming mode with an active traffic stream on the selected VAP. This value is also included in the Number of Traffic Stream Clients field.
Medium Time Admitted	Current sum of medium time (bandwidth) allocated to clients using a traffic stream on the selected VAP. Medium time is measured in 32 μ sec/sec units.
Medium Time Unallocated	Amount of medium time (bandwidth) not currently allocated for clients connected through this VAP. Medium time is measured in 32 μ sec/sec units.
Medium Time Roaming Unallocated	Amount of medium time (bandwidth) not currently allocated for roaming clients. Medium time is measured in 32 μ sec/sec units.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Distributed Tunneling Information

The AP-AP tunneling mode is used to support L3 roaming for wireless clients without forwarding any data traffic to the wireless switch.

In the AP-AP tunneling mode, when a client first associates with an AP in the wireless system, the AP forwards the wireless client's data using VLAN forwarding mode. The AP the client initially associates with is called the *Home AP*. The AP the client roams to is called the *Association AP*.

Use the menu above the table to select the AP with the distributed tunneling information to view. The AP is identified by its MAC address and location.

[Table 277](#) describes the fields you see on the **Managed Access Point Distributed Tunneling Status** page for the managed access point status.

Table 277: Distributed Tunneling Status

Field	Description
Distributed Tunnel Clients using AP as Home	Number of clients that roamed away from this AP using distributed tunneling mode and are tunneling data back to this AP.
Distributed Tunnel Clients using AP as Associate	Number of clients that roamed to this AP using distributed tunneling mode and are tunneling data to the Home AP.
Distributed Tunnels	Number of APs to which this AP has a distributed L2 tunnel. The AP may be acting as Home AP or Association AP for clients using the tunnel.
Distributed Tunnel Multicast Replications	Maximum number of tunnels on the Home AP that are members of the same VLAN.
VLAN with Max Multicast Replications	The VLAN ID that is currently replicated the most number of times by the AP for sending multicasts into distributed tunnels.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Managed Access Point Statistics

The managed AP statistics page shows information about traffic on the wired and wireless interfaces of the access point. This information can help diagnose network issues, such as throughput problems.

The following figure shows the **Managed Access Point Statistics** page with a managed AP.

MAC Address	Packets Received	Bytes Received	Packets Transmitted	Bytes Transmitted
1c:af:f7:1f:27:40	180	22220	14734	1993520
1c:af:f7:1f:27:80	83801	9191532	704527	77976121

Figure 316: Managed AP Statistics

The following tabs are available from the **Managed AP Statistics** page:

- **WLAN Summary:** Shows summary information about the wireless interfaces on each AP the switch manages.
- **Ethernet Summary:** Shows summary information about the Ethernet (wired) interfaces on each AP the switch manages.
- **Detail:** Shows the number and type of packets transmitted and received on a specific AP.
- **Radio:** Shows per-radio information about the number and type of packets transmitted and received for a specific AP.
- **VAP:** Shows per-VAP information about the number of packets transmitted and received and the number of wireless client failures for a specific AP.
- **Distributed Tunneling:** Shows information about the L2 tunnels currently in use on the AP.

On the WLAN Summary and Ethernet Summary pages, click the MAC address of the AP to view detailed statistics about the AP.

Table 278: Managed Access Point WLAN Summary Statistics

Field	Description
MAC Address	The Ethernet address of the DWS-4000 Series switch-managed AP.
Packets Received	Total packets received by the AP on the wireless network.
Bytes Received	Total bytes received by the AP on the wireless network.
Packets Transmitted	Total packets transmitted by the AP on the wireless network.
Bytes Transmitted	Total bytes transmitted by the AP on the wireless network.



Note: You can sort the list of APs by clicking any of the column headings. For example, to sort the APs by the number of packets transmitted, click **Packets Transmitted**.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point Ethernet Statistics

The Ethernet summary statistics show information about the number of packets and bytes transmitted and received on the wired interface of each access point managed by the switch. The wired interface is physically connected to the LAN.

[Table 279](#) describes the fields you see on the **Ethernet Summary** page for the managed access point statistics.

Table 279: Managed Access Point Ethernet Summary Statistics

<i>Field</i>	<i>Description</i>
MAC Address	The Ethernet address of the DWS-4000 Series switch-managed AP.
Packets Received	Total packets received by the AP on the wired network.
Bytes Received	Total bytes received by the AP on the wired network.
Packets Transmitted	Total packets transmitted by the AP on the wired network.
Bytes Transmitted	Total bytes transmitted by the AP on the wired network.

Viewing Detailed Managed Access Point Statistics

The detailed AP statistics show information about the packets and bytes transmitted and received on the wired and wireless interface of a particular access point managed by the switch. To view statistics for a specific AP that the switch manages, select its MAC address from the drop-down menu above the table. The location, if available, is also displayed with the MAC address.

[Table 280](#) describes the fields you see on the **Detail** page for the managed access point statistics.

Table 280: Detailed Managed Access Point Statistics

<i>Field</i>	<i>Description</i>
WLAN Packets Received	Total packets received by the AP on the wireless network.
WLAN Bytes Received	Total bytes received by the AP on the wireless network.
WLAN Packets Transmitted	Total packets transmitted by the AP on the wireless network.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on the wireless network.
WLAN Packets Receive Dropped	Number of packets received by the AP on the wireless network that were dropped.

Table 280: Detailed Managed Access Point Statistics (Cont.)

Field	Description
WLAN Bytes Receive Dropped	Number of bytes received by the AP on the wireless network that were dropped.
WLAN Packets Transmit Dropped	Number of packets transmitted by the AP on the wireless network that were dropped.
WLAN Bytes Transmit Dropped	Number of bytes transmitted by the AP on the wireless network that were dropped.
Ethernet Packets Received	Total packets received by the AP on the wired network.
Ethernet Bytes Received	Total bytes received by the AP on the wired network.
Ethernet Packets Transmitted	Total packets transmitted by the AP on the wired network.
Ethernet Bytes Transmitted	Total bytes transmitted by the AP on the wired network.
Multicast Packets Received	Total multicast packets received by the AP on the wired network.
Total Receive Errors	Total receive errors detected by the AP on the wired network.
Total Transmit Errors	Total transmit errors detected by the AP on the wired network.
ARP Reqs Converted from Bcast to Ucast	Number of ARP requests that the AP converted from a broadcast packet to a unicast packet before sending to the wireless link.
Filtered ARP Requests	Number of ARP requests that AP was able to drop instead of sending on the wireless link.
Broadcasted ARP Requests	The number of ARP requests sent as broadcasts on the VAPs. This counter does not include WDS links. The same ARP frame may be counted multiple times when it is broadcasted on multiple VAPs. The counter is available even when ARP suppression is disabled.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point Radio Statistics

The radio statistics show detailed information about the packets and bytes transmitted and received on the radio (wireless) interface of a particular access point managed by the switch.

Use the options above the table to select the AP and radio with the settings to view. The AP is identified by its MAC address and location. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off.

[Table 281](#) describes the fields you see on the **Radio** page for the managed access point statistics.

Table 281: Managed Access Point Radio Statistics

Field	Description
WLAN Packets Received	Total packets received by the AP on this radio interface.
WLAN Bytes Received	Total bytes received by the AP on this radio interface.
WLAN Packets Transmitted	Total packets transmitted by the AP on this radio interface.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on this radio interface.
WLAN Packets Receive Dropped	Number of packets received by the AP on this radio interface that were dropped.
WLAN Bytes Receive Dropped	Number of bytes received by the AP on this radio interface that were dropped.
WLAN Packets Transmit Dropped	Number of packets transmitted by the AP on this radio interface that were dropped.
WLAN Bytes Transmit Dropped	Number of bytes transmitted by the AP on this radio interface that were dropped.
Fragments Received	Count of successfully received MPDU frames of type data or management.
Fragments Transmitted	Number of transmitted MPDU with an individual address or an MPDU with a multicast address of type Data or Management.
Multicast Frames Received	Count of MSDU frames received with the multicast bit set in the destination MAC address.
Multicast Frames Transmitted	Count of successfully transmitted MSDU frames where the multicast bit is set in the destination MAC address.
Duplicate Frame Count	Number of times a frame is received and the Sequence Control field indicates is a duplicate.
Failed Transmit Count	Number of times a MSDU is not transmitted successfully due to transmit attempts exceeding either the short retry limit or the long retry limit.
Transmit Retry Count	Number of times a MSDU is successfully transmitted after one or more retries.
Multiple Retry Count	Number of times a MSDU is successfully transmitted after more than one retry.
RTS Success Count	Count of CTS frames received in response to an RTS frame.
RTS Failure Count	Count of CTS frames not received in response to an RTS frame.
ACK Failure Count	Count of ACK frames not received when expected.
FCS Error Count	Count of FCS errors detected in a received MPDU frame.

Table 281: Managed Access Point Radio Statistics

Field	Description
Frames Transmitted	Count of each successfully transmitted MSDU.
WEP Undecryptable Count	Count of encrypted frames received and the key configuration of the transmitter indicates that the frame should not have been encrypted or that frame was discarded due to the receiving station not implementing the privacy option.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Managed Access Point VAP Statistics

The VAP statistics show information about the client failures and number of packets and bytes transmitted and received on each VAP on radio one or two for a particular access point managed by the switch.

Use the options above the table to select the AP, radio, and VAP with the settings to view. The AP is identified by its MAC address and location. The radio is identified by its number and configured mode. If the radio is disabled, the radio mode will be displayed as Off. The VAP is identified by the VAP ID and its SSID. All VAPs are available regardless of whether they are enabled.

[Table 282](#) describes the fields you see on the **VAP** page for the managed access point statistics.

Table 282: Managed Access Point VAP Statistics

Field	Description
WLAN Packets Received	Total packets received by the AP on this VAP.
WLAN Bytes Received	Total bytes received by the AP on this VAP.
WLAN Packets Transmitted	Total packets transmitted by the AP on this VAP.
WLAN Bytes Transmitted	Total bytes transmitted by the AP on this VAP.
WLAN Packets Receive Dropped	Number of packets received by the AP on this VAP that were dropped.
WLAN Bytes Receive Dropped	Number of bytes received by the AP on this VAP that were dropped.
WLAN Packets Transmit Dropped	Number of packets transmitted by the AP on this VAP that were dropped.
WLAN Bytes Transmit Dropped	Number of bytes transmitted by the AP on this VAP that were dropped.
Client Association Failures	Number of clients that have been denied association to the VAP.
Client Authentication Failures	Number of clients that have failed authentication to the VAP.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Distributed Tunneling Statistics

The distributed tunneling statistics show information about the number of packets and bytes transmitted and received by clients that use L2 distributed tunnels on an access point managed by the switch.

Use the menu above the table to select the AP with the settings to view. The AP is identified by its MAC address and location.

[Table 283](#) describes the fields you see on the **Distributed Tunneling Statistics** page for the managed access point statistics.

Table 283: Managed Access Point Distributed Tunneling Statistics

Field	Description
Bytes Transmitted	Total bytes transmitted via all distributed tunnels by the AP.
Bytes Received	Total bytes received via all distributed tunnels by the AP.
Multicast Packets Transmitted	Total multicast packets transmitted via all distributed tunnels by the AP.
Multicast Packets Received	Total multicast packets received via all distributed tunnels by the AP.
Packets Transmitted	Total packets transmitted via all distributed tunnels by the AP.
Packets Received	Total packets received via all distributed tunnels by the AP.
Total Roamed Clients of AP	Number of Clients that used this AP for distributed tunneling. The count include clients that roamed away and roamed to this AP.
Roamed Clients Idle Timed Out	Number of Clients that roamed away from this AP and were timed out due to not sending traffic on the tunnel.
Roamed Clients Age Timed Out	Number of Clients that roamed away from this AP and were timed out due to age of the tunnel.
Client Limit Denials	Number of times the AP denied the clients attempt to set up a distributed tunnel due to the AP reaching the configured tunneled client limit.
Client Max Replication Denials	Number of times the AP denied the clients attempt to set up a distributed tunnel due to the AP reaching the configured maximum number of VLAN replications.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

AP Authentication Failure Status

An AP might fail to associate to the switch due to errors such as invalid packet format or vendor ID, or because the AP is not configured as a valid AP with the correct local or RADIUS authentication information.

To view a list of APs that failed to associate with the DWS-4000 Series switch, click **WLAN > Monitoring > Access Point > AP Authentication Failure Status**.



MAC Address (*) Peer Reported	IP Address	Last Failure Type	Age
<input type="checkbox"/> 00:22:b0:3a:c9:80	10.27.65.147	No Database Entry	0d:00:00:13

Auto Refresh

Figure 317: AP Authentication Failure Status

The AP authentication failure list shows information about APs that failed to establish communication with the DWS-4000 Series switch. The AP can fail due to one of the following reasons:

- No Database Entry — The MAC address of the AP is not in the local Valid AP database or the external RADIUS server database, so the AP has not been validated.
- Local Authentication — The authentication password configured in the AP did not match the password configured in the local database.
- Not Managed — The AP is in the Valid AP database, but the AP Mode in the local database is not set to Managed.
- RADIUS Authentication — The password configured in the RADIUS client for the RADIUS server was rejected by the server.
- RADIUS Challenged — The RADIUS server is configured to use the Challenge-Response authentication mode, which is incompatible with the AP.
- RADIUS Unreachable — The RADIUS server that the AP is configured to use is unreachable.
- Invalid RADIUS Response — The AP received a response packet from the RADIUS server that was not recognized or invalid.
- Invalid Profile ID — The profile ID specified in the RADIUS database may not exist on the switch. This can also happen with the local database when the configuration has been received from a peer switch.
- Profile Mismatch-Hardware Type — The AP hardware type specified in the AP Profile is not compatible with the actual AP hardware.

If you use the local database for AP Validation, you can click the **WLAN > Administration > Basic Setup > Valid AP** tab to modify the AP configuration. If you use a RADIUS server for AP validation, you must add the MAC address of the AP to the RADIUS server database.

Click the MAC address of the AP to view more information about the AP. If the AP is not a D-Link AP, some values are unknown.

Table 284: Access Point Authentication Failure Status

Field	Description
MAC Address	The Ethernet address of the AP. If the MAC address of the AP is followed by an asterisk (*), it was reported by a peer switch.
IP Address	The IP address of the AP.
Last Failure Type	Indicates the last type of failure that occurred, which can be one of the following: <ul style="list-style-type: none"> • Local Authentication • No Database Entry • Not Managed • RADIUS Authentication • RADIUS Challenged • RADIUS Unreachable • Invalid RADIUS Response • Invalid Profile ID • Profile Mismatch-Hardware Type
Age	Time since failure occurred. The AP failure status entries are collected at a point in time and eventually age out. The age value for each entry shows how long ago the switch recorded the entry. You can configure the age out time for status entries on the WLAN > Advanced Configuration > Global page. You can also manually delete status entries.

Command Buttons

The page includes the following buttons:

- **Delete All**—Delete the entries for all APs in the failure list.
- **Manage**—Add one or more selected APs from the Access Point Failure list to the Valid AP database.
- **Refresh**—Updates the page with the latest information.

Viewing Details About AP Authentication Failures

To view additional data (beacon information) for an AP in the authentication failure list, click the MAC address of the AP.

AP Authentication Failure Status			
MAC address	00:22:b0:3a:c9:80	Reporting Switch	Local Switch
IP Address	10.27.65.147	Switch MAC Address	00:17:9A:95:1F:0C
Last Failure Type	No Database Entry	Switch IP Address	10.27.65.145
Vendor ID	D-Link	Validation Failures	48832
Protocol Version	2	Authentication Failures	0
Software Version	D.08.03.1	Age	0d:00:00:10
Hardware Type	DWL-8600AP Dual Radio a/b/g/n		

Figure 318: AP Authentication Failure Details

The following table describes the fields on the detailed **Access Point Authentication Failure Status** page.

Table 285: Access Point Authentication Failure Details

Field	Description
MAC Address	The Ethernet address of the AP.
IP Address	The network IP address of the AP.
Last Failure Type	Indicates the last type of failure that occurred, which can be one of the following: <ul style="list-style-type: none"> • Local Authentication • No Database Entry • Not Managed • RADIUS Authentication • RADIUS Challenged • RADIUS Unreachable • Invalid RADIUS Response • Invalid Profile ID • Profile Mismatch-Hardware Type
Vendor ID	Vendor of the AP software.
Protocol Version	Indicates the protocol version supported by the software on the AP.
Software Version	Indicates the version of software on the AP.
Hardware Type	Hardware platform for the AP.
Reporting Switch	Shows whether the switch that reported the AP authentication failure is the local switch or a peer switch.
Switch MAC Address	Shows the IP address of the switch in the cluster that reported the AP authentication failure.
Switch IP Address	Shows the MAC address of the switch in the cluster that reported the AP authentication failure.

Table 285: Access Point Authentication Failure Details (Cont.)

Field	Description
Validation Failures	The count of association failures for this AP.
Authentication Failures	The count of authentication failures for this AP.
Age	Time since failure occurred. Status entries for the AP Authentication Failure page are collected at a point in time and eventually age out. The age value for each entry shows how long ago the switch recorded the entry. You can configure the age out time for status entries on the WLAN > Advanced Configuration > Global page. You can also manually delete status entries.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

AP RF Scan Status

The radios on each AP can periodically scan the radio frequency to collect information about other APs and wireless clients that are within range. In normal operating mode the AP always scans on the operational channel for the radio. Two other scan modes are available for each radio on the APs:

- **Scan Other Channels:** Configures the AP to periodically leave its operational channel and scan other channels within that frequency.
- **Scan Sentry:** Disables normal operation of the radio and performs a continuous radio scan. In this mode, no beacons are sent, and no clients are allowed to associate with the AP.

When Scan Other Channels or Scan Sentry modes are enabled, the AP scans all available channels on each radio. When the scan is complete, the AP sends information it collected during the RF scan to the switch that manages it. For information about how to configure the scan mode, see [“Radio Configuration” on page 538](#).

The DWS-4000 Series switch considers an access point to be a rogue if it is detected during the RF scan process and is classified as a threat by one of the threat detection algorithms. To view the threat detection algorithms enabled on the system, go to the **WLAN > Administration > Advanced Configuration > WIDS Security** page.

From the **WLAN > Monitoring > Access Point > AP RF Scan Status** page, you can view information about all APs detected via RF scan, including those reported as Rogues.

You can sort the APs in the list based any of the column headings. For example, to group all Rogue APs together, click **Status**.

AP RF Scan Status					
MAC Address	SSID	Physical Mode	Channel	Status	Age
<input type="checkbox"/> 00:02:bc:00:17:d0	ALT-VLAN-8	802.11b/g	11	Unknown	0d:00:01:36
<input type="checkbox"/> 00:0c:41:d7:ee:a7	b9trcnewap54gv11	802.11b/g	1	Unknown	0d:11:44:55
<input type="checkbox"/> 00:0e:84:e2:11:50	brcmwp	802.11b/g	1	Unknown	0d:06:04:11
<input type="checkbox"/> 00:0e:84:f2:d0	brcmwp	802.11b/g	6	Unknown	0d:00:16:36
<input type="checkbox"/> 00:10:18:80:15:90	Nowhere	802.11a	161	Unknown	0d:05:49:07
<input type="checkbox"/> 00:10:18:82:d2:c0	WDS-path1	802.11b/g	6	Unknown	0d:00:17:35
<input type="checkbox"/> 00:15:2b:92:c9:a0	brcmwp	802.11b/g	11	Unknown	0d:00:01:36
<input type="checkbox"/> 00:17:9a:d2:02:18	dlink1	802.11b/g	11	Unknown	0d:00:01:36
<input type="checkbox"/> 00:1b:e9:16:22:80	Guest Network	802.11b/g	2	Unknown	0d:00:10:35
<input type="checkbox"/> 00:1b:e9:16:22:90	Guest Network	802.11a	36	Unknown	0d:12:11:03
<input type="checkbox"/> 00:1b:e9:16:25:c0	Broadcom VAP	802.11b/g	3	Unknown	0d:00:09:35
<input type="checkbox"/> 00:1b:e9:16:25:d0	Broadcom VAP	802.11a	157	Unknown	0d:03:25:39
<input type="checkbox"/> 00:1b:e9:16:26:00	Broadcom VAP	802.11b/g	4	Unknown	0d:00:52:44
<input type="checkbox"/> 00:1b:e9:16:29:80	HSI BRCM 11	802.11b/g	1	Unknown	0d:02:57:30
<input type="checkbox"/> 00:1b:e9:16:29:90	HSI BRCM 21	802.11a	36	Unknown	0d:12:11:03
<input type="checkbox"/> 00:1b:e9:16:34:50	MP EAP R1 VAP0	802.11a	157	Unknown	0d:07:01:53
<input type="checkbox"/> 00:1b:e9:16:34:c0	GP Net 0	802.11b/g	11	Unknown	0d:00:01:36
<input type="checkbox"/> 00:1b:e9:16:34:c1	GP Net 1	802.11b/g	11	Unknown	0d:00:01:36
<input type="checkbox"/> 00:1b:e9:16:34:c2	GP Net 2	802.11b/g	11	Unknown	0d:00:01:36
<input type="checkbox"/> 00:1b:e9:16:34:c3	GP Net 3	802.11b/g	11	Unknown	0d:00:01:36

1 2 3

Auto Refresh

Figure 319: RF Scan

To view additional information about a detected AP, click the MAC address of the AP.

Table 286 describes the fields on the **Rogue/RF Scan** page.

Table 286: Access Point RF Scan Status

Field	Description
MAC Address	The Ethernet MAC address of the detected AP. This could be a physical radio interface or VAP MAC. For D-Link APs this is always a VAP MAC address.
SSID	Service Set ID of the network, which is broadcast in the detected beacon frame.
Physical Mode	Indicates the 802.11 mode being used on the AP.
Channel	Transmit channel of the AP.
Status	Indicates the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. The valid values are: <ul style="list-style-type: none"> Managed: The neighbor AP is managed by the wireless system. Standalone: The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS). Rogue: The AP is classified as a threat by one of the threat detection algorithms. Unknown: The AP is detected in the network but is not classified as a threat by the threat detection algorithms.
Transmit Rate	Indicates the rate at which the AP is currently transmitting data.
Age	Time since this AP was last detected in an RF scan. Status entries for the RF Scan Status page are collected at a point in time and eventually age out. The age value for each entry shows how long ago the switch recorded the entry. You can configure the age out time for status entries on the WLAN > Advanced Configuration > Global page. You can also manually delete status entries.

Command Buttons

The page includes the following buttons:

- **Delete All**—Clears all APs from the RF scan list. The list repopulates as the APs are discovered.
- **Manage**—Configures a Rogue AP to be managed by the switch the next time it is discovered. The switch adds the selected AP to the Valid AP database as a Managed AP and assigns it the default AP profile. Then, you can use the switch to configure the AP settings. If you use a RADIUS server for AP validation, you must add the MAC address of the AP to the AP database on the RADIUS server.
- **Acknowledge**—Clear the rogue status of the selected AP in the RF Scan database.
- **Acknowledge All Rogues**—Acknowledges all APs with a Rogue status. The status of an acknowledged rogue is returned to the status it had when it was first detected. If the detected AP fails any of the tests that classify it as a threat, it will be listed as a Rogue again.
- **Refresh**—Updates the page with the latest information.

Viewing Details About an AP Detected in the RF Scan

After you click the MAC address of an AP to view details, the detailed **Access Point RF Scan Status** page for the AP appears.

The detailed status for access points detected during the RF scan shows information about an individual AP detected through the RF scan. To view information about another AP detected through the RF Scan, return to the main **Rogue/RF Scan** page and click the MAC address of the AP with the information to view.

AP RF Scan Status		AP Triangulation Status		WIDS AP Rogue Classification	
AP RF Scan Status					
MAC address	00:02:bc:00:17:d0	BSSID	00:02:bc:00:17:d0		
SSID	ALT-VLAN-8	Physical Mode	802.11b/g		
Channel	6	Security Mode	Open		
Status	Standalone	802.11n Mode	Supported		
Initial Status	Unknown	Beacon Interval	100 msec		
Transmit Rate	1 Mbps	Highest Supported Rate	130 Mbps		
WIDS Rogue AP Mitigation	Not Required	Peer Managed AP			
Age	0d:00:00:16	Ad hoc Network	Not Ad hoc		
Discovered Age	1d:03:34:57	OUI Description	LVL 7 Systems, Inc.		
<input type="button" value="Refresh"/>					

Figure 320: RF Scan AP Details

Table 287 shows the information the Access Point RF Scan Status page shows for an individual access point.

Table 287: Detailed Access Point RF Scan Status

Field	Description
MAC Address	The Ethernet MAC address of the detected AP. This could be a physical radio interface or VAP MAC. For D-Link APs this is always a VAP MAC address.
SSID	Service Set ID of the network, which is broadcast in the detected beacon frame.
Channel	Transmit channel of the AP.
Status	Indicates the managed status of the AP, whether this is a valid AP known to the switch or a Rogue on the network. The valid values are: <ul style="list-style-type: none"> Managed: The neighbor AP is managed by the wireless system. Standalone: The AP is managed in standalone mode and configured as a valid AP entry (local or RADIUS). Rogue: The AP is classified as a threat by one of the threat detection algorithms. Unknown: The AP is detected in the network but is not classified as a threat by the threat detection algorithms.
Initial Status	If the AP is not rogue, the initial status is equal to Status (Managed, Standalone, or Unknown). For rogue APs, the initial status is the classification prior to this AP becoming rogue.
Transmit Rate	Indicates the rate at which the AP is currently transmitting data.
WIDS Rogue AP Mitigation	Status indicating whether rogue AP mitigation is in progress for this AP. If mitigation is not in progress then this field displays the reason, which can be one of the following: <ul style="list-style-type: none"> Not Required (AP s not rogue) Already mitigating too many APs. AP Is operating on an illegal channel. AP is spoofing valid managed AP MAC address. AP is Ad hoc.
Age	Time since this AP was last detected in an RF scan.
Discovered Age	Time since this AP was first detected in an RF scan.
BSSID	Basic Service Set Identifier advertised by the AP in the beacon frames.
Physical Mode	Indicates the 802.11 mode being used on the AP.
Security Mode	Security mode used by the AP.
802.11n Mode	Indicates whether this AP supports IEEE 802.11n mode.
Beacon Interval	Beacon interval for the neighbor AP network.
Highest Supported Rate	Highest supported rate advertised by this AP in the beacon frames. The rate is represented in increments of 1 Mbps.
Peer Managed AP	Indicates whether this AP is managed by a switch in the cluster.
Ad hoc Network	Indicates whether the beacon frame was received from an ad hoc network.
OUI Description	Identifies the manufacturer of the AP or wireless client adapter based on the information in the OUI database on the switch.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing AP Triangulation Information

Triangulation information is provided to help locate the rogue client by showing which managed APs detect the each device discovered through the RF Scan. Up to six triangulation entries are reported for each AP detected through the RF Scan: three entries by non-sentry APs and three entries by sentry APs. Since an AP may have one radio configured in sentry mode and another radio configured in non-sentry mode, the same AP can appear in both lists. If the AP has not been detected by three APs, then the list may contain zero, one or two entries.

To view information about another AP detected through the RF Scan, return to the main **Rogue/RF Scan** page and click the MAC address of the AP with the information to view.

Access Point Triangulation Status						
Detected AP MAC Address : 00:02:bc:00:17:d0						
Sentry	MAC Address	Radio	RSSI (%)	Signal Strength (dBm)	Noise Level (dBm)	Age
Non-Sentry	00:22:b9:3a:c1:80	1	39	-63	-95	0d:00:00:35
Non-Sentry	00:22:b9:3a:c9:80	1	46	-58	-89	0d:00:01:31

Figure 321: AP Triangulation Status

Table 288 shows the information the Access Point Triangulation Status page shows for an individual access point.

Table 288: Access Point Triangulation Status

Field	Description
Detected AP MAC Address	The Ethernet MAC address of the detected AP. This could be a physical radio interface or VAP MAC. For D-Link APs this is always a VAP MAC address.
Sentry	Identifies whether the AP that detected the entry is in sentry or non-sentry mode.
MAC Address	Shows the MAC address of the AP that detected the RF Scan entry. The address links to the Valid AP database.
Radio	Identifies the radio on the AP that detected the RF Scan entry.
RSSI	Shows the received signal strength indicator in terms of percentage for the non-sentry AP. The range is 0—100%. A value of 0 indicates the AP is not detected.
Signal Strength	Received signal strength for the non-sentry AP. The range is –127 dBm to 127 dBm, but most values are expected to range from –95 dBm to –10 dBm.
Noise Level	Noise reported on the channel by the non-sentry AP.
Age	Time since this AP was last detected in an RF scan.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing WIDS AP Rogue Classification Information

The Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network. The DWS-4000 Series switch allows you to activate or deactivate various threat detection tests and set threat detection thresholds. The **WIDS AP Rogue Classification** page provides information about the results of these tests. If an AP has been classified as a rogue, this page provides information about which tests the AP might have failed to trigger the classification.

If an AP is classified as a rogue, the system provides additional information to identify the threat type that caused the switch to classify the AP as a rogue.

The WIDS RF Security encompasses three functions:

- Detect wireless devices by listening to control and data frames in the air.
- Classify whether the wireless device is a threat by comparing the received data to various databases as well as sending trace frames into the wired network and listening for the trace frames on the wireless network.
- Take action to protect the network from threats.

These changes can be done without disrupting network connectivity. Since some of the work is done by access points, the switch needs to send messages to the APs to modify its WIDS operational properties.

To view information about another AP detected through the RF Scan, return to the main **Rogue/RF Scan** page and click the MAC address of the AP with the information to view.

The screenshot shows a web interface with three tabs: "AP RF Scan Status", "AP Triangulation Status", and "WIDS AP Rogue Classification". The active tab is "WIDS AP Rogue Classification". Below the tabs, the page title is "WIDS AP Rogue Classification". It displays the MAC Address as "00:01:02:03:07:10" and the Status as "Rogue". A table lists various test descriptions, their detection conditions, reporting MAC addresses, radio counts, test configurations, results, and time since reports. At the bottom of the table are "Acknowledge" and "Refresh" buttons.

Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Administrator configured rogue AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Managed SSID from an unknown AP	True	00:22:b0:3a:c9:80	2	Enabled	Rogue	1d:00:26:35	0d:20:50:35
Managed SSID from a fake managed AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
AP without an SSID	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Fake managed AP on an invalid channel	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Managed SSID detected with incorrect security	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Invalid SSID from a managed AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
AP is operating on an illegal channel	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Standalone AP with unexpected configuration	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Unexpected WDS device detected on network	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Unmanaged AP detected on wired network	False	None	0	Enabled		0d:00:00:00	0d:00:00:00

Figure 322: WIDS AP Rogue Classification

Table 289 shows the information the WIDS AP Rogue Classification page shows for an individual access point.

Table 289: WIDS AP Rogue Classification

Field	Description
MAC Address	The Ethernet MAC address of the detected AP. This could be a physical radio interface or VAP MAC. For D-Link APs this is always a VAP MAC address.
Test Description	Identifies the tests that were performed, which includes the following: <ul style="list-style-type: none"> • Administrator-Configured rogue AP • Managed SSID received from an unknown AP • Managed SSID received from an AP without SSID • Beacon Received from a fake managed AP on a invalid channel • Managed SSID detected with incorrect security configuration • Invalid SSID received from managed AP. • AP is operating on an illegal channel • Standalone AP is operating with unexpected configuration. • Unexpected WDS device is detected on the network. • Unmanaged AP detected on wired network.
Condition Detected	Indicates whether the result of the test was true or false.
Reporting MAC Address	Identifies the MAC address of the AP that reported the test results.
Radio	Identifies which physical radio on the reporting AP was responsible for the test results.
Test Config	Shows whether this test is configured to report rogues. Each test can be globally enabled or disabled to report a positive result as a rogue.
Test Result	Shows whether this test reported the device as rogue. In some cases the test may report a positive result, be enabled, but not report the device as rogue because the device is allowed to operate in this mode.
Time Since First Report	Time stamp indicating how long ago this test first detected the condition.
Time Since Last Report	Time stamp indicating how long ago this test last detected the condition.

Command Buttons

The page includes the following buttons:

- **Acknowledge**—Clears the rogue status of the AP in the RF Scan database.
- **Refresh**—Updates the page with the latest information.

AP De-Authentication Attack Status

The **AP De-Authentication Attack Status** page contains information about rogue APs that the Cluster Controller has attacked by using the de-authentication attack feature.

The wireless switch can protect against rogue APs by sending de-authentication messages to the rogue AP. The de-authentication attack feature must be globally enabled in order for the wireless system to do this function. Make sure that no legitimate APs are classified as rogues before enabling the attack feature. This feature is disabled by default.

The wireless system can conduct the de-authentication attack against 16 APs at the same time. The intent of this attack is to serve as a temporary measure until the rogue AP is located and disabled.

The de-authentication attack is not effective for all rogue types, and therefore is not used on every detected rogue. The following rogues are not subjected to the attack:

- If the detected rogue is spoofing the BSSID of the valid managed AP then the wireless system does not attempt to use the attack because that attack may deny service to a legitimate AP and provide another avenue for a hacker to attack the system.
- The de-authentication attack is not effective against Ad hoc networks because these networks do not use authentication.
- The APs operating on channels outside of the country domain are not attacked because sending any traffic on illegal channels is against the law.

The wireless switch maintains a list of BSSIDs against which it is conducting a de-authentication attack. The switch sends the list of BSSIDs and channels on which the rogue APs are operating to every managed AP.

Click the MAC address of an AP in the list to access the detailed RF Scan information for the AP.

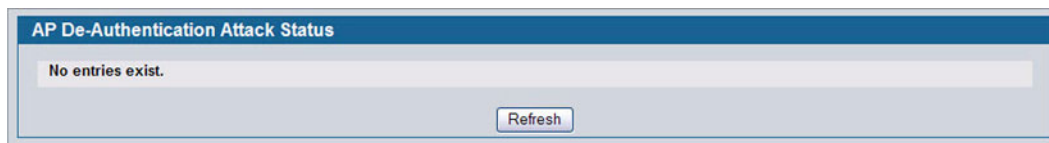


Figure 323: AP De-Authentication Attack Status

The following table describes the fields on the **AP De-Authentication Attack Status** page.

Table 290: AP De-Authentication Attack Status

Field	Description
BSSID	Shows the BSSID of the AP against which the attack is launched. The BSSID is a MAC address.
Channel	Identifies the channel on which the rogue AP is operating.
Time Since Attack Started	Shows the amount of time that has passed since the attack started on the AP.
RF Scan Report Age	Shows the amount of time that has passed since the RF Scan reported this AP.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Associated Client Status/Statistics

You can view a variety of information about the wireless clients that are associated with the APs the switch manages. To access the associated client information, click **WLAN > Monitoring > Client > Associated Client**.

MAC Address (*)-Peer Associated	AP MAC Address	SSID	BSSID	Detected IP Address	NetBIOS Name	Location	Channel	Radio	Encryption	Status	Network Time
<input type="checkbox"/> 00:1fe1:cc:ce:93	1c:af:f7:1f:27:80	DLINK TEST 12	1c:af:f7:1f:27:80	10.27.65.190	LBRDU-DEV-28	157	1-802.11a/n	WPA Personal	Authenticated	0d:19:37:44	

Figure 324: Associated Client Status

The following tabs are available on the **Associated Client** page:

- **Status:** Shows status information about wireless clients that are associated with APs managed by the switch and contains the following information:
 - **Summary:** Shows basic information about associated clients.
 - **Detail:** Shows more detailed information about associated clients, such as which VLAN the client is assigned to and how long the client has been inactive.
 - **Neighbor APs:** Shows the managed APs that are within range of the wireless clients, which can help you determine the managed AP an associated client might use for roaming.
 - **Distributed Tunneling:** Shows information about the Distributed Tunnel status of the client.
- **SSID Status:** Shows the SSID and client MAC address of all clients connected to specific networks.
- **VAP Status:** Shows the clients associated with a specific VAP on a AP
- **Statistics:** Shows statistics about wireless clients that are associated with APs managed by the switch and contains the following information:
 - **Association Summary:** Shows the statistics for a wireless client while it is associated with a single AP.
 - **Session Summary:** If a wireless client roams among different managed APs, the switch can track the statistics for the entire session.
 - **Association Detail:** Shows additional information about packets the associated client transmits and receives during association with a single managed AP.
 - **Session Detail:** Shows additional information about packets the associated client transmits and receives during a session, which can include statistics for one or more managed AP associations if the client has roamed.

Since the associated client database supports roaming across APs, an entry is not removed when a client disassociates from a specific AP. After a client has disassociated, the entry is deleted after the client times out. You configure the timeout value in the **Client Roam Timeout** field on the **WLAN > Administration > Advanced Configuration > Global** page. The timeout value corresponds to the time allowed for a client to roam to another managed AP.

Viewing Associated Client Summary Status

MAC Address (*)-Peer Associated	AP MAC Address	SSID	BSSID	Detected IP Address	NetBIOS Name	Location	Channel	Radio	Encryption	Status	Network Time
<input type="checkbox"/> 00:1fe1:cc:ce:93	1c:aff7:1f:27:80	DLINK TEST 12	1c:af77:1f:27:80	10.27.65.190	LBRDU- DEV-28		157	1-802.11a/n	WPA Personal	Authenticated	0d:19:37:44

Disassociate Disassociate All Refresh

Figure 325: Associated Client Status

Table 291 describes the information available on the **WLAN > Monitoring > Client > Associated Clients > Summary** page for the associated client status.

Table 291: Associated Client Status Summary

Field	Description
MAC Address	The Ethernet address of the client station. If the MAC address is followed by an asterisk (*), the client is associated with an AP managed by a peer switch.
AP MAC Address	The Ethernet address of the AP.
SSID	The network on which the client is connected.
BSSID	The Ethernet MAC address for the managed AP VAP where this client is associated.
Client IP Address	The IP address of the associated client, if available.
NetBIOS Name	The NetBIOS name of the wireless client. For Microsoft Windows hosts, the NetBIOS name is typically the same as, or based on the host name of the client.
Location	The configured descriptive location for the managed AP.
Channel	The operating channel for the client association.
Radio	The radio and mode.
Encryption	The type of encryption in use.

Table 291: Associated Client Status Summary

Field	Description
Status	Indicates whether or not the client has associated and/or authenticated. The valid values are: <ul style="list-style-type: none"> • Associated: The client is currently associated to the managed AP. • Authenticated: The client is currently associated and authenticated to the managed AP. • Disassociated: The client has disassociated from the managed AP. If the client does not roam to another managed AP within the client roam timeout, it will be deleted.
Network Time	Indicates the amount of time that has passed since this client first authenticated with the network.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the selected client from the managed AP.
- **Disassociate All**—Disassociates all clients from the managed AP.
- **Refresh**—Updates the page with the latest information.

Viewing Detailed Associated Client Status

For each client associated with an AP that the switch manages, you can view detailed status information about the client and its association with the access point. Use the menu above the table to select the MAC address of the client with the information to view.

Associated Client Status			
00:26:4a:ba:2e:1d			
SSID	techPubNet	Associating Switch	Local Switch
BSSID	00:22:B0:3A:C9:90	Switch MAC Address	00:17:9A:95:1F:0C
AP MAC Address	00:22:B0:3A:C9:80	Switch IP Address	10.27.65.51
Status	Authenticated	Location	
Channel	11	Radio	2
User Name		VLAN	1
Inactive Period	0d:00:00:03	Transmit Data Rate	48 Mbps
Age	0d:00:00:01	Network Time	0d:00:04:11
Dot11n Capable	No	Detected IP Address	10.27.65.112
NetBIOS Name		Tunnel IP Address	

Figure 326: Associated Client Status Detail

[Table 292 on page 491](#) describes the information available on the **Detail** page for the associated client status.

Table 292: Detailed Associated Client Status

Field	Description
SSID	Indicates the network on which the client is connected.
BSSID	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.
AP MAC Address	This field indicates the base AP Ethernet MAC address for the managed AP.
Status	Indicates whether or not the client has associated and/or authenticated. The valid values are: <ul style="list-style-type: none"> • Associated: The client is current associated to the managed AP. • Authenticated: The client is currently associated and authenticated to the managed AP. • Disassociated: The client has disassociated from the managed AP, if the client does not roam to another managed AP within the client roam timeout, it will be deleted.
Channel	Indicates the operating channel for the client association.
User Name	Indicates the user name of client that have authenticated via 802.1X. Clients on networks with other security modes will not have a user name.
Inactive Period	This field shows the amount of time since data packets were last received from the client
Age	Indicates the amount of time that has passed since the switch received new status or statistics updates for this client.
Dot11n Capable	Indicates whether the associated client supports the IEEE 802.11n standard.
NetBIOS Name	Identifies the NetBIOS name of the wireless client. For Microsoft Windows hosts, the NetBIOS name is typically the same as, or based on the host name.
Associating Switch	Shows whether the AP that the wireless client is associated to is managed by the local switch or a peer switch.
Switch MAC Address	Shows the MAC address of the switch that manages the AP to which the wireless client is associated.
Switch IP Address	Shows the IP address of the switch that manages the AP to which the wireless client is associated.
Location	The descriptive location configured for the managed AP.
Radio	Displays the managed AP radio interface the client is associated to and its configured mode.
VLAN	If client is on a VAP using VLAN data forwarding mode, indicates the current assigned VLAN.
Transmit Data Rate	Indicates the rate at which the client station is currently transmitting data.
Network Time	Indicates the amount of time that has passed since this client first authenticated with the network.
Detected IP Address	Identifies the IPv4 address of the client, if available.
Tunnel IP Address	This field is blank for all non-tunneled clients. For a tunneled client, this is the assigned tunnel IP address.
Captive Portal	If client is authenticated via Captive Portal, this field contains a link to the associated Captive Portal client status page. Please note that this field is visible only for Captive Portal-enabled switch configurations.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the client from the managed AP.
- **Refresh**—Updates the page with the latest information.

Viewing Associated Client QoS Status

The **WLAN > Monitoring > Client > Associated Clients > Client QoS** page for the associated client status shows information about the bandwidth restrictions for each client associated to an AP managed by the switch. Use the menu above the table to select the MAC address of the client with the information to view.

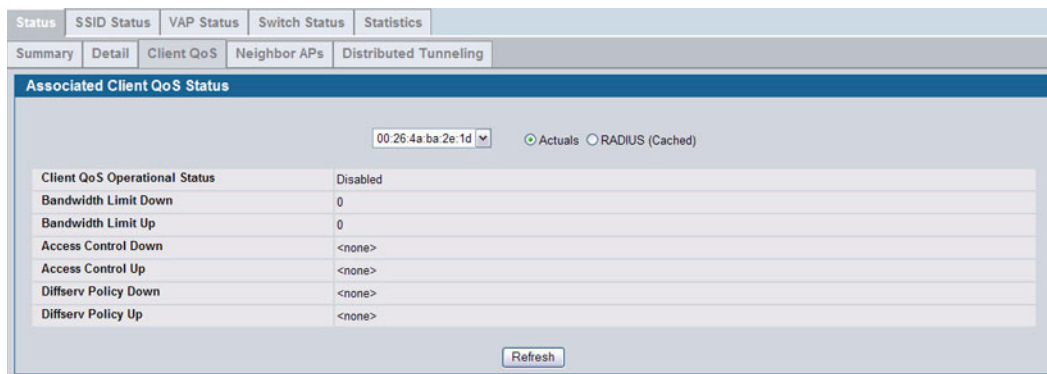


Figure 327: Associated Client QoS Status

Table 293 on page 492 describes the information available on the **Client QoS** page for the associated client status.

Table 293: Associated Client QoS Status

Field	Description
Actual RADIUS (Cached)	Use the selector to determine the source of the information the page displays: <ul style="list-style-type: none"> • Select Actual to display either the actual status parameters configured on the AP. • Select RADIUS (Cached) to display any client QoS parameters that were obtained for the client from a RADIUS server when using 802.1X authentication.
Client QoS Operational Status	Shows whether QoS is enforced for the client.
Bandwidth Limit Down	Shows the maximum rate at which the client receives traffic from the AP in bits per second. The rate shown in this field is the configured value rounded down to the nearest 64 kbps, A value of 0 means no bandwidth limiting is in effect in this direction.
Bandwidth Limit Up	Shows the maximum rate at which the client transmits traffic to the AP in bits per second. The rate shown in this field is the configured value rounded down to the nearest 64 kbps, A value of 0 means no bandwidth limiting is in effect in this direction.
Access Control Down	Shows which ACL, if any, is applied to traffic from the AP to the client.

Table 293: Associated Client QoS Status (Cont.)

Field	Description
Access Control Up	Shows which ACL, if any, is applied to traffic from the client to the AP.
Diffserv Policy Down	Shows which DiffServ policy, if any, is applied to traffic from the AP to the client.
Diffserv Policy Up	Shows which DiffServ policy, if any, is applied to traffic from the client to the AP.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Associated Client Neighbor AP Status

The **WLAN > Monitoring > Client > Associated Clients > Neighbor APs** page for the associated client status shows information about access points that the client detects. The information on this page can help you determine the managed AP an associated client might use for roaming. Use the menu above the table to select the MAC address of the client with the information to view.

**Figure 328: Associated Client Neighbor AP Status**

Table 294 describes the information available on the **Neighbor AP** page for the associated client status.

Table 294: Associated Client Neighbor AP Status

Field	Description
AP MAC Address	The base Ethernet address of the DWS-4000 Series switch managed AP.
Location	The configured descriptive location for the managed AP.
Radio	The radio interface and its configured mode that detected this client as a neighbor.

Table 294: Associated Client Neighbor AP Status (Cont.)

Field	Description
Discovery Reason	<p>Indicates one or more discovery methods for the neighbor client. One or more of the following values may be displayed:</p> <ul style="list-style-type: none"> • RF Scan: The client was reported from an RF scan on the radio. Note that client stations are difficult to detect via RF scan, the other methods are more common for client neighbor detection. • Probe Request: The managed AP received a probe request from the client. • Associated to Managed AP: This neighbor client is associated to another managed AP. • Associated to this AP: The client is associated to this managed AP on the displayed radio. • Associated to Peer AP: The client is associated to an AP managed by a peer switch. • Ad Hoc Rogue: The client was detected as part of an ad hoc network with this AP.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Associated Client Distributed Tunneling Status

The **WLAN > Monitoring > Client > Associated Clients > Distributed Tunneling** page for the associated client status shows information about access points that the client detects. The AP-AP tunneling mode is used to support L3 roaming for wireless clients without forwarding any data traffic to the wireless switch.

In the AP-AP tunneling mode, when a client first associates with an AP in the wireless system, the AP forwards the wireless client's data using VLAN forwarding mode. The AP the client initially associates with is called the *Home AP*. The AP the client roams to is called the *Association AP*.

Use the menu above the table to select the MAC address of the client with the information to view.

Associated Client Distributed Tunneling Status			
00:26:4a:ba:2e:1d			
Distributed Tunneling Status	Disabled	Home AP MAC Address	00:00:00:00:00:00
Client Roam Status	Roaming	Associated AP MAC Address	00:00:00:00:00:00
Refresh			

Figure 329: Associated Client Distributed Tunneling Status

Table 295 describes the information available on the **Distributed Tunneling** page for the associated client status.

Table 295: Associated Client Distributed Tunneling Status

Field	Description
Distributed Tunneling Status	Indicates whether this client is associated with a network that supports L2 distributed tunneling.
Client Roam Status	Indicates whether the client is on the Home AP or has roamed to another AP and is using a tunnel. The field can display one of the following values: <ul style="list-style-type: none">• Home—Client is not using a tunnel.• Roaming—Client is using a tunnel. If distributed tunneling is disabled, the field displays the roam status as Roaming.
Home AP MAC Address	Shows the MAC Address of the Home AP for the client. The value is meaningful only for clients that are associated with networks enabled for distributed tunneling.
Associated AP MAC Address	Shows the MAC Address of the AP to which the client roamed via the distributed tunneling protocol.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Associated Client TSPEC Status

The **TSPEC** page for the associated client status shows information about a client's active traffic streams. If there are no associated clients with active traffic streams, the page displays a message indicating that there are no traffic streams for any associated clients.

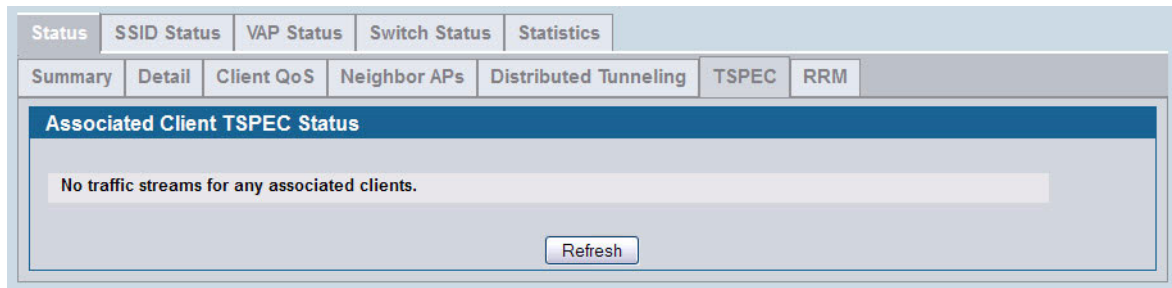


Figure 330: Associated Client TSPEC Status

Use the menu above the table to select the MAC address of the client with the information to view. Only clients with an active traffic stream appear in the selection list.

[Table 292](#) describes the information available on the **TSPEC** page for the associated client status.

Table 296: Associated Client TSPEC Status

Field	Description
Client MAC Address	MAC address of a client that has one or more active traffic streams on an AP managed by the switch.
Traffic Stream Identifier (TID)	Identifying number of the traffic stream as specified in the TSPEC. The TID range is 0–7.
Access Category (AC)	The access category to which the traffic stream corresponds, which is either voice or video.
Direction	The direction of the traffic stream as indicated in the TSPEC. The possible values are: <ul style="list-style-type: none"> • Uplink • Downlink • Bidirectional
User Priority (UP)	The user priority indicated in the TSPEC, which identifies the traffic stream or the client.
Medium Time	Medium time (bandwidth) allocated to the client for this traffic stream. This value is calculated by the AP using the TSPEC parameters provided by the client and is measured in 32μsec/sec units.
Excess Usage Events	Number of times the client has exceeded the medium time (bandwidth) established for its TSPEC.
BSSID	Basic service-set identifier. The MAC address of the (virtual) AP to which the client is associated.
SSID	Service set identifier. The network name assigned to the BSSID to which the client is associated.

Table 296: Associated Client TSPEC Status (Cont.)

Field	Description
Radio	Radio number to which the client is associated.
Roam TS (managed AP only)	Indicates whether this traffic stream was established by a roaming client.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Associated Client RRM Status

The **RRM Status** page for associated clients contains information about whether a client supports specific resource radio measurement features defined in the 802.11k specification.

Figure 331: Associated Client RRM Status

Use the menu above the table to select the MAC address of the client with the information to view.

Table 297: Associated Client RRM Status

Field	Description
Support Radio Resource Measurement	Indicates whether this client support 802.11k resource radio measurement.
Support RRM Location Configuration Reports	Indicates whether this client responds to location configuration requests.
Support RRM Beacon Table Measurement	Indicates whether this client can report detected APs via the beacon table report.
Support RRM Beacon Active Measurement	Indicates whether the client supports active scan capability.

Table 297: Associated Client RRM Status (Cont.)

Field	Description
Support RRM Beacon Passive Measurement	Indicates whether the client supports passive scan capability.
RRM Channel Load Measurement	Indicates whether the client supports channel load measurement

Command Buttons

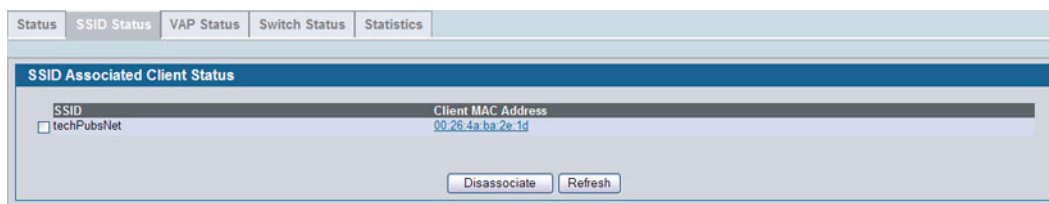
The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Associated Client SSID Status

Each managed AP can have up to 16 different networks that each have a unique SSID. Although several wireless clients might be connected to the same physical AP, they might not connect by using the same SSID. The **WLAN > Monitoring > Client > Associated Clients > SSID Status** page lists the SSIDs of the networks that each wireless client associated with a managed AP has used for WLAN access.

To disconnect a client from an AP, select the box next to the SSID, and then click **Disassociate**.

**Figure 332: SSID Associated Client Status****Table 298: SSID Associated Client Status**

Field	Description
SSID	Indicates the network on which the client is connected.
MAC Address	The Ethernet address of the client station.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the client from the managed AP.
- **Refresh**—Updates the page with the latest information.

Viewing Associated Client VAP Status

Each AP has 16 Virtual Access Points (VAPs) per radio, and every VAP has a unique MAC address (BSSID). The **WLAN > Monitoring > Client > Associated Clients > VAP Status** tab displays the **VAP Associated Client Status** page which shows information about the VAPs on the managed AP that have associated wireless clients. To disconnect a client from an AP, select the box next to the BSSID, and then click **Disassociate**.

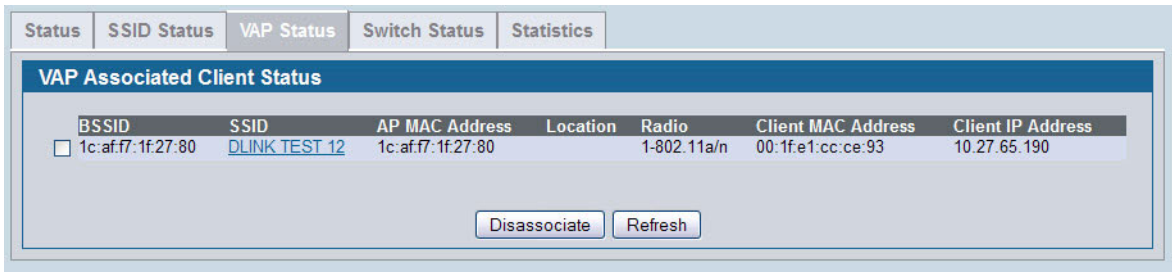


Figure 333: VAP Associated Client Status

Table 299: VAP Associated Client Status

Field	Description
BSSID	Indicates the Ethernet MAC address for the managed AP VAP where this client is associated.
SSID	Indicates the SSID for the managed AP VAP where this client is associated.
AP MAC Address	This field indicates the base AP Ethernet MAC address for the managed AP.
Location	The descriptive location configured for the managed AP.
Radio	Displays the managed AP radio interface the client is associated to and its configured mode.
Client MAC Address	The Ethernet address of the client station.
Client IP Address	The IP address of the client station.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the client from the managed AP.
- **Refresh**—Updates the page with the latest information.

Switch Associated Client Status

The **WLAN > Monitoring > Client > Associated Clients > Switch Status** tab displays the **Switch Associated Client Status** page which shows information about the switch that manages the AP to which the client is associated.

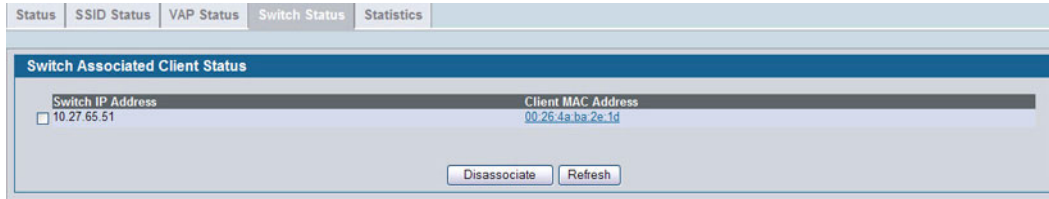


Figure 334: Switch Associated Client Status

To disconnect a client from an AP, select the box next to the switch IP address, and then click **Disassociate**.

Table 300: Switch Associated Client Status

<i>Field</i>	<i>Description</i>
Switch IP Address	Shows the IP address of the switch that manages the AP to which the client is associated.
Client MAC Address	Shows the MAC address of the associated client.

Command Buttons

The page includes the following buttons:

- **Disassociate**—Disassociates the client from the managed AP.
- **Refresh**—Updates the page with the latest information.

Viewing Associated Client Statistics

A wireless client can roam among APs without interruption in WLAN service. The DWS-4000 Series switch tracks the traffic the client sends and receives during the entire wireless session while the client roams among APs that the switch manages. The switch stores statistics about client traffic while it is associated with a single AP as well as throughout the roaming session.

The statistics on the **WLAN > Monitoring > Client > Associated Clients > Statistics > Association Summary** displays the **Associated Client Statistics** page. This page shows information about the traffic a wireless client receives and transmits while it is associated with a single AP.

MAC Address	Packets Received	Bytes Received	Packets Transmitted	Bytes Transmitted
00:1fe1:cc:ce:93	11	891	11	1056

Figure 335: Associated Client Association Summary Statistics

Table 301: Associated Client Association Summary Statistics

Field	Description
MAC Address	The Ethernet address of the client station.
Packets Received	Packets received from the client station.
Bytes Received	Bytes received from the client station.
Packets Transmitted	Packets transmitted to the client station.
Bytes Transmitted	Bytes transmitted to the client station.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Associated Client Session Summary Statistics

The statistics on the **WLAN > Monitoring > Client > Associated Clients > Statistics > Session Summary** page show information about the traffic a wireless client receives and transmits while it is connected to the same WLAN network shared by APs that the switch manages.

MAC Address	Packets Received	Bytes Received	Packets Transmitted	Bytes Transmitted
00:26:4a:ba:2e:1d	826	94449	656	259087

Figure 336: Associated Client Statistics Session Summary

If the client roams from one AP to another AP but remains connected to the same network, the session continues and the session statistics continue to accumulate. If the client closes the wireless connection or roams out of the range of an AP managed by the switch, the session ends.

Table 302: Associated Client Session Summary Statistics

Field	Description
MAC Address	The Ethernet address of the client station.
Packets Received	Packets received from the client station.
Bytes Received	Total bytes received from the client station.
Packets Transmitted	Total packets transmitted to the client station.
Bytes Transmitted	Total bytes transmitted to the client station.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detailed Associated Client Association Statistics

The statistics on the **WLAN > Monitoring > Client > Associated Clients > Statistics > Association Detail** tab displays the **Associated Client Statistics** page. This page shows information about the traffic a wireless client receives and transmits while it is associated with a single AP. Use the menu above the table to view details about an associated client. Each client is identified by its MAC address.

Associated Client Statistics			
00:26:4a:ba:2e:1d			
Packets Received	702	Bytes Received	58127
Packets Transmitted	691	Bytes Transmitted	120402
Packets Receive Dropped	0	Bytes Receive Dropped	0
Packets Transmit Dropped	0	Bytes Transmit Dropped	0
Fragments Received	0	Fragments Transmitted	645
Transmit Retries	250	Transmit Retries Failed	48
Duplicates Received	66		

Figure 337: Associated Client Association Detail Statistics

Table 303: Associated Client Association Detail Statistics

Field	Description
Packets Received	Total packets received from the client station.
Bytes Received	Total bytes received from the client station.
Packets Transmitted	Total packets transmitted to the client station.
Bytes Transmitted	Total bytes transmitted to the client station.
Packets Receive Dropped	Number of packets received from the client station that were dropped.
Bytes Receive Dropped	Number of bytes received from the client station that were dropped.
Packets Transmit Dropped	Number of packets transmitted to the client station that were dropped.
Bytes Transmit Dropped	Number of bytes transmitted to the client station that were dropped.
Fragments Received	Total fragmented packets received from the client station.
Fragments Transmitted	Total fragmented packets transmitted to the client station.
Transmit Retries	Number of times transmits to client station succeeded after one or more retries.
Transmit Retries Failed	Number of times transmits to client station failed after one or more retries.
Duplicates Received	Total duplicate packets received from the client station.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detailed Associated Client Session Statistics

The statistics on the **WLAN > Monitoring > Client > Associated Clients > Statistics > Session Detail** page show information about the traffic a wireless client receives and transmits while it is connected to the same WLAN network shared by APs that the switch manages. Use the menu above the table to view details about an associated client. Each client is identified by its MAC address.

Associated Client Statistics			
00:26:4a:ba:2e:1d			
Packets Received	1877	Bytes Received	177698
Packets Transmitted	1926	Bytes Transmitted	763915
Packets Receive Dropped	0	Bytes Receive Dropped	0
Packets Transmit Dropped	0	Bytes Transmit Dropped	0
Fragments Received	0	Fragments Transmitted	1795
Transmit Retries	609	Transmit Retries Failed	133
Duplicates Received	141		

Figure 338: Associated Client Session Detail Statistics

Table 304: Associated Client Session Detail Statistics

Field	Description
Packets Received	Total packets received from the client station.
Bytes Received	Total bytes received from the client station.
Packets Transmitted	Total packets transmitted to the client station.
Bytes Transmitted	Total bytes transmitted to the client station.
Packets Receive Dropped	Number of packets received from the client station that were dropped.
Bytes Receive Dropped	Number of bytes received from the client station that were dropped.
Packets Transmit Dropped	Number of packets transmitted to the client station that were dropped.
Bytes Transmit Dropped	Number of bytes transmitted to the client station that were dropped.
Fragments Received	Total fragmented packets received from the client station.
Fragments Transmitted	Total fragmented packets transmitted to the client station.
Transmit Retries	Number of times transmits to client station succeeded after one or more retries.
Transmit Retries Failed	Number of times transmits to client station failed after one or more retries.
Duplicates Received	Total duplicate packets received from the client station.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detailed Associated Client TSPEC Statistics

The statistics on the **TSPEC** page show information about each client's active traffic streams. If there are no associated clients with active traffic streams, the page displays a message indicating that there are no traffic streams for any associated clients.



Note: The client TSPEC statistics do not persist across any client disassociation event, including a client roam. The TSPEC statistics reset any time a client disassociates from an AP.

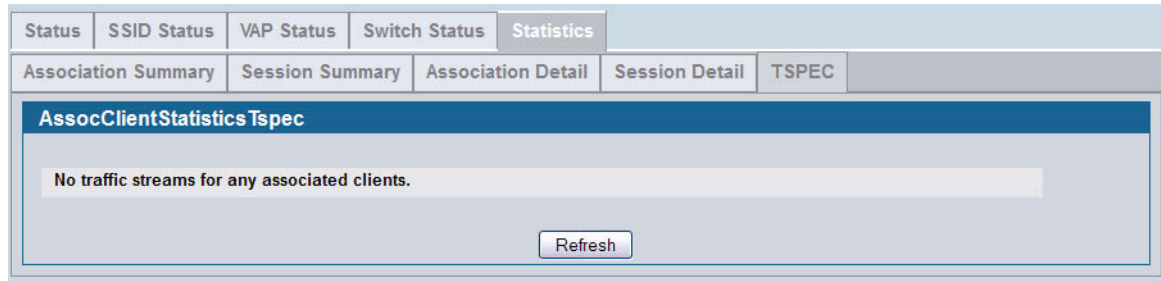


Figure 339: Associated Client Session Detail Statistics

Use the menu above the table to select the MAC address of the client with the information to view. Only clients with an active traffic stream appear in the selection list.

Table 305: Associated Client TSPEC Statistics

Field	Description
TS Packets Received	Count of packets received by an AP from a wireless client for the specified access category.
TS Bytes Received	Count of bytes received by an AP from a wireless client for the specified access category.
TS Packets Transmitted	Count of packets transmitted by an AP to a wireless client for the specified access category.
TS Bytes Transmitted	Count of bytes transmitted by an AP to a wireless client for the specified access category.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Ad Hoc Client Status

An ad hoc client is a wireless client that gains access to the WLAN through a wireless client that is associated with an access point. The ad hoc client does not communicate directly with the AP. Ad hoc networks are a particular concern because they consume RF bandwidth and can present a security risk.

From the **WLAN > Monitoring > Client > Ad Hoc Clients** page, you can view and manage wireless clients that are connected to the WLAN through an ad hoc network.

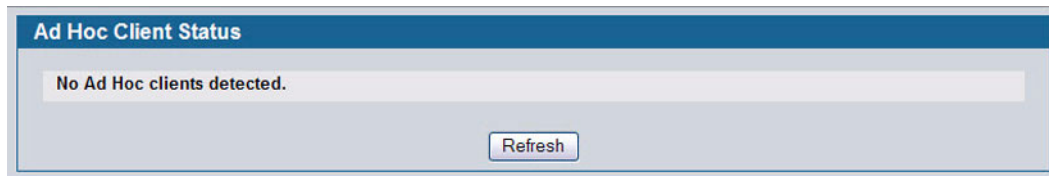


Figure 340: Ad Hoc Clients

To view or configure the default action specified for a wireless client (Allow, Deny, or Global Action), go to the **WLAN > Administration > Advanced Configuration > Clients > Known Client** page and click the MAC address of the client to view or configure.

The switch does not remove MAC entries from this list even when a client successfully authenticates with an AP. The historical ad hoc data gives you more time to take action against clients that establish ad hoc networks on the WLAN.

Table 306: Ad Hoc Client Status

Field	Description
MAC Address	The Ethernet address of the client. If the Detection Mode is Beacon then the client is represented as an AP in the RF Scan database and the Neighbor AP List. If the Detection Mode is Data Frame then the client information is in the Neighbor Client List.
AP MAC Address	The base Ethernet MAC Address of the managed AP which detected the client.
Location	The configured descriptive location for the managed AP.
Radio	The radio interface and its configured mode that detected the ad hoc device.
Detection Mode	The mechanism of detecting this Ad Hoc device. The possible values are Beacon Frame or Data Frame.
Age	Time since last detection of the ad hoc network.

Command Buttons

The page includes the following buttons:

- **Delete All**—Deletes all ad hoc client entries from the list. Clearing the list does not disassociate any of the ad hoc clients, and the clients might still be involved in the ad hoc network.
- **Deny**—Blocks an ad hoc client from WLAN access. The MAC address is added to the Known Client database where the default action is Deny.

- **Allow**—Allows an ad hoc client access to the WLAN. The MAC address is added to the Known Client database where the default action is Allow.
- **Refresh**—Updates the page with the latest information.



Note: If the **Deny** button is not available, it means all profiles use Allow as the default MAC Authentication action. Likewise, if the **Allow** button is not available, no profiles have an Allow default action.



Note: If you use RADIUS for MAC authentication in one or more AP profiles, you must add the MAC Address of the client to the RADIUS database.

Detected Client Status

Wireless clients are detected by the wireless system when the clients either attempt to interact with the system or when the system detects traffic from the clients. The **Detected Client Status** page contains information about clients that have authenticated with an AP as well information about clients that disassociate and are no longer connected to the system. To access the page click **WLAN > Monitoring > Client > Detected Clients**.

The Cluster Controller receives information about associated clients from all switches in the cluster, and you can disassociate clients on any AP in the cluster from the Cluster Controller.

Detected Client Status				
MAC Address	Client Name	Client Status	Age	Create Time
<input type="checkbox"/> 00:0c:41:dc:00:90		Known	0d:00:02:20	1d:03:45:06
<input type="checkbox"/> 00:0e:84:e2:11:50		Known	0d:00:00:20	1d:03:51:31
<input type="checkbox"/> 00:0e:84:f5:f2:d0		Rogue	0d:00:00:20	1d:03:51:31
<input type="checkbox"/> 00:10:18:97:00:e4		Detected	0d:04:50:46	0d:04:52:20
<input type="checkbox"/> 00:10:18:97:00:f2		Detected	0d:04:53:49	0d:05:14:19
<input type="checkbox"/> 00:11:50:e2:ba:5a		Rogue	0d:00:00:50	1d:03:52:01
<input type="checkbox"/> 00:14:6c:59:d1:99		Rogue	0d:00:00:20	1d:03:51:31
<input type="checkbox"/> 00:15:2b:92:c9:a0		Rogue	0d:00:00:20	1d:03:51:31
<input type="checkbox"/> 00:16:01:73:03:1f		Rogue	0d:00:23:29	0d:23:19:36
<input type="checkbox"/> 00:19:7e:44:c3:4d		Rogue	0d:00:00:20	1d:03:52:01
<input type="checkbox"/> 00:19:7e:88:60:9e		Rogue	0d:00:01:20	0d:05:10:19
<input type="checkbox"/> 00:19:7e:88:61:7e		Detected	0d:06:16:49	0d:06:55:49
<input type="checkbox"/> 00:19:7e:88:61:81		Detected	0d:01:17:03	1d:03:41:36
<input type="checkbox"/> 00:19:7e:88:61:86		Rogue	0d:00:10:50	0d:01:18:33
<input type="checkbox"/> 00:19:7e:90:c1:3f		Detected	0d:21:08:50	1d:03:52:01
<input type="checkbox"/> 00:19:7e:90:c2:3d		Rogue	0d:00:23:29	0d:06:08:49
<input type="checkbox"/> 00:19:7e:90:c6:ac		Rogue	0d:00:00:20	1d:03:52:01
<input type="checkbox"/> 00:19:7e:90:c6:ad		Detected	0d:04:38:46	0d:04:39:20
<input type="checkbox"/> 00:19:7e:90:c6:ae		Detected	0d:07:47:49	0d:07:49:20
<input type="checkbox"/> 00:19:7e:90:c6:af		Detected	0d:06:27:20	0d:06:27:20

1 2 3

Figure 341: Detected Client Status

To learn more about a client listed on the page, click the MAC address of the client.

Table 307: Detected Client Status

Field	Description
MAC Address	The Ethernet address of the client.
Client Name	Shows the name of the client, if available, from the Known Client Database. If client is not in the database then the field is blank.
Client Status	Shows the client status, which can be one of the following: <ul style="list-style-type: none"> • Authenticated—The wireless client is authenticated with the wireless system. • Detected—The wireless client is detected by the wireless system but is not a security threat. • Black-Listed—The client with this MAC address is specifically denied access via MAC Authentication. • Rogue—The client is classified as a threat by one of the threat detection algorithms.
Age	Time since any event has been received for this client that updated the detected client database entry.
Create Time	Time since this entry was first added to the detected clients database.

Command Buttons

The page includes the following buttons:

- **Delete**—Delete the selected client from the list. If the client is detected again, it will be added to the list.
- **Delete All**—Deletes all non-authenticated clients from the Detected Client database. As clients are detected, they are added to the database and appear in the list.
- **Acknowledge All Rogues**—Clear the rogue status of all clients listed as rogues in the Detected Client database, The status of an acknowledge client is returned to the status it had when it was first detected. If the detected client fails any of the tests that classify it as a threat, it will be listed as a Rogue again
- **Refresh**—Updates the page with the latest information.

Viewing Detailed Detected Client Status

The detailed **Detected Client Status** page shows information about specific clients detected on the wireless network. To view information about other clients detected on the network, return to the **Detected Clients** page and click a different client MAC address.

Detected Client Status			
MAC address	00:10:18:97:00:e4	Auth Msgs Recorded	0
Client Status	Detected	Auth Collection Interval	0d:00:00:56
Authentication Status	Not Authenticated	Highest Auth Msgs	0
Threat Detection	Detected	De-Auth Msgs Recorded	0
Threat Mitigation Status	Not Done	De-Auth Collection Interval	0d:00:00:56
Time Since Entry Last Updated	0d:04:53:30	Highest De-Auth Msgs	0
Time Since Entry Create	0d:04:55:04	Authentication Failures	0
Client Name		Probes Detected	4
RSSI	4	Broadcast BSSID Probes	2
Signal	-88	Broadcast SSID Probes	2
Noise	-95	Specific BSSID Probes	0
Probe Req Recorded	0	Specific SSID Probes	0
Probe Collection Interval	0d:00:00:56	Last Non-Broadcast BSSID	00:00:00:00:00:00
Highest Probes Detected	0	Last Non-Broadcast SSID	
Channel	6	Threat Mitigation Sent	0d:00:00:00
OUI Description	BROADCOM CORPORATION		

Figure 342: Detailed Detected Client Status

Table 308: Detailed Detected Client Status

Field	Description
MAC Address	The Ethernet address of the client.
Client Status	Shows the client status, which can be one of the following: <ul style="list-style-type: none"> • Authenticated—Client is Authenticated with the system and is not Rogue. • Detected—Client is detected, not Authenticated, not rogue, and is not found in the Known Clients Database. • Known—Client is detected and found in the Known Clients Database, but is not authenticated. • Black-Listed—Client tried to associate with the system, but was rejected due to MAC authentication. • Rogue—Client failed the enabled threat tests.
Authentication Status	Indicates whether this client is authenticated. Note: The Client Status can be Rogue, but the authentication status can still be Authenticated.
Threat Detection	Indicates whether one of the threat detection tests has been triggered for this client. If the test is disabled, the client will not be marked as a rogue, but you can still investigate why the threat was triggered.

Table 308: Detailed Detected Client Status (Cont.)

Field	Description
Threat Mitigation Status	Indicates whether threat mitigation has been done for this client.
Time Since Entry Last Updated	Shows the amount of time that has passed since any event has been received for this client that updated the detected client database entry.
Time Since Entry Create	Shows the amount of time that has passed since this entry was first added to the detected clients database.
Client Name	Shows the name of the client, if available, from the Known Client Database. If the client is not in the database then the field is blank.
RSSI	If the client is authenticated with the managed AP, this field displays the last RSSI value reported by the AP with which the client is authenticated. The RSSI is a percentage from 1–100%. A value of 0 means the AP is not detected.
Signal	Last signal strength reported by the managed AP with which the client is authenticated. The possible range is –128 to 128 dBm.
Noise	Last channel noise reported by the managed AP with which the client is authenticated. The possible range is –128 to 128 dBm.
Probe Req Recorded	Number of probe requests recorded so far during the probe collection interval.
Probe Collection Interval	Shows the amount of time spent in each probe collection period. The probe collection helps the switch decide whether the client is a threat.
Highest Probes Detected	Shows the largest number of probes that the switch detected during a probe collection interval.
Channel	Identifies the channel that the client is using.
Auth Msgs Recorded	Shows the number of IEEE 802.11 Authentication messages recorded so far during the authentication collection interval.
Auth Collection Interval	Shows the amount of time spent in each authentication collection period. The authentication collection helps the switch decide whether the client is a threat.
Highest Auth Msgs	Shows the largest number of authentication messages that the switch detected during an authentication collection interval.
De-Auth Msgs Recorded	Shows the number of IEEE 802.11 De-Authentication messages recorded so far during the deauthentication collection interval.
De-Auth Collection Interval	Shows the amount of time spent in each de-authentication collection period. The deauthentication collection helps the switch decide whether the client is a threat.
Highest De-Auth Msgs	Shows the largest number of de-authentication messages that the switch detected during a deauthentication collection interval.
Authentication Failures	Shows the number of 802.1X Authentication failures detected for this client.
Probes Detected	Shows the number of probes detected in the last RF Scan.
Broadcast BSSID Probes	Shows the number of probes to broadcast BSSID in the last RF Scan.
Broadcast SSID Probes	Shows the number of probes to broadcast SSID in the last RF Scan.
Specific BSSID Probes	Shows the number of probes to a specific BSSID in the last RF Scan.
Specific SSID Probes	Shows the number of probes to a specific SSID in the last RF Scan
Last Directed Probe BSSID	Shows the last directed probe BSSID detected in the RF Scan, which is a MAC address.

Table 308: Detailed Detected Client Status (Cont.)

Field	Description
Last Directed Probe SSID	Shows the name of the last directed Probe SSID detected in the RF Scan.
Threat Mitigation Sent	Shows the amount of time that has passed since the switch sent the last threat mitigation message to this client.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Acknowledge Rogue**—Clear the rogue status of the client in the Detected Client database, The status of an acknowledge client is returned to the status it had when it was first detected. If the detected client fails any of the tests that classify it as a threat, it will be listed as a Rogue again

Viewing WIDS Client Rogue Classification

The Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network. The DWS-4000 Series switch allows you to activate or deactivate various threat detection tests and set threat detection thresholds. The **WIDS Client Rogue Classification** page provides information about the results of these tests. If a client has been classified as a rogue, this page provides information about which tests the client might have failed to trigger the classification.

To view WIDS information about another client detected through the RF Scan, return to the main **Detected Clients** page and click the MAC address of the client with the information to view.

WIDS Client Rogue Classification							
MAC Address : 00:19:7d:28:1d:11							
Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Known Client Database Test	True	1c:af:f7:1f:27:80	1	Disabled		0d:18:31:51	0d:02:40:52
Client exceeds configured rate for auth msgs	False	1c:af:f7:1f:27:80	1	Enabled		0d:19:52:35	0d:02:40:52
Client exceeds configured rate for probe msgs	False	1c:af:f7:1f:27:80	1	Enabled		0d:19:52:35	0d:02:40:52
Client exceeds configured rate for de-auth msgs	False	1c:af:f7:1f:27:80	1	Enabled		0d:19:52:35	0d:02:40:52
Client exceeds max failing authentications	False	1c:af:f7:1f:27:80	1	Enabled		0d:19:52:35	0d:02:40:52
Known client authenticated with unknown AP	False	1c:af:f7:1f:27:80	1	Disabled		0d:19:52:35	0d:02:40:52
Client OUI not in the OUI Database	False	1c:af:f7:1f:27:80	1	Disabled		0d:19:52:35	0d:02:40:52

Refresh

Figure 343: WIDS Client Rogue Classification

The following table shows information about the security test performed on the detected client.

Table 309: WIDS Client Rogue Classification

Field	Description
MAC Address	The Ethernet MAC address of the detected wireless client.
Test Description	Identifies the tests that were performed, which includes the following: <ul style="list-style-type: none"> • Client is denied access in the Known Client Database. • Client exceeds the configured rate for transmitting 802.11 authentication requests. • Client exceeds the configured rate for transmitting probe requests. • Client exceeds the configured rate for transmitting de-authentication requests. • Client exceeds the maximum number of failing authentications. • Known Client is authenticated with an Unknown AP.
Condition Detected	Indicates whether the result of the test was true or false.
Reporting MAC Address	Identifies the MAC address of the AP that reported the test results.
Radio	Identifies which physical radio on the reporting AP was responsible for the test results.
Test Config	Shows whether this test is configured to report rogues. Each test can be globally enabled or disabled to report a positive result as a rogue.
Test Result	Shows whether this test reported the device as rogue. In some cases the test may report a positive result, be enabled, but not report the device as rogue because the device is allowed to operate in this mode.
Time Since First Report	Time stamp indicating how long ago this test first detected the condition.
Time Since Last Report	Time stamp indicating how long ago this test last detected the condition.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detected Client Pre-Authentication History

To help authenticated clients roam without losing sessions and needing to re-authenticate, wireless clients can attempt to authenticate to other APs within range that the client could possibly associate with. For successful pre-authentication, the target AP must have a VAP with an SSID and security configuration that matches that of the client, including MAC authentication, encryption method, and pre-shared key or RADIUS parameters. The AP that the client is associated with captures all pre-authentication requests and sends them to the switch.

The **Detected Client Pre-Authentication History** page shows information about the pre-authentication requests that the detected client has made.

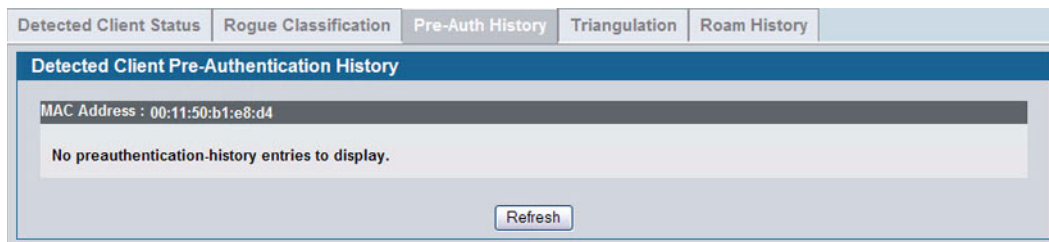


Figure 344: Detected Client Pre-Authentication History

Table 310 describes the fields on the **Detected Client Pre-Authentication History** page.

Table 310: Detected Client Pre-Authentication History

<i>Field</i>	<i>Description</i>
MAC Address	MAC address of the client.
AP MAC Address	MAC Address of the managed AP to which the client has pre-authenticated.
Radio Interface Number	Radio number to which the client is authenticated, which is either Radio 1 or Radio 2.
VAP MAC Address	VAP MAC address to which the client roamed.
SSID	SSID Name used by the VAP.
Age	Time since the history entry was added.
User Name	Indicates the user name of client that authenticated via 802.1X.
Pre-Authentication Status	Indicates whether the client successfully authenticated and shows a status of Success or Failure.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detected Client Triangulation

The **Detected Client Triangulation** page lists up to three non-sentry and three sentry managed APs that have detected the client. The signal strength reported by the APs can help triangulate the location of the client. Since an AP can have one radio configured in sentry mode and another radio configured in non-sentry mode, the same AP might appear in both lists. If the AP or the Client has not been detected by three APs, the list can contain zero, one or two entries.

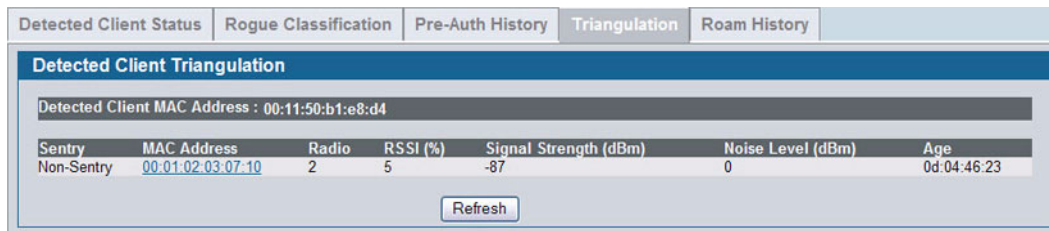


Figure 345: Detected Client Triangulation

Table 311 describes the fields on the **Detected Client Triangulation** page.

Table 311: Detected Client Triangulation

Field	Description
Detected Client MAC Address	MAC address of the client.
Sentry	Identifies whether the radio that detected the client is in sentry or non-sentry mode. <ul style="list-style-type: none"> Non-Sentry: The radio that detected the client is not configured in sentry mode. This means the radio can accept connections from wireless clients and send and receive traffic Sentry: The radio that detected the client is configured in sentry mode. Networks that deploy sentry APs or radios can detect devices on the network quicker and perform more thorough security analysis.
MAC Address	MAC Address of the managed AP that detected the client.
Radio	Radio number to which the client is authenticated, which is either Radio 1 or Radio 2.
RSSI	Received signal strength indicator in terms of percentage for the non-sentry AP. The range is 0–100, where the maximum value is 100. A value of 0 indicates that the client is not detected.
Signal Strength	Received signal strength in dBm. The possible range is –127 to 127. However, realistically, this value is expected to range from –95 to –10.
Noise Level	Noise reported on the channel by the non-sentry AP. The possible range is –127 to 127.
Age	Time since this AP detected the signal.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Viewing Detected Client Roam History

The wireless system keeps a record of clients as they roam from one managed AP to another managed AP. A history of up to 10 APs is kept for each client. The **Detected Client Roam History** page shows the managed APs with which the client has associated.

The first entry in the client list is the oldest. After the list fills up, the oldest entry is deleted and all other entries are moved one slot up.

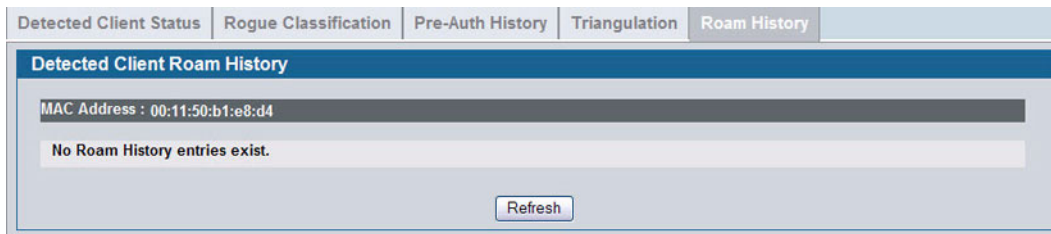


Figure 346: Detected Client Roam History

The following table describes the fields on the **Detected Client Roam History** page.

Table 312: Detected Client Roam History

Field	Description
MAC Address	MAC address of the detected client.
AP MAC Address	MAC Address of the managed AP to which the client authenticated.
Radio Interface Number	Radio Number to which the client is authenticated.
VAP MAC Address	VAP MAC address to which the client roamed.
SSID	SSID Name used by the VAP.
New Authentication	A flag indicating whether the history entry represents a new authentication or a roam event.
Age	Time since the history entry was added.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Detected Client Pre-Authentication Summary

To help authenticated clients roam without losing sessions and needing to re-authenticate, wireless clients can attempt to authenticate to other APs within range that the client could possibly associate with. For successful pre-authentication, the target AP must have a VAP with an SSID and security configuration that matches that of the client, including MAC authentication, encryption method, and pre-shared key or RADIUS parameters. The AP that the client is associated with captures all pre-authentication requests and sends them to the switch.

The **Detected Client Pre-Authentication History Summary** page lists detected clients that have made pre-authentication requests and identifies the APs that have received the requests.



Figure 347: Detected Client Pre-Authentication History Summary

The following table describes the fields on the **Detected Client Pre-Authentication History Summary** page.

Table 313: Detected Client Pre-Authentication History Summary

<i>Field</i>	<i>Description</i>
MAC Address	MAC address of the client.
AP MAC Address	MAC Address of the managed AP to which the client has pre-authenticated. This field can show a history of up to ten pre-authentications for each client.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Detected Client Roam History Summary

The wireless system keeps a record of clients as they roam from one managed AP to another managed AP. A history of up to 10 APs is kept for each client. The **Detected Client Roam History Summary** page lists each client that has roamed from at least one AP and provides information about the roaming history.

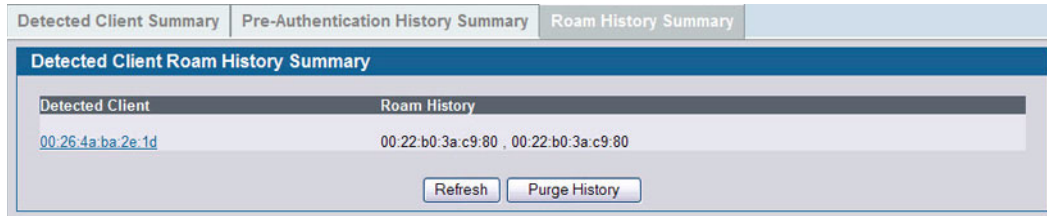


Figure 348: Detected Client Roam History Summary

The following table describes the fields on the **Detected Client Roam History Summary** page.

Table 314: Detected Client Roam History

<i>Field</i>	<i>Description</i>
MAC Address	MAC address of the detected client.
AP MAC Address	MAC Address of the managed AP to which the client authenticated. This field lists the MAC address of the last 10 APs to which the client has roamed and authenticated.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Radio Resource Measurement Status Information

The Radio Resource Measurement (RRM) feature enables the Wireless System to provide information to the wireless clients to help them make roaming decisions. The RRM feature also enables the Wireless system to gather information from wireless clients.

The RRM feature implements a subset of the radio resource measurement capabilities defined by the IEEE 802.11k standard.

Viewing the RRM Channel Load Configuration

The **RRM Channel Load Configuration** page allows you to ask a client to measure utilization on a specified channel for a specified duration. The page displays the results of the currently loaded channel.

The Channel Load feature is intended for network debugging. The Wireless System does not take any automatic actions based on the reported channel utilization.

Figure 349: RRM Channel Load Configuration

The following table describes the fields on the **RRM Channel Load Configuration** page.

Table 315: RRM Channel Load Configuration

Field	Description
Current Request Status	
Client MAC Address	Shows the MAC Address of the client with the channel load currently being measured.
Channel	Shows the channel the client uses to measure the load.
Measurement Duration	Number of time units (TUs) for which to measure the channel. Each TU is equal to 1024 μ s.

Table 315: RRM Channel Load Configuration (Cont.)

Field	Description
Channel Load Measurement Status	Status of the current measurement, which is one of the following: <ul style="list-style-type: none"> • Not Started • In Progress • Success—Last measurement completed. • Timed Out—Last measurement timed out. • Aborted—Administrator aborted the last request. • Incapable—Client is not capable of taking the requested measurement. • Refused—Client refused to perform the measurement.
Time Remaining	Number of seconds before the measurement request times out.
<i>New Request Configuration</i>	
Client MAC Address	Enter the MAC address of the client to measure its channel load.
Channel	Enter the channel the client should use to measure the load.
Duration	Enter the number of time units (TUs) for which to measure the channel. Each TU is equal to 1024 μ s.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Abort**—Cancel the current measurement request.
- **Refresh**—Updates the page with the latest information.

Viewing the RRM Channel Load History

The **RRM Channel Load History** page shows the last 100 channel load history entries. If a new entry is added when the list is full then the oldest entry is purged.

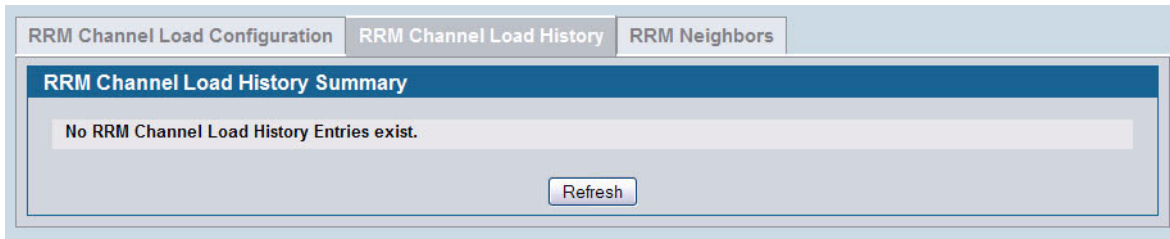


Figure 350: RRM Channel Load History

The following table describes the fields on the **RRM Channel Load History** page.

Table 316: RRM Channel Load History

Field	Description
Client MAC Address	MAC Address of the client that reported the channel load measurement.
Channel	Channel on which the client measured utilization.
Duration	How long the client measured the channel. The value is in time units (TUs). for which to measure the channel. Each TU is equal to 1024 μ s.
Channel Load	Measured Channel Load. The value is reported in terms of percentage utilization.
Age	Time since this measurement was reported.

Command Buttons

The page includes the following buttons:

- **Delete All**—Remove all entries from the list.
- **Refresh**—Updates the page with the latest information.

Viewing RRM Neighbors

The **RRM Neighbors Summary** page shows neighbor information for each VAP. This table is visible only from the Cluster Controller. The Cluster Controller builds the neighbor summary table from RF Scan reports, from the list of managed APs in the cluster, and from the information available in the profile configuration database.

Use the drop-down menu to view RRM neighbors for a specific AP (identified by MAC address) or to view RRM neighbors for all APs.

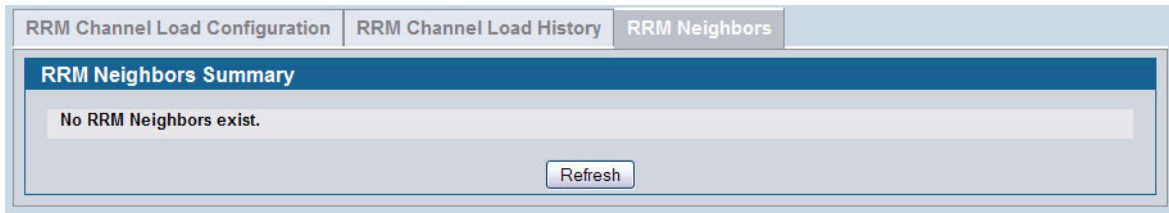


Figure 351: RRM Neighbors

The following table describes the fields on the **RRM Neighbors Summary** page.

Table 317: RRM Neighbors Summary

Field	Description
AP MAC Address	The MAC address of the managed AP.
VAP MAC Address	The VAP on the managed AP to which the neighbors apply.
Neighbor MAC Address	The MAC address of the detected neighbor VAP.
RSSI	The signal strength with which this neighbor is detected
SSID	Network name on which the VAP and the neighbor are operating.
Channel	Channel on which the neighbor is operating.
Age	Number of seconds since the neighbor AP was detected and reported via the RF-Scan report.

Command Buttons

The page includes the following button:

- **Delete All**—Remove all entries from the list.
- **Refresh**—Updates the page with the latest information.

WDS-Managed AP Information

The Wireless Distribution System (WDS)-Managed AP feature allows you to add managed APs to the cluster using over-the-air WDS links through other managed APs. With WDS, APs may be located outdoors where wired connection to the data network is unavailable, or in remote buildings that are not connected to the main campus with a wired network.

The WDS AP group consists of the following managed APs:

- Root AP — Acts as a bridge or repeater on the wireless medium and communicates with the switch via the wired link
- Satellite AP — Communicates with the switch via a WDS link to the root AP

The WDS links are secured using WPA2 Personal authentication and AES encryption.

For more information about the WDS feature, see [“Configuring the Wireless Distribution System” on page 626](#)

WDS Group Status Summary

The **WDS Group Status Summary** page displays summary information about configured WDS links. At least one group must be configured for the fields to display. To configure a WDS AP group, use the pages available within the **WLAN > WDS** folder.

Group Id	Configured AP Count	Connected Root AP Count	Connected Satellite AP Count	Configured WDS Link Count	Detected WDS Links Count
1	2	1	0	1	0
2	2	0	0	1	0

Figure 352: WDS Group Status Summary

The following table describes the fields on the **WDS Group Status Summary** page.

Table 318: WDS Group Status Summary

Field	Description
Group ID	Unique number that identifies the WDS AP group
Configured AP Count	Number of APs configured in this WDS AP group
Connected Root AP Count	Number of root APs currently being managed by the switch that are members of this WDS AP group.
Connected Satellite AP Count	Number of satellite APs currently being managed by the switch that are members of this WDS AP group.

Table 318: WDS Group Status Summary (Cont.)

Field	Description
Configured WDS Link Count	Number of configured bidirectional links in the WDS AP group.
Detected WDS Links Count	Number of WDS links detected in the system. APs on both sides of the link must detect each other in order for the link to be counted.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

WDS AP Group Status

The **WDS AP Group Status** page displays detailed information about the configured APs and links in the WDS Group. From this page, you can also send a new password to group members.

Figure 353: WDS AP Group Status

The following table describes the fields on the **WDS AP Group Status** page.

Table 319: WDS AP Group Status

Field	Description
Group ID	Use the drop-down menu above the fields to select the group number that identifies the configured WDS AP group.
Configured AP Count	Number of APs configured in this WDS AP group
Connected AP Count	Number of APs managed by the switch that are members of this WDS AP group. This number is the sum of the connected root APs and connected satellite APs.
Root AP Count	Number of root APs currently being managed by the switch that are members of this WDS AP group.

Table 319: WDS AP Group Status (Cont.)

Field	Description
Satellite AP Count	Number of satellite APs currently being managed by the switch that are members of this WDS AP group.
Root Bridge AP MAC	MAC Address of the device elected as the Spanning Tree Root Bridge. If spanning tree is disabled this value is 00:00:00:00:00:00.
Root Device Type	The type of device elected as the Spanning Tree Root bridge: <ul style="list-style-type: none"> • None (STP is disabled) • Root AP • Satellite AP • External Device (STP Root is not one of the APs)
Config WDS Link Count	Number of configured bidirectional links in the WDS AP group.
Detect WDS Links Count	Number of WDS links detected in the system. APs on both sides of the link must detect each other in order for the link to be counted.
Blocked WDS Link Count	Number of WDS links blocked by the spanning tree protocol. If the AP on one side of the link reports the link as blocking then the link is counted by this status parameter.
WDS Group Password Change Status	Status of the last attempt to configure the password for the WDS group: <ul style="list-style-type: none"> • Not Started • Success • Invalid Password • Requested • Timed Out
New WDS Group Password	To change the password for all switches and APs in this WDS group, select the Edit checkbox, type the new password, and then click Apply Password .

Command Buttons

The page includes the following buttons:

- **Refresh** — Updates the page with the latest information.
- **Apply Password** — Apply the password in the **New WDS Group Password** field to members of the WDS group.

WDS Group AP Status Summary

The **WDS AP Group Status Summary** page displays summary information about the APs in a configured WDS group.

AP MAC Address	AP Connection Status	Satellite Mode	STP Root Mode	Root Path Cost	Ethernet Port STP State	Ethernet Port Mode	Ethernet Port Link State
00:12:c9:3e:36:ba	Not Connected	None	Not STP Root	0	Disabled	Disabled	Down
1c:af:f7:1f:27:80	Not Connected	Wired	Not STP Root	0	Disabled	Disabled	Up

Figure 354: WDS AP Group Status Summary

The following table describes the fields on the **WDS AP Group Status Summary** page.

Table 320: WDS AP Group Status Summary

Field	Description
Group ID	Use the drop-down menu above the fields to select the group number that identifies the configured WDS AP group.
AP MAC Address	Identifies the AP in the group by its MAC address
AP Connection Status	Indicates whether the AP is currently being managed by one of the switches in the cluster.
Satellite Mode	Indicates whether the AP is a satellite AP connected to the network via a WDS link or a root AP connected to the network via a wired link.
STP Root Mode	Indicates whether this AP is the root of the spanning tree. If spanning tree is disabled then the AP is always reported as <i>Not STP Root</i> .
Root Path Cost	Spanning Tree Path Cost to the root. The root AP always reports this value as 0. If spanning tree is disabled the value is also 0.
Ethernet Port STP State	When spanning tree is enabled on the APs in the WDS group this status parameter reports the spanning tree status of the Ethernet port, which is one of the following: <ul style="list-style-type: none"> • Disabled (STP is disabled or Link is down) • Forwarding • Learning • Listening • Blocking
Ethernet Port Mode	On satellite APs the Ethernet port can be manually disabled. On root APs the port is always enabled.
Ethernet Port Link State	When the Ethernet port is enabled, this status reports the link state of the port.

Command Buttons

The page includes the following button:

- **Refresh** — Updates the page with the latest information.

WDS AP Link Status Summary

The **WDS AP Link Status Summary** page displays summary information about the link configuration and link state in a WDS group.

WDS Group Link Status Summary									
WDS AP Group Id	Source MAC Address	Source Radio	Destination MAC Address	Destination Radio	Source End-Point Detected	Destination End-Point Detected	Aggregation Mode	Source STP State	Destination STP State
1	1c:aff7:1f:27:80	1	00:12:c9:3e:36:ba	1	No	No	No	Forwarding	Disabled
2	00:21:29:00:0a:90	2	00:1b:e9:16:37:50	2	No	No	No	Disabled	Disabled

Figure 355: WDS AP Link Status Summary

The following table describes the fields on the **WDS AP Link Status Summary** page.



Note: The WDS links are bidirectional. The terms *Source* and *Destination* simply reflect the WDS link endpoints specified in the WDS group configuration.

Table 321: WDS AP Link Status Summary

Field	Description
WDS AP Group ID	The group number that identifies the configured WDS AP group.
Source MAC Address	The MAC address of one end-point of the WDS link
Radio Source	The radio number of the WDS link endpoint on the source AP.
Destination MAC Address	The MAC address of the Source AP in the group.
Destination Radio	The radio number of the WDS link endpoint on the destination AP.
Source End-Point Detected	Indicates whether the AP specified by the destination MAC detected the AP specified by the source MAC.
Destination End-Point Detected	Indicates whether the AP specified by the source MAC detected the AP specified by the destination MAC.
Aggregation Mode	When parallel links are defined between two APs, this field indicates whether this link is part of the aggregation link pair.

Table 321: WDS AP Link Status Summary

Field	Description
Source STP State	Spanning Tree State of the link on the source AP, which is one of the following: <ul style="list-style-type: none">• Disabled (STP is disabled or Link is down)• Forwarding• Learning• Listening• Blocking
Destination STP State	Spanning Tree State of the link on the destination AP, which is one of the following: <ul style="list-style-type: none">• Disabled (STP is disabled or Link is down)• Forwarding• Learning• Listening• Blocking

Command Buttons

The page includes the following button:

- **Refresh** — Updates the page with the latest information.

WDS Group Link Statistics Summary

The **WDS Group Link Statistics Summary** page displays summary information about the packets sent and received on the WDS links.

WDS Group Link Statistics Summary													
WDS AP Group Id	Source MAC Address	Source Radio	Destination MAC Address	Destination Radio	Source AP Packets Sent	Source AP Bytes Sent	Source AP Packets Received	Source AP Bytes Received	Destination AP Packets Sent	Destination AP Bytes Sent	Destination AP Packets Received	Destination AP Bytes Received	
1	1c:af:f7:1f:27:80	1	00:12:c9:3e:36:ba	1	0	0	0	0	0	0	0	0	
2	00:21:29:00:0a:90	2	00:1b:e9:16:37:50	2	0	0	0	0	0	0	0	0	

Figure 356: WDS Group Link Statistics Summary

The following table describes the fields on the **WDS AP Link Status Summary** page.



Note: The WDS links are bidirectional. The terms *Source* and *Destination* simply reflect the WDS link endpoints specified in the WDS group configuration.

Table 322: WDS Group Link Statistics Summary

Field	Description
WDS AP Group ID	The group number that identifies the configured WDS AP group.
Source MAC Address	The MAC address of one end-point of the WDS link
Radio Source	The radio number of the WDS link endpoint on the source AP.
Destination MAC Address	The MAC address of the Source AP in the group.
Destination Radio	The radio number of the WDS link endpoint on the destination AP.
Source AP Packets Sent	Number of packets sent by the source AP.
Source AP Bytes Sent	Number of bytes sent by the source AP.
Source AP Packets Received	Number of packets received by the source AP.
Source AP Bytes Received	Number of bytes received by the source AP.
Destination AP Packets Sent	Number of packets sent by the destination AP.
Destination AP Bytes Sent	Number of bytes sent by the destination AP.
Destination AP Packets Received	Number of packets received by the destination AP.
Destination AP Bytes Received	Number of bytes received by the destination AP.

Command Buttons

The page includes the following button:

- **Refresh** — Updates the page with the latest information.

Basic Setup

The **WLAN > Administration > Basic Setup** page contains several tabs that allow you to access Web pages to configure global wireless settings for the DWS-4000 Series switch, device discovery settings, and default AP profile settings. The **Basic Setup** page also provides a tab for access to pages to configure information in the Valid AP Database on the switch. If AP MAC address validation is performed locally on the switch, and not by a RADIUS server, the MAC address of the AP must be added to the Valid AP database to allow the switch to manage the AP.

Wireless Global Configuration

In order for the DWS-4000 Series switch to be able to discover and manage access points, the WLAN admin mode on the switch must be enabled, and the WLAN Switch Operational Status must report that it is enabled. However, before you enable the WLAN Switch field, set the correct country code for the switch so that the access points can operate only in the modes permitted in your country. The default country code is US for operation in the United States. To set the country code, enable the switch by using the Web interface, and configure other global wireless settings on the switch, click **WLAN > Basic Setup**.

Wireless Global Configuration	
Enable WLAN Switch	<input checked="" type="checkbox"/>
Auto IP Assign Mode	<input checked="" type="checkbox"/>
WLAN Switch Operational Status	Enabled
IP Address	10.27.32.164
Switch Static IP Address	0.0.0.0
AP Validation	
AP MAC Validation	<input checked="" type="radio"/> Local <input type="radio"/> RADIUS
Require Authentication Passphrase	<input type="checkbox"/>
RADIUS Server Configuration	
RADIUS Authentication Server Name	Default-RADIUS-Server
RADIUS Authentication Server Status	Not Configured
RADIUS Accounting Server Name	Default-RADIUS-Server
RADIUS Accounting Server Status	Not Configured
RADIUS Accounting	<input type="checkbox"/>
Country Code	US - United States
Network Mutual Authentication Status	Not Started
Regenerate X.509 Certificate Status	Not In Progress
Manage AP with Previous Release Code	<input type="checkbox"/>

Figure 357: Wireless Global Configuration

The following table describes the fields available on the Wireless Global Configuration page.

Table 323: Basic Wireless Global Configuration

Field	Description
Enable WLAN Switch	<p>Select this option to enable WLAN switching functionality on the system. Clear the option to administratively disable the WLAN switch.</p> <p>If you clear the option, all peer switches and APs that are associated with this switch are disassociated.</p> <p>Disabling the WLAN switch does not affect non-WLAN features on the switch, such as VLAN or STP functionality.</p>
Auto IP Assign Mode	<p>Select this option to allow the wireless feature to automatically assign itself an IP address from one of the active interfaces. If this option is cleared, you must manually assign the IP address in the Switch Static IP Address field.</p>
WLAN Switch Operational Status	<p>Shows the operational status of the switch. The status can be one of the following values:</p> <ul style="list-style-type: none"> • Enabled • Enable-Pending • Disabled • Disable-Pending <p>If the status is pending, click Refresh to update the screen with the latest information.</p>
WLAN Switch Disable Reason	<p>If the status is disabled, this field appears and one of the following reasons is listed:</p> <ul style="list-style-type: none"> • None: The cause for the disabled status is unknown. • Administrator disabled: The Enable WLAN Switch check box has been cleared. • No IP Address: The WLAN interface does not have an IP address. • No SSL Files: The DWS-4000 Series switch communicates with the APs it manages by using Secure Sockets Layer (SSL) connections. The first time you power on the DWS-4000 Series switch, it automatically generates a server certificate that will be used to set up the SSL connections. The SSL certificate and key generation typically completes within a few minutes. <p>If routing is enabled on the switch, the operational status might be disabled due to one of the following reasons:</p> <ul style="list-style-type: none"> • No Loopback Interface: The switch does not have a loopback interface. • Global Routing Disabled: Even if the routing mode is enabled on the WLAN switch interface, it must also be enabled globally for the operational status to be enabled.

Table 323: Basic Wireless Global Configuration (Cont.)

Field	Description
IP Address	<p>This field shows the IP address of the WLAN interface on the switch. If the switch does not have the Routing Package installed, or if routing is disabled, the IP address is the network interface. If the routing package is installed and enabled, this is the IP address of the routing or loopback interface you configure for the DWS-4000 Series switch features.</p> <p>If routing is enabled, it is strongly recommend that you define a loopback interface on the switch. By creating a loopback interface, you can control which routing interface the wireless function uses for its IP address when multiple routing interfaces exist. This can avoid discovery problems for the discovery modes where the AP knows the IP address of the UWS. With the loopback interface, the IP address of the wireless function is always the same.</p> <p>In this context, the loopback interface does not refer to the loopback interface with the 127.0.0.1 IP address. When you configure a loopback interface for the wireless interface on the switch, it is essentially a permanent logical interface and cannot have an IP address of 127.0.0.1. You must create a dedicated subnet for the loopback interface, and other devices on the network must be able to contact the IP address of the loopback interface.</p>
Switch Static IP Address	<p>If you do not use the an automatically assigned address, enter a static IPv4 address for the wireless feature. If Auto IP Assign Mode is enabled, then this setting is ignored.</p>
AP Validation	
AP Validation Method	<p>For a DWS-4000 Series switch to manage an AP, you must add the MAC address of the AP to the Valid AP database, which can be kept locally on the switch or in an external RADIUS server. When the switch discovers an AP that is not managed by another DWS-4000 Series switch, it looks up the MAC address of the AP in the Valid AP database. If it finds the MAC address in the database, the switch validates the AP and assumes management.</p> <p>Select the database to use for AP validation and, optionally, for authentication if the Require Authentication Passphrase option is selected.</p> <ul style="list-style-type: none"> • Local: If you select this option, you must add the MAC address of each AP to the local Valid AP database. • RADIUS: If you select this option, you must configure the MAC address of each AP in an external RADIUS server.
Require Authentication Passphrase	<p>Select this option to require APs to be authenticated before they can associate with the switch.</p> <p>If you select this option, you must configure the passphrase on the AP while it is in standalone mode as well as in the Valid AP database. To configure the pass phrase on a standalone AP, log onto the AP Administration Web UI and go to the Managed Access Point page, or log onto the AP CLI and use the <code>set managed-ap pass-phrase</code> command.</p> <p>To configure the passphrase for an AP in the local Valid AP database, click the Valid AP tab from the Basic Setup page. Then, click the MAC address of the AP and enter the passphrase in the Authentication Password field.</p> <p>If you enable authentication, it takes place immediately after the switch validates the AP.</p>

Table 323: Basic Wireless Global Configuration (Cont.)

Field	Description
RADIUS Server Configuration	
RADIUS Authentication Server Name	Enter the name of the RADIUS server used for AP and client authentications when a network-level RADIUS server is not defined on the WAN > Basic Setup > SSID > Wireless Network Configuration page. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted. The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the APs and wireless clients.
RADIUS Authentication Server Status	Indicates whether the RADIUS authentication server is configured. To configure RADIUS server information, go to LAN > Security > RADIUS > RADIUS Configuration .
RADIUS Accounting Server Name	Enter the name of the RADIUS server used for reporting wireless client associations and disassociations when a network-level RADIUS accounting server is not defined on the WAN > Basic Setup > VAP > Wireless Network Configuration page. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.
RADIUS Accounting Server Status	Indicates whether the RADIUS accounting server is configured. To configure RADIUS accounting server information, go to LAN > Security > RADIUS > Accounting Server Configuration .
RADIUS Accounting	Select this option to enable RADIUS accounting for wireless clients.
Country Code	Select the country code that represents the country where your switch and APs operate. When you click Submit , a pop-up message asks you to confirm the change. Wireless regulations vary from country to country. Make sure you select the correct country code so that your WLAN system complies with the regulations in your country. Note: Changing the country code disables and re-enables the switch. Any channel and radio mode settings that are invalid for the regulatory domain are reset to the default values. The country code (IEEE 802.11d) is transmitted in beacons and probe responses from the access points.
Network Mutual Authentication Status	The mutual authentication feature allows authentication between switches and APs and between peer switches. Mutual authentication is accomplished by using X.509 certificate exchange. This field shows the status of the mutual authentication feature. The field has one of the following values: <ul style="list-style-type: none"> • Not Started • In Progress—Mutual authentication is in the process of being enabled or disabled. • Complete Without Errors—The mutual authentication process finished without any problems. • Complete With Errors —Mutual authentication finished, but problems were detected. This means that you may need to provision some switches or APs separately.

Table 323: Basic Wireless Global Configuration (Cont.)

Field	Description
Regenerate X.509 Certificate Status	<p>Status of the request to generate an X.509 certificate. To initiate X.509 certificate generation, go to the Advanced Configuration > Switch Provisioning page.</p> <p>The field has one of the following values:</p> <ul style="list-style-type: none"> • Certificate Generation is not in progress • Start Certificate Generation • Certificate Generation is in progress.
Manage AP with Previous Release Code	<p>For networks that include DWL-8600APs running a software version earlier than v2.0, you must select this option to allow the switch to discover the APs and upgrade the AP software to the current release.</p> <p>Note: After the APs have been discovered, upgraded, and become managed by the switch, clear this option.</p>

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click Tool > Save Changes.
- **Next**—Navigates to the next page in the Basic Setup configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click Tool > Save Changes.

Wireless Discovery Configuration

The DWS-4000 Series switch can discover, validate, authenticate, or monitor the following system devices:

- Peer wireless switches
- APs
- Wireless clients
- Rogue APs
- Rogue wireless clients

The DWS-4000 Series switch can discover peer wireless switches and APs regardless of whether these devices are connected to each other, located in the same Layer 2 broadcast domain, or attached to different IP subnets.

You can enable discovery between the switch and peer switches or APs by using one of following four mechanisms:

1. Manually add the IP address of the switch to the AP when it is in Standalone mode.
2. Configure a DHCP server to include the switch IP address in the DHCP response to the AP DHCP client request.
3. Use VLANs to broadcast the L2 Wireless Device Discovery Protocol.
4. Manually add the IP address of the AP to the switch.



Note: With this method, multiple peer switches might find the same access point. The first association always takes precedence. The AP does not change its association unless the connectivity to the current wireless switch fails or the switch tells the AP to disassociate and associate with another switch.

The **Discovery** tab is available from the **WLAN > Basic Setup** page and allows you to configure the switch to discover APs and other switches by using methods 3 and 4.

Global Discovery Profile Radio SSID Valid AP OUI

Wireless Discovery Configuration

L3/IP Discovery

IP List <empty list>

IP Address Range From To

Add Delete

L2/VLAN Discovery

VLAN List 1 - Default

VLAN (1-4094)

Add Delete

Note: The discovered access points will fail to get managed by this wireless switch if their MAC addresses are not added to the Local or RADIUS AP Database. To add them to the local AP database, either navigate to the **Monitoring->Access Points ->All Access Points** page or to the **Valid AP** tab on this page. Before doing that make sure you complete the default profile configuration in the next 3 tabs. That profile will be sent to the AP.

Refresh Submit Next

Figure 358: Wireless Discovery Configuration

In order for the DWS-4000 Series switch to discover other WLAN devices and establish communication with them, the devices must have their own IP address, must be able to find other WLAN devices, and must be compatible.

When the DWS-4000 Series switch discovers and validates APs, the switch takes over the management of the AP. If you configure the AP in Standalone mode, the existing AP configuration is replaced by the default AP Profile configuration on the switch.

L3/IP Discovery

You can configure up to 256 IP addresses in the DWS-4000 Series switch for potential peer switches and APs. The switch sends association invitations to all IP addresses in this list. If the device accepts the invitation and is successfully validated by the switch, the switch and the AP or peer switch are associated.

This discovery method mechanism is useful for peer switch discovery and AP discovery when the devices are in different IP subnets. In fact, for a switch to recognize a peer that is not on the same subnet, you must configure the IP addresses of each switch in the peer's L3 discovery list.



Note: The list of IP addresses is separate and independent from the list of valid managed APs. Devices discovered through this list might not be valid APs or switches.



Note: If an AP has already been discovered through another method, the DWS-4000 Series switch will not poll the IP address of the AP.

Table 324: L3 VLAN Discovery

Field	Description
L3/IP Discovery	Select or clear this option to enable or disable IP-based discovery of access points and peer wireless switches. When the L3/IP Discovery option is selected, IP polling is enabled and the switch will periodically poll each address in the configured IP List. By default, L3/IP Discovery is enabled.
IP List	Shows the list of IP addresses configured for discovery. To remove entries from the list, select one or more entries and click Delete . There are no default entries, and the maximum number of entries supported is 256.
IP Address Range	This text field is used to add a range of IP address entries to the IP List. Enter the IP address at the start of the address range in the From field, and enter the IP address at the end of the range in the To field, then click Add . All IP addresses in the range are added to the IP List. Only the last octet is allowed to differ between the From address and the To address. Note: To add a single IP address, enter the address in the From field and leave the To field blank, then click Add . Once all desired entries are added, click Submit to save the list in the running configuration.

To view the IP discovery status of the devices you add to the IP List, such as whether the switch successfully polled the IP address you entered, navigate to the **WLAN > Monitoring > Global > IP Discovery tab**.

L2/VLAN Discovery

The D-Link Wireless Device Discovery Protocol is a good discovery method to use if the DWS-4000 Series switch and APs are located in the same Layer 2 multicast domain. The DWS-4000 Series switch periodically sends a multicast packet containing the discovery message on each VLAN enabled for discovery. You can enable the discovery protocol on up to 16 VLANs.

By default, VLAN 1 is enabled on the AP, and VLAN 1 is enabled for discovery on the DWS-4000 Series switch. If the switch and AP are in the same Layer 2 multicast domain, you might not need to take any action to enable AP-to-DWS-4000 Series switch discovery. The DWS-4000 Series switch also uses L2/VLAN discovery to find peer switches within the L2 multicast domain.

The APs process the discovery message only when it comes in on the management VLAN. The APs do not forward the L2 discovery messages onto the wireless media.

From the DWS-4000 Series switch, you can check the discovery status of APs and peer switches. To view information about whether the switch discovered any APs, navigate to the **WLAN > Monitoring > Access Point > Managed AP Status** page. If you have not added the MAC address of the AP to the local or RADIUS Valid AP database, the AP appears in the **WLAN > Monitoring > Access Points > AP Authentication Failure Status** list, and the failure type is listed as No Database Entry.

To view information about whether the switch discovered any peer switches, navigate to the **WLAN > Monitoring > Peer Switch page**.

Command Buttons

The page includes the following buttons:

- **Add**—Adds the data in the IP Address or VLAN field to the appropriate list.
- **Delete**—Deletes the selected entry from the IP or VLAN list.
- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click Tool > Save Changes.
- **Next**—Navigates to the next page in the Basic Setup configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click Tool > Save Changes.

Profile

The switch can support APs that have different hardware capabilities, such as the supported number of radios and the supported IEEE 802.11 modes. APs that use the same profile should have the same hardware capabilities so that the settings you configure in the profile are valid for all APs within the profile.

Figure 359: AP Hardware Capabilities

Table 325 describes the fields available on the Profile page.

Table 325: Profile

Field	Description
Hardware Type ID	Select the hardware type for the APs that use this profile. The hardware type is determined, in part, by the number of radios the AP supports (single or dual) and the IEEE 802.11 modes that the radio supports (a/b/g or a/b/g/n). The options available in the Hardware Type ID are: <ul style="list-style-type: none"> • Any (can support all models in the DWL-X600AP family) • DWL-8600AP Dual Radio a/b/g/n • DWL-3600AP Single Radio b/g/n • DWL-6600AP Dual Radio a/b/g/n
Wired Network Discovery VLAN ID	Enter the VLAN ID that the switch uses to send tracer packets in order to detect APs connected to the wired network. The tracer packets help the switch identify unauthorized APs that do not belong to the Unified Wired and Wireless Access System but are connected to the wired network.

To add a new profile, go to the **WLAN > Administration > Advanced Configuration > AP Profile** page, enter a name for the new profile in the available field, and click **Add**.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click Tool > Save Changes.
- **Next**—Navigates to the next page in the Basic Setup configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click Tool > Save Changes.

Radio Configuration

In order to accommodate a broad range of wireless clients and wireless network requirements, the DWL-8600AP and DWL-6600AP support two radios. Radio 1 can broadcast in one of the following modes:

- IEEE 802.11a mode
- IEEE 802.11a and IEEE 802.11n modes
- 5 GHz IEEE 802.11n mode

Radio 2 can broadcast in one of the following modes:

- IEEE 802.11b and IEEE 802.11g modes
- IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n modes
- 2.4 GHz IEEE 802.11n mode

The DWL-3600AP supports one radio that can broadcast in one of the following modes:

- IEEE 802.11b and IEEE 802.11g modes
- IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n modes
- 2.4 GHz IEEE 802.11n mode



The DWL-3600AP is a single-radio AP. Any settings you configure for Radio 1 (802.11a/n) are not applied to the DWL-3600AP.

You configure the default radio settings from the **WLAN > Basic Setup > Radio** tab, which the following figure shows.

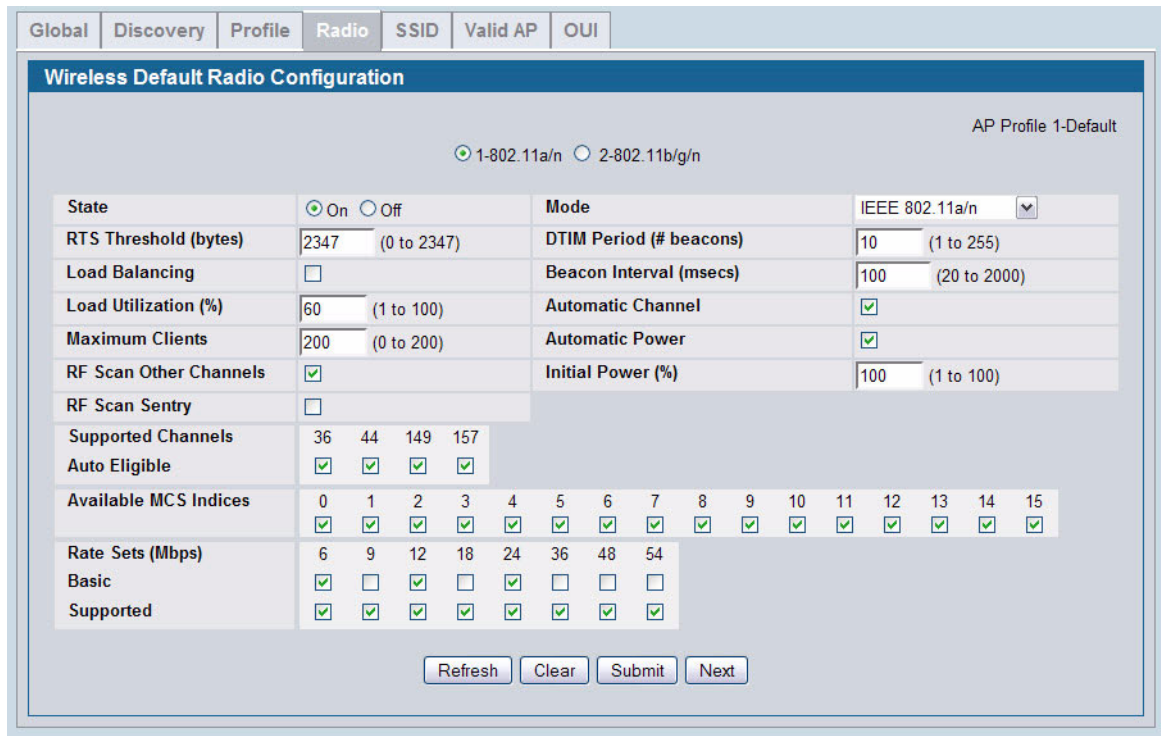


Figure 360: Radio Settings

The following table describes the fields you can configure from the **Radio** tab on the **Basic Setup** page. To change the settings on this page, you must first select the radio you want to configure (1 or 2). After you change the settings, click **Submit** to apply the settings. Changes to the settings apply only to the selected radio.

Table 326: Radio Settings

Field	Description
1-802.11a/n 2-802.11b/g/n	From this field, you can select the radio that you want to configure. By default, Radio 1 operates in IEEE 802.11a/n mode, and Radio 2 operates in IEEE 802.11b/g/n mode. If you change the mode, the labels for the radios change accordingly. Changes to the settings apply only to the selected radio. The DWL-3600AP is a single-radio AP. Any settings you configure for Radio 1 (802.11a/n) are not applied to the DWL-3600AP. If the selected Hardware Type ID for the AP profile is DWL-3600AP, the radio selectors are not available.
State	Specify whether you want the radio on or off by clicking On or Off . If you turn off a radio, the AP sends disassociation frames to all the wireless clients it is currently supporting so that the radio can be gracefully shutdown and the clients can start the association process with other available APs.

Table 326: Radio Settings (Cont.)

Field	Description
Mode	<p>The Mode defines the Physical Layer (PHY) standard the radio uses. Select one of the following modes for each radio interface.</p> <p>Radio 1 supports:</p> <ul style="list-style-type: none"> • IEEE 802.11a is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps. • IEEE 802.11a/n operates in the 5 GHz ISM band and includes support for both 802.11a and 802.11n devices. IEEE 802.11n is an extension of the 802.11 standard that includes multiple-input multiple-output (MIMO) technology. IEEE 802.11n supports data ranges of up to 248 Mbps and nearly twice the indoor range of 802.11 b, 802.11g, and 802.11a. • 5 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 5 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a). <p>Radio 2 supports:</p> <ul style="list-style-type: none"> • IEEE 802.11b/g operates in the 2.4 GHz ISM band. IEEE 802.11b is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps. IEEE 802.11g is a higher speed extension (up to 54 Mbps) to the 802.11b PHY. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps. • IEEE 802.11b/g/n operates in the 2.4 GHz ISM band and includes support for 802.11b, 802.11g, and 802.11n devices. • 2.4 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 2.4 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a).
RTS Threshold	<p>Specify a Request to Send (RTS) Threshold value between 0 and 2347.</p> <p>The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.</p> <p>Changing the RTS threshold can help control traffic flow through the AP, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.</p>

Table 326: Radio Settings (Cont.)

Field	Description
DTIM Period	<p>The Delivery Traffic Information Map (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up.</p> <p>The DTIM period you specify indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup.</p> <p>Specify a DTIM period within the given range (1–255).</p> <p>The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the AP at every beacon. If you set this field to 10, clients will check on every 10th beacon.</p>
Beacon Period	<p>Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).</p> <p>The Beacon Interval value is set in milliseconds. Enter a value from 20 to 2000.</p>
Load Balancing	<p>If you enable load balancing, you can control the amount of traffic that is allowed on the AP.</p>
Load Utilization	<p>This field allows you to set a threshold for the percentage of network bandwidth utilization allowed on the radio. Once the level you specify is reached, the AP stops accepting new client associations. Enter a percentage of utilization from 1 to 100.</p>
Maximum Clients	<p>Specify the maximum number of stations allowed to associate with this access point at any one time.</p> <p>You can enter a value between 0 and 200.</p>
Automatic Channel	<p>The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface.</p> <p>When the AP boots, each AP radio scans the RF area for occupied channels and selects a channel from the available non-interfering or clear channels. However, channel conditions can change during operation.</p> <p>Enabling the Automatic Channel makes the radio of APs assigned to this profile eligible for auto-channel selection. You can automatically or manually run the auto-channel selection algorithm to allow the DWS-4000 Series switch to adjust the channel on APs as WLAN conditions change.</p> <p>By default, the global auto-channel mode is set to manual. To enable the automatic channel selection mode, go to the WLAN > Administration > AP Management > RF Management page and select Fixed or Interval for the Channel Plan mode. You can also run the automatic channel selection algorithm manually from the Manual Channel Plan page.</p> <p>Note: If you assign a static channel to a radio of an AP in the Valid AP database or on the Advanced AP Management page, the AP radio will not participate in the auto-channel selection.</p>
Automatic Power	<p>The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range.</p> <p>Automatic power uses a proprietary algorithm to automatically adjust the RF signal to broadcast far enough to reach wireless clients, but not so far that it interferes with RF signals broadcast by other APs. The power level algorithm increases or decreases the power level in 10% increments based on presence or absence of packet retransmission errors.</p>

Table 326: Radio Settings (Cont.)

Field	Description
Initial Power	The automatic power algorithm will not reduce the power below the number you set in the initial power field. By default, the power level is 100%. Therefore, even if you enable the automatic power, the power of the RF signal will not decrease. The power level is a percentage of the maximum transmission power for the RF signal.
RF Scan Other Channels	The access point can perform RF scans to collect information about other wireless devices within range and then report this information to the DWS-4000 Series switch. If you select the Scan Other Channels option, the radio periodically moves away from the operational channel to scan other channels. Enabling this mode causes the radio to interrupt user traffic, which may be noticeable with voice connections. When the Scan Other Channels option is cleared, the AP scans only the operating channel.
RF Scan Sentry	Select this option to allow the radio to operate in sentry mode. When the RF Scan Sentry option is selected, the radio primarily performs dedicated RF scanning. The radio passively listens for beacons and traffic exchange between clients and other access points but does not accept connections from wireless clients. In sentry mode, all VAPs are disabled. Networks that deploy sentry APs or radios can detect devices on the network quicker and perform more thorough security analysis. In this mode, the radio switches from one channel to the next. The length of time spent on each channel is controlled by the scan duration. The default scan duration is 10 milliseconds.
Supported Channels	This field displays the channels that are supported for the radio mode currently selected on the page and for the country configured on the Global Wireless Settings page.
Auto Eligible	Select the Auto Eligible option beneath each channel to include the channel in the automatic channel assignment process.
Rate Sets	Select the transmission rate sets you want the access point to support and the basic rate sets you want the access point to advertise. Rates are expressed in megabits per second.
Basic	These numbers indicate the data rates that all stations associating with the AP must support.
Supported	These numbers indicate rates that the access point supports. You can select multiple rates. The AP automatically chooses the most efficient rate based on factors like error rates and distance of client stations from the AP.



Note: If you access the Access Point Profile Radio configuration through the **Radio** tab for a profile from the **WLAN > Administration > Advanced Configuration > AP Profile** page, additional fields are available for configuration.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.

- **Clear**—Resets the settings on the page to the default values.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP).
- **Next**—Navigates to the next page in the Basic Setup configuration. Any changes you made to the current page are saved to the running configuration (but not startup configuration) before the next page is displayed.

Wireless Default VAP Configuration

The **SSID** tab displays the virtual access point (VAP) settings associated with the default AP profile. Each VAP has an associated network, which is identified by its network number and Service Set Identifier (SSID). You can configure and enable up to 16 VAPs per radio on each physical access point.

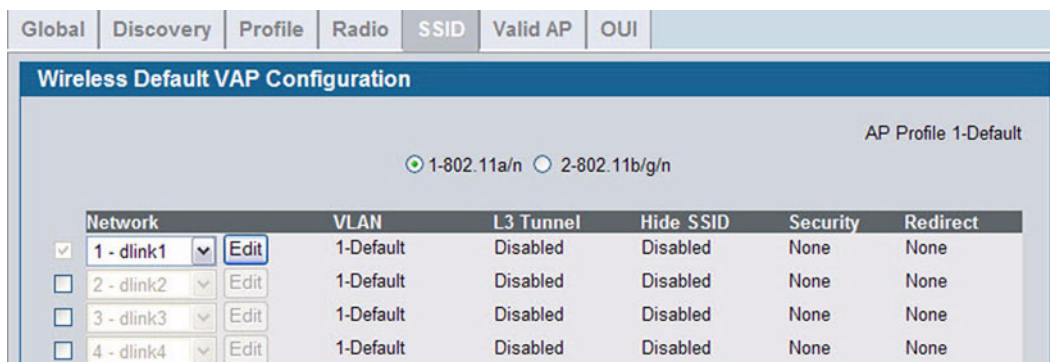


Figure 361: VAP Settings

VAPs segment the wireless LAN into multiple broadcast domains that are the wireless equivalent of Ethernet VLANs. To a wireless client, each VAP appears to be a single physical access point. However, since the VAPs use the same channel, there is no risk of RF interference among the networks that are on a single AP.

VAPs can help you maintain better control over broadcast and multicast traffic, which affects network performance. You can also configure different security mechanisms for each VAP.

A VAP is a physical entity. Each VAP maps directly to a MAC address. A network is a logical entity that you apply to a VAP. Networks are identified by a network number and an associated SSID. The SSID does not need to be unique for each network. You can create and modify a network in one place and apply the network to one or more VAP as needed. This allows you to mix networks within different profiles without having to reconfigure everything. When you edit a network configuration that is applied to more than one VAP, you edit it for every VAP that uses the network.

Managing the Virtual Access Point Configuration

The Default AP profile has one VAP on each radio enabled by default. The default VAP uses the dlink1 SSID, and there is no security to prevent wireless clients from associating with the VAP. To enable additional VAPs, select the check box next to the VAP. Once you enable a VAP, you can select the network (SSID) to use from the drop-down menu. To change Network settings, click **Edit**.

The following table describes the fields on the **SSID** page.

Table 327: Default VAP Configuration

Field	Description
Radio 1 Radio 2	You configure the VAPs for Radio 1 and Radio 2 separately. Select the radio to configure the settings for before you enable the VAP. The DWL-3600AP is a single-radio AP. Any settings you configure for Radio 1 (802.11a/n) are not applied to the DWL-3600AP. If the selected Hardware Type ID for the AP profile is DWL-3600AP, the radio selectors are not available.
Network	Use the option to the left of the network to enable or disable the corresponding VAP on the selected radio. When enabled, use the menu to select a networks to assign to the VAP. You can configure up to 64 separate networks on the switch and apply them across multiple radio and VAP interfaces. By default, 16 networks are pre-configured and applied in order to the VAPs on each radio. Enabling a VAP on one radio does not automatically enable it on the other radio. Note: You cannot disable the default VAP, VAP0. To configure additional networks, click WLAN > Administration > Advanced Configuration > Networks .
Edit	Click Edit to modify settings for the corresponding network. When you click Edit , the Wireless Network Configuration page appears.
VLAN	Shows the VLAN ID of the VAP. To change this setting, click Edit .
L3 Tunnel	Shows whether L3 Tunneling is enabled on the VAP. To change this setting, click Edit . Note: When L3 tunneling is enabled, the VLAN ID is not used. In fact, the switch puts the management VLAN ID, if any, on the tunneled packets.
Hide SSID	Shows whether the VAP broadcasts the SSID. If enabled, the SSID for this network is not included in AP beacons. To change this setting, click Edit .
Security	Shows the current security settings for the VAP. To change this setting, click Edit .
Redirect	Shows whether HTTP redirect is enabled. The possible values for the field are as follows: <ul style="list-style-type: none"> • HTTP: HTTP Redirect is enabled • None: HTTP Redirect is disabled

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click **Tool > Save Changes**.
- **Next**—Navigates to the next page in the Basic Setup configuration. Any changes you made to the current page are saved before the next page is displayed. To retain the new values across a power cycle, you must perform a save on the WLAN switch (not the AP). To perform a save, click **Tool > Save Changes**.

Configuring the Default Network

Each network is identified by its Service Set Identifier (SSID), which is an alphanumeric key that identifies a wireless local area network. You can configure up to 64 different networks on the DWS-4000 Series switch. Each network can have a unique SSID, or you can configure multiple networks with the same SSID.

When you click **Edit** on the VAP page, the Wireless Network Configuration page appears, as the following figure shows.

Wireless Network Configuration	
SSID	DLINK TEST 12
Hide SSID	<input type="checkbox"/>
Ignore Broadcast	<input type="checkbox"/>
VLAN	1 (1 to 4094)
L3 Tunnel	<input type="checkbox"/>
L3 Tunnel Status	None
L3 Tunnel Subnet	0.0.0.0
L3 Tunnel Mask	255.255.255.0
MAC Authentication	<input type="radio"/> Local <input type="radio"/> RADIUS <input checked="" type="radio"/> Disable
Redirect	<input checked="" type="radio"/> None <input type="radio"/> HTTP
Redirect URL	
Wireless ARP Suppression Mode	Disable
L2 Distributed Tunneling Mode	Disable
RADIUS Authentication Server Name	
	Default-RADIUS-Server
RADIUS Authentication Server Status	
	Configured
RADIUS Accounting Server Name	
	Default-RADIUS-Server
RADIUS Accounting Server Status	
	Configured
RADIUS Use Network Configuration	
	Enable
RADIUS Accounting	
	<input type="checkbox"/>
Security	
	<input type="radio"/> None <input type="radio"/> WEP <input checked="" type="radio"/> WPA/WPA2
	<input checked="" type="radio"/> WPA Personal <input type="radio"/> WPA Enterprise
WPA Versions	
	<input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2
WPA Ciphers	
	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> CCMP(AES)
WPA Key Type	
	ASCII
WPA Key	
	hshitest
Bcast Key Refresh Rate	
	300 (0 to 86400)
Client QoS	
	<input type="checkbox"/>
Client QoS Bandwidth Limit Down (bits-per-second)	
	0 (0 to 4294967295, 0 - Disable)
Client QoS Bandwidth Limit Up (bits-per-second)	
	0 (0 to 4294967295, 0 - Disable)
Client QoS Access Control Down	
	<none>
Client QoS Access Control Up	
	<none>
Client QoS Diffserv Policy Down	
	<none>
Client QoS Diffserv Policy Up	
	<none>
<input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="Clear"/>	

Figure 362: Configuring Network Settings

Table 328 describes the fields on the Wireless Network Configuration page. After you change the wireless network settings, click **Submit** to save the changes.

Table 328: Wireless Network Configuration

Field	Description
SSID	Wireless clients identify a wireless network by the SSID, which is an alphanumeric key that uniquely identifies a wireless local area network. The SSID can be up to thirty-two characters in length, and there are no restrictions on the characters that may be used in an SSID.
Hide SSID	<p>You can hide the SSID broadcast to discourage stations from automatically discovering your access point. When the broadcast SSID of the AP is hidden, the network name is not displayed in the list of available networks on a client station. Instead, the client must have the exact network name configured in the supplicant before it is able to connect.</p> <p>Disabling the broadcast SSID is sufficient to prevent clients from accidentally connecting to your network, but it will not prevent even the simplest of attempts by a hacker to connect, or monitor unencrypted traffic.</p> <p>Hiding the SSID offers a very minimal level of protection on an otherwise exposed network (such as a guest network) where the priority is making it easy for clients to get a connection and where no sensitive information is available.</p>
Ignore Broadcast	<p>If a wireless client broadcasts probe requests to all available SSIDs, this option controls whether the AP will respond to the probe request.</p> <ul style="list-style-type: none"> • Select this option to prohibit the AP from responding to client probe requests • Clear this option to allow the AP to respond to client probe requests.
VLAN	<p>A virtual LAN (VLAN) is a software-based, logical grouping of devices on a network that allow them to act as if they are connected to a single physical network, even though they may not be. The nodes in a VLAN share resources and bandwidth and are isolated on that network.</p> <p>The D-Link Unified Switch supports the configuration of a wireless VLAN. You can configure each VAP to be on a unique VLAN or on the same VLAN as other VAPs.</p> <p>When a wireless client connects to the AP by using this network (SSID), the AP tags the client's traffic with the VLAN ID you configure in this field. By default, all networks use VLAN 1, which is also untagged by default.</p> <p>Note: The VLAN ID you configure in this field can be overridden by the VLAN ID configured for the AP in the RADIUS server. In other words, if your network uses a RADIUS server to assign wireless clients to VLANs, the wireless client uses the VLAN ID from the RADIUS server and ignores the VLAN ID configured on the VAP.</p>
L3 Tunnel	<p>The L3 Tunnel feature allows mobile stations to maintain their IP connections while roaming from one access point to another access point even when these access points are attached to different IP subnets.</p> <p>Note: When L3 tunneling is enabled the VLAN ID is not used. In fact, the switch puts the management VLAN ID, if any, on the tunneled packets.</p> <p>Note: If the wireless network topology changes (for example, a DWS-4000 Series switch reboots) while the L3 tunneling feature is in use, you should perform an ARP refresh on wired clients to speed up the process of re-establishing connectivity to the tunneled network.</p>

Table 328: Wireless Network Configuration (Cont.)

Field	Description
L3 Tunnel Status	<p>This field shows the status of L3 Tunneling. In order for tunnel to be completely configured, routing must be enabled and the switch must have a routing interface IP address that is in the tunnel subnet. The the status can be one of the following:</p> <ul style="list-style-type: none"> • None (L3 Tunnel is disabled or the network is not associated with any AP profiles) • Configured • Not Configured - Routing Disabled • Not Configured - No Routing Interface
L3 Tunnel Subnet	The network IP address you enter in this field must be in the same subnet as a routing interface for the WLAN that you define on the switch.
L3 Tunnel Mask	Enter the subnet mask for the network IP address on the L3 Tunnel subnet.
MAC Authentication	<p>If you enable MAC authentication, wireless clients must be authenticated by the AP in order to connect to the network. To use MAC authentication, configure the client MAC addresses in one of the following databases:</p> <ul style="list-style-type: none"> • Local • RADIUS <p>In the database, you set a default action to either accept or deny that client or use the global action configured on the WLAN > Administration > Advanced Configuration > Global page.</p> <p>MAC authentication is useful in networks that operate in Open mode to grant or deny access to clients with specific MAC addresses. MAC Authentication can also be used in conjunction with 802.1X security methods, in which case the MAC Authentication is done prior to the 802.1X authentication.</p>
Redirect	<p>Select the HTTP option in the Redirect field to redirect wireless clients to a custom Web page.</p> <p>When redirect mode is enabled, the user will be redirected to the URL you specify after the wireless client associates with an AP and the user opens a Web browser on the client to access the Internet.</p> <p>The custom Web page must be located on an external Web server and might contain information such as the company logo and network usage policy.</p> <p>Note: The wireless client is redirected to the external Web server only once while it associated with the AP.</p> <p>Redirect functionality allows you to implement captive portal functionality; a captive portal is often used at Wi-Fi hotspots to provide branding for the hotspot provider and/or display a legal disclaimer, which the user can click-through to access the Internet.</p>
Redirect URL	Enter the URL where all initial HTTP accesses should be redirected to. This field is accessible only when HTTP is selected as the redirect type.
Wireless ARP Suppression Mode	<p>Enable the mode to allow the APs to reduce the number of broadcasted ARP requests on the wireless interfaces. Reducing broadcasts helps conserve power on the wireless clients. The wireless clients that use power-save mode must wake up and use more power when they detect broadcast frames.</p> <p>Note: Enabling this feature slightly degrades AP packet forwarding performance due to extra packet filtering to find DHCP packets and extra processing for ARP request and reply packets. Networks that do not use IPv4 should not enable this feature.</p>

Table 328: Wireless Network Configuration (Cont.)

Field	Description
L2 Distributed Tunneling Mode	<p>The distributed L2 tunneling mode supports L3 roaming for wireless clients without forwarding any data traffic to the DWS-4000 Series switch. Use the menu to enable or disable the mode.</p> <p>L2 tunneling is recommended when the DWS-4000 Series switch does not support hardware forwarding acceleration or hardware-based L2 tunnels.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. When there is only one switch managing all APs and that switch goes down, all APs shut down their radios and the tunnel is terminated. After the switch recovers and the AP becomes managed again, the client that was previously tunneling traffic will re-associate and obtain an IP address on the network where its currently located. This IP address will be different from the IP address it was using when it was tunneling, and the traffic will not be tunneled. 2. If the network has peer switches and the tunnel is established between the APs managed by the peer switches then, when a switch managing the home AP fails, the switch managing the association AP detects the failure and terminates the tunnel. At this point the client is disassociated. When the client re-associates it obtains a new IP address. 3. If the switch managing the association AP fails, then the scenario is the same as in item 1 above. The AP takes down all radios and the clients disassociate.
RADIUS Authentication Server Name	<p>Enter the name of the RADIUS server that the VAP uses for AP and client authentications. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.</p> <p>Any RADIUS information you configure for the wireless network overrides the global RADIUS information configured on the Wireless Global Configuration page.</p> <p>The switch acts as the RADIUS client and performs all RADIUS transactions on behalf of the APs and wireless clients.</p>
RADIUS Authentication Server Status	<p>Indicates whether the RADIUS authentication server is configured for the VAP. To configure RADIUS server information, go to the LAN > Security > RADIUS > Server Configuration page.</p>
RADIUS Accounting Server Name	<p>Enter the name of the RADIUS server that the VAP uses for reporting wireless client associations and disassociations. The name can contain up to 32 alphanumeric characters. Spaces, underscores, and dashes are also permitted.</p> <p>Any RADIUS information you configure for the wireless network overrides the global RADIUS information configured on the Wireless Global Configuration page.</p>
RADIUS Accounting Server Status	<p>Indicates whether the RADIUS accounting server is configured. To configure RADIUS accounting server information, go to LAN > Security > RADIUS > Accounting Server Configuration.</p>
RADIUS Use Network Configuration	<p>This field controls whether the VAP uses the network RADIUS settings or the global RADIUS settings.</p> <ul style="list-style-type: none"> • Enable: Use RADIUS Servers defined on the Wireless Network Configuration page. • Disable: Use RADIUS servers defined on the Wireless Global Configuration page.
RADIUS Accounting	<p>Select this option to enable RADIUS accounting for wireless clients.</p>

Table 328: Wireless Network Configuration (Cont.)

Field	Description
Security	<p>The default AP profile does not use any security mechanism by default. In order to protect your network, D-Link strongly recommends that you select a security mechanism so that unauthorized wireless clients cannot gain access to your network. The following WLAN network security options are available:</p> <ul style="list-style-type: none"> • None • WEP • WPA/WPA2 • WPA Personal • WPA Enterprise <p>If you select WEP or WPA/WPA2 as your security mechanism, a dialogue box asks if you want to change network security. After you click OK, additional fields appear, and any network settings that you modified are applied to the switch.</p> <p>“Configuring AP Security” on page 551 describes the security mechanisms and the additional fields you can configure if you select WEP or WPA/WPA2.</p>
Client QoS	<p>The Client QoS parameters allow the switch to apply access control lists (ACLs) and differentiated service (DiffServ) policies to wireless clients associated to the AP and extend the switch QoS features into the wireless domain.</p> <p>Select this option to enable Client QoS operation for wireless clients that associate with the AP using the SSID in the previous field.</p> <p>Client QoS provides control over certain QoS aspects of wireless clients that connect to the network, such as the amount of bandwidth and type of traffic an individual client is allowed to send and receive. To control general categories of traffic, such as HTTP traffic or traffic from a specific subnet, you can configure ACLs and assign them to one or more VAPs. Client QoS also allows you to configure per-client conditioning of various micro-flows through DiffServ.</p> <p>ACLs are a collection of permit and deny conditions, called rules, that provide security by blocking unauthorized users and allowing authorized users to access specific resources. ACLs can block any unwarranted attempts to reach network resources.</p> <p>Each ACL is a set of up to ten rules applied to traffic sent from a wireless client or to be received by a wireless client. Each rule specifies whether the contents of a given field should be used to permit or deny the packet from being transmitted. Rules can be based on various criteria and may apply to one or more fields within a packet, such as the source or destination IP address, the source or destination L4 port, or the protocol carried in the packet.</p> <p>DiffServ policies are a useful tool for establishing general micro-flow definition and treatment characteristics that can be applied to each wireless client, both inbound and outbound, when it is authenticated on the network. Packets are classified and processed based on defined criteria. The classification criteria is defined by a class. The processing is defined by a policy's attributes.</p>
Client QoS Bandwidth Limit Down	<p>Enter the maximum allowed transmission rate from the AP to the wireless client in bits per second. The valid range is 0-4294967295 bps.</p> <p>A non-zero configured value is rounded down to the nearest 64 Kbps value for use in the AP, but to no less than 64 Kbps. A value of 0 means that the bandwidth maximum limit is not enforced in this direction.</p>

Table 328: Wireless Network Configuration (Cont.)

Field	Description
Client QoS Bandwidth Limit Up	<p>Enter the maximum allowed client transmission rate to the AP in bits per second. The valid range is 0-4294967295 bps.</p> <p>A non-zero configured value is rounded down to the nearest 64 Kbps value for use in the AP, but to no less than 64 Kbps. A value of 0 means that the bandwidth maximum limit is not enforced in this direction.</p>
Client QoS Access Control Down	<p>Select the name of the access list applied to traffic in the outbound (down) direction. Only existing IP access lists are listed in the menu and are prefixed with the access list type. To create an IP access list, use the pages in the LAN > Access Control Lists folder.</p> <ul style="list-style-type: none"> On the IP ACL Configuration page, create a new standard, extended, or named IP ACL. On the IP ACL Rule Configuration page, create one or more rules to define the packet match criteria and the deny or permit action for each rule. <p>After switching the packet to the outbound interface, the ACL rules are checked for a match. The packet is transmitted if it is permitted, and discarded if it is denied.</p>
Client QoS Access Control Up	<p>Select the name of the access list applied to traffic in the inbound (up) direction. Only existing IP access lists are listed in the menu and are prefixed with the access list type. To create an IP access list, use the pages in the LAN > Access Control Lists folder.</p> <ul style="list-style-type: none"> On the IP ACL Configuration page, create a new standard, extended, or named IP ACL. On the IP ACL Rule Configuration page, create one or more rules to define the packet match criteria and the deny or permit action for each rule. <p>When a packet is received by the AP, the ACL rules are checked for a match. The packet is processed if it is permitted, and discarded if it is denied.</p>
Client QoS DiffServ Policy Down	<p>Select the name of the DiffServ policy applied to traffic from the AP in the outbound (down) direction. Only existing DiffServ policies are listed in the menu. To create a DiffServ policy, use the pages in the LAN > QoS > Differentiated Services folder.</p> <ul style="list-style-type: none"> On the Class Configuration page, create a class and define class criteria. On the Policy Configuration page, create a policy and then associate a class with the policy. On the Policy Class Definition page, define policy statements to define what happens to a packet when it matches the class criteria.
Client QoS DiffServ Policy Up	<p>Select the name of the DiffServ policy applied to traffic sent to the AP in the inbound (up) direction. Only existing DiffServ policies are listed in the menu. To create a DiffServ policy, use the pages in the LAN > QoS > Differentiated Services folder.</p> <ul style="list-style-type: none"> On the Class Configuration page, create a class and define class criteria. On the Policy Configuration page, create a policy and then associate a class with the policy. On the Policy Class Definition page, define policy statements to define what happens to a packet when it matches the class criteria.

Configuring AP Security

The Default AP profile does not use any security mechanism by default. To protect your network, D-Link strongly recommends that you select a security mechanism so that unauthorized wireless clients cannot gain access to your network.

From the **VAP** tab of the **Wireless Network Configuration** page, you can select **None**, **WEP** or **WPA/WPA2** as the WLAN security mechanisms, as the following figure shows. The default is **None**.

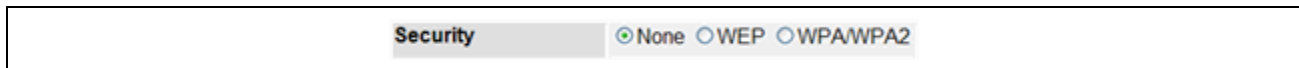


Figure 363: AP Network Security Options

The following sections describe the security mechanisms.

Using No Security

If you select **None** as your security mode, no further options are configurable on the AP. This mode means that any data transferred between the AP and the associated wireless clients is not encrypted, and any wireless client can associate with the AP.

This security mode can be useful during initial network configuration or for problem solving, but it is not recommended for regular use on the internal network because it is not secure.

Using Static or Dynamic WEP

Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. If you select this security mechanism, all wireless clients and access points on the network are configured with a 64-bit (40-bit secret key + 24-bit initialization vector (IV)) or 128-bit (104-bit secret key + 24-bit IV) Shared Key for data encryption.

Static WEP is not the most secure mode available, but it offers more protection than setting the security mode to **None** as it does prevent an outsider from easily sniffing out unencrypted wireless traffic.

Dynamic WEP is more secure than Static WEP, but you need a RADIUS server to manage the dynamically generated keys.

WEP encrypts data moving across the wireless network based on a static key. (The encryption algorithm is a stream cipher called RC4.)

If you select WEP as the Security Mode, additional fields display, as the following figure shows.

Security	<input type="radio"/> None <input checked="" type="radio"/> WEP <input type="radio"/> WPA/WPA2
	<input checked="" type="radio"/> Static WEP <input type="radio"/> WEP IEEE802.1x
Authentication	<input checked="" type="checkbox"/> Open System <input type="checkbox"/> Shared Key
WEP Key Type	<input type="radio"/> ASCII <input checked="" type="radio"/> HEX
WEP Key Length (bits)	<input type="radio"/> 64 <input checked="" type="radio"/> 128
WEP Keys	Tx (Characters required: 26)
	<input checked="" type="radio"/> 1 <input type="text"/>
	<input type="radio"/> 2 <input type="text"/>
	<input type="radio"/> 3 <input type="text"/>
	<input type="radio"/> 4 <input type="text"/>

Figure 364: Static WEP Configuration

Table 329 describes the configuration options for WEP.

Table 329: Static WEP

Field	Description
Static WEP or WEP IEEE 802.1X	<p>Static WEP uses static key management. You manually configure the same keys to encrypt data on both the wireless client and the AP. Dynamic WEP (WEP IEEE 802.1x) uses dynamically generated keys to encrypt client-to- AP traffic. Dynamic WEP is more secure than Static WEP, but you need a RADIUS server to manage the keys.</p> <p>If you select WEP IEEE 802.1X, the screen refreshes, and there are no more fields to configure. The AP uses the global RADIUS server or the RADIUS server you specify for the wireless network.</p> <p>For information about how to configure the global RADIUS server settings on the DWS-4000 Series switch, see “Wireless Global Configuration” on page 529.</p>
Authentication	<p>Choose the authentication type:</p> <ul style="list-style-type: none"> • Open System: No authentication is performed. • Shared Key: Provides a rudimentary form of user authentication, which many experts consider to be less secure than Open System since it sends the WEP key to the client in plain text. • Both: Only WEP clients are authenticated.
WEP Key Type	<p>Select the key type by clicking one of the radio buttons:</p> <ul style="list-style-type: none"> • ASCII: Includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #. • Hex: Includes digits 0 to 9 and the letters A to F.

Table 329: Static WEP (Cont.)

Field	Description
WEP Key Length	Specify the length of the key by clicking one of the radio buttons: <ul style="list-style-type: none"> • 64 bits • 128 bits
Tx	The Transfer Key Index indicates which WEP key the access point uses to encrypt the data it transmits. To select a transfer key, click the button located between the key number and the field where you enter the key. In Figure 364 , the transfer key is 3.
WEP Keys	You can specify up to four WEP keys. In each text box, enter a string of characters for each key. These are the RC4 WEP keys shared with the stations using the access point. Use the same number of characters for each key. The number of keys you enter depends on the Key Type and Key Length. The following list shows the number of keys to enter in the field: <ul style="list-style-type: none"> • 64 bit: ASCII: 5 characters; Hex: 10 characters • 128 bit: ASCII: 13 characters; Hex: 26 characters Each client station must be configured to use one of these same WEP keys in the same slot as specified here on the AP.

Static WEP Rules

If you use Static WEP, the following rules apply:

- All client stations must have the Wireless LAN (WLAN) security set to WEP and all clients must have one of the WEP keys specified on the AP in order to de-code AP-to-station data transmissions.
- The AP must have all keys used by clients for station-to-AP transmit so that it can de-code the station transmissions.
- The same key must occupy the same slot on all nodes (AP and clients). For example if the AP defines *abc12* key as WEP key 3, then the client stations must define that same string as WEP key 3.
- Client stations can use different keys to transmit data to the access point. (Or they can all use the same key, but this is less secure because it means one station can decrypt the data being sent by another.)
- On some wireless client software, you can configure multiple WEP keys and define a client station “transfer key index”, and then set the stations to encrypt the data they transmit using different keys. This ensures that neighboring APs cannot decode each other’s transmissions.
- You cannot mix 64-bit, 128-bit, and 152-bit WEP keys between the access point and its client stations.

Using WPA/WPA2 Personal or Enterprise

WPA and WPA2 are Wi-Fi Alliance IEEE 802.11i standards, which include AES-CCMP and TKIP mechanisms. The WPA/WPA2 Personal employs a pre-shared key to perform an initial check of credentials. The WPA/WPA2 Enterprise security uses a RADIUS server to authenticate users.



Note: The 802.11n clients cannot use the TKIP cipher. Therefore if only TKIP is enabled then the 802.11 clients will not be able to authenticate with the network.

If you select WPA/WPA2 as the security mode, additional fields display, as the following figure shows.

Security	<input type="radio"/> None <input type="radio"/> WEP <input checked="" type="radio"/> WPA/WPA2
	<input checked="" type="radio"/> WPA Personal <input type="radio"/> WPA Enterprise
WPA Versions	<input checked="" type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2
WPA Ciphers	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> CCMP(AES)
WPA Key Type	ASCII
WPA Key	<input type="text"/>
Bcast Key Refresh Rate	300 (0 to 86400)

Figure 365: WPA Personal Configuration

The following table describes the configuration options for the WPA Personal and WPA Enterprise security mode.

Table 330: WPA Security

Field	Description
WPA Personal or WPA Enterprise	<p>WPA/WPA2 Personal uses static key management. You manually configure the same keys to encrypt data on both the wireless client and the AP. WPA/WPA2 Enterprise uses a RADIUS server and dynamically generated keys to encrypt client-to- AP traffic. WPA Enterprise is more secure than WPA Personal, but you need a RADIUS server to manage the keys.</p> <p>If you select WPA Enterprise, the screen refreshes, and the WPA Key Type and WPA Key fields are hidden. The AP uses the global RADIUS server or the RADIUS server you specify for the wireless network</p> <p>For information about how to configure the global RADIUS server settings on the DWS-4000 Series switch, see “Wireless Global Configuration” on page 529.</p>
WPA Versions	<p>Select the types of client stations you want to support:</p> <ul style="list-style-type: none"> • WPA: If all client stations on the network support the original WPA but none support the newer WPA2, then select WPA. • WPA2: If all client stations on the network support WPA2, D-Link suggests using WPA2 which provides the best security per the IEEE 802.11i standard. • WPA and WPA2: If you have a mix of clients, some of which support WPA2 and others which support only the original WPA, select both of the boxes. This lets both WPA and WPA2 client stations associate and authenticate, but uses the more robust WPA2 for clients who support it. This WPA configuration allows more interoperability, at the expense of some security.
WPA Ciphers	<p>Select the cipher suite you want to use:</p> <ul style="list-style-type: none"> • TKIP • CCMP (AES) • TKIP and CCMP (AES) <p>Both TKIP and AES clients can associate with the access point. WPA clients must have one of the following to be able to associate with the AP:</p> <ul style="list-style-type: none"> • A valid TKIP key • A valid AES-CCMP key <p>Note: The 802.11n clients cannot use the TKIP cipher. Therefore if only TKIP is enabled then the 802.11 clients will not be able to authenticate with the network.</p>

Table 330: WPA Security (Cont.)

Field	Description
WPA Key Type	The key type is ASCII, which includes upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
WPA Key	The WPA Key is the shared secret key for WPA Personal. Enter a string of at least 8 characters to a maximum of 63 characters. Acceptable characters include upper and lower case alphabetic letters, the numeric digits, and special symbols such as @ and #.
Bcast Key Refresh Rate	Enter a value to set the interval at which the broadcast (group) key is refreshed for clients associated to this VAP. The valid range is 0-86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.
Additional Fields for WPA/WPA2 Enterprise	
Pre-Authentication	If you select WPA/WPA2 Enterprise, you can enable Pre-Authentication. Click the Pre-Authentication check box if you want WPA2 wireless clients to send pre-authentication packets. The pre-authentication information is relayed from the access point the client is currently using to the target access point. Enabling this feature can help speed up authentication for roaming clients who connect to multiple access points. Only clients that connect by using WPA2 can use this feature. It is not supported by the original WPA.
Pre-Authentication Limit	Enter the number of pre-authentications that can be in progress simultaneously on an AP. The limit prevents too much load on the RADIUS server. This does not prevent the pre-authentication from being attempted again when the load is lighter. A value of 0 represents no limit.
Key Caching Hold Time	Enter the amount of minutes a PMK will be held by the AP. This applies to Pairwise Master Keys (PMKs) generated by RADIUS, those that come from pre-authentication, and those that are forwarded to the AP. Note that this time limit can be overridden by RADIUS if the RADIUS server returns a longer time in the Session-Timeout attribute for a particular user. The valid values of this are from 1–1440 minutes. If you do not enter a value, APs will not forward the PMK for the wireless client to other APs in case the client roams to another AP.
Session Key Refresh Rate	Enter a value to set the interval at which the AP will refresh session (unicast) keys for each client associated to the VAP. The valid range is 0-86400 seconds. A value of 0 indicates that the broadcast key is not refreshed.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.
- **Clear**—Resets the settings on the page to the default values.

Valid Access Point Summary

The Wireless Global Configuration page contains a field to select whether to use a local or RADIUS database for AP Validation. The **Valid Access Point Summary** page contains information about APs configured in the local database. If the AP Validation is set to RADIUS, information about the APs to be managed by the switch must be added to the external RADIUS database.

You can add an AP into the local list of Valid APs from the **WLAN > Administration > Basic Setup > Valid AP** tab, as the following figure shows, or you can add an AP from the AP Authentication Failures or Rogue AP/RF Scan lists.

Figure 366: Adding a Valid AP

Table 331: Valid Access Point Summary

Field	Description
AP Database	Identifies the total number of APs that have been added to the AP database.
Managed AP	Identifies the number of APs in the database with an AP Mode set to Managed.
Rogue AP	Identifies the number of APs in the database with an AP Mode set to Rogue.
Standalone AP	Identifies the number of APs in the database with an AP Mode set to Standalone.
MAC Address	Enter the MAC address of the AP in this field. When you add the MAC address, you add the AP to the local database on the switch.
Location	Enter a location to help identify the AP. This field is optional and accepts up to 32 alphanumeric characters, including special characters.
AP Mode	This field displays the current mode of the AP, which can be one of the following: <ul style="list-style-type: none"> • Managed • Standalone • Rogue To configure a different mode, click the MAC address of the AP to go to the Valid Access Point Configuration page.

Table 331: Valid Access Point Summary

Field	Description
Profile	This field displays the AP profile assigned to the AP. To assign a different profile to the AP, click the MAC address of the AP to go to the Valid Access Point Configuration page. Click the profile name to access the configuration pages for the profile.

After you enter the MAC address and location of the AP to add to the list, click **Add** to add the AP to the database and to access the configuration page for the AP. For an AP that is already in the database, click the MAC address of the AP to access its configuration page.

Command Buttons

The page includes the following buttons:

- The **Delete** button clears an entry from the current list.
- The **Delete All** button clears all entries from the list.
- The **Refresh** button refreshes the list of APs.
- The **Change Profile** button changes the profile assigned to the selected AP or APs.

Valid Access Point Configuration

From the **Valid AP Configuration** page, you can manually set the channel and RF signal transmit power level for an individual AP. You can also configure the AP mode and local authentication password, and you can specify which profile the AP uses.

If you use the local database for AP validation, the switch maintains the database of access points that you validate. When you add the MAC address of an AP to the database, you can specify whether the AP is a managed AP, standalone AP, or a rogue. If the AP is to be managed by the switch, you can assign an AP profile to the device. When the switch collects and reports information from the RF scan, it can assign the appropriate status to an AP if it is in the database.



Note: Any configuration changes for a managed AP will not be applied until the AP is reset and re-authenticated. If you select a different profile from the menu, a pop-up message asks you to confirm the change. If the AP is managed, a second message asks if you would like to reset the AP. If you click OK, the AP is reset.

The screenshot shows the 'Valid Access Point Configuration' page. At the top, there are tabs for 'Global', 'Discovery', 'Profile', 'Radio', 'SSID', 'Valid AP', and 'OUI'. The 'Valid AP' tab is selected. The main content area contains the following fields and controls:

- MAC address:** A dropdown menu showing '00:22:b0:3a:c1:80'.
- AP Mode:** A dropdown menu showing 'Managed'.
- Location:** An empty text input field.
- Authentication Password:** An empty text input field with an 'Edit' checkbox to its right.
- Profile:** A dropdown menu showing '1 - Default'.
- Radio 1 - 802.11a/n:** A section with 'Channel' set to 'Auto' and 'Power (%)' set to '0'.
- Radio 2 - 802.11b/g/n:** A section with 'Channel' set to 'Auto' and 'Power (%)' set to '0'.

At the bottom of the form, there are three buttons: 'Refresh', 'Delete', and 'Submit'.

Figure 367: Configuring a Valid AP

Table 332 describes the fields available on the Valid Access Point Configuration page.

Table 332: Valid AP Configuration

Field	Description
MAC Address	This field shows the MAC address of the AP. To change this field, you must delete the entire Valid AP configuration and then enter the correct MAC address from the page that lists all Valid APs.
AP Mode	You can configure the AP to be in one of three modes: <ul style="list-style-type: none"> • Standalone: The AP acts as an individual access point in the network. You do not manage the AP by using the switch. Instead, you log on to the AP itself and manage it by using the Administrator Web User Interface (UI), CLI, or SNMP. If you select the Standalone mode, the screen refreshes and different fields appear. See the following table for the Standalone mode field descriptions. • Managed: The AP is part of the D-Link Unified Switch, and you manage it by using the DWS-4000 Series switch. If an AP is in Managed Mode, the Administrator Web UI and SNMP services on the AP are disabled. • Rogue: Select Rogue as the AP mode if you wish to be notified (through an SNMP trap, if enabled) when this AP is detected in the network. Additionally, when this AP is detected through an RF scan, the status is listed as Rogue. If you select the Rogue mode, the screen refreshes, and fields that do not apply to this mode are hidden.
Location	To help you identify the AP, you can enter a location. This field accepts up to 32 alphanumeric characters.
Authentication Password	You can require that the AP authenticate itself with the switch upon discovery. If you require authentication, which is a setting on the Basic Setup > Global tab, select the Edit option and enter the password in this field. The valid password range is between 8 and 63 alphanumeric characters. The password in this field must match the password configured on the AP.
Profile	If you configure multiple AP Profiles, you can select the profile to assign to this AP. For more information about configuring AP Profiles, see “Advanced Global Settings” on page 581 .

Table 332: Valid AP Configuration (Cont.)

Field	Description
Channel	<p>The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface and the country in which the APs operate.</p> <p>In the United States, IEEE 802.11b, 802.11g, and 2.4 GHz 802.11n modes (802.11 b/g/n) support the use of channels 1 through 11 inclusive, while IEEE 802.11a and 5-GHz 802.11n modes supports a larger set of non-consecutive channels (36,40,44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165).</p> <p>Interference can occur when multiple access points within range of each other are broadcasting on the same or overlapping channels. The impact of this interference on network performance can intensify during busy times when a large amount of data and media traffic is competing for bandwidth.</p> <p>If you select auto, the AP scans the RF area for occupied channels and selects a channel from the available non-interfering, or clear channels. The AP selects the best channel whenever its radio or radios restart.</p> <p>If you specify a channel, make sure that the channel does not interfere with the channel that neighbor APs use.</p> <p>Note: The channel you set for an AP in the valid AP database is fixed and takes precedence over initial channel selection done by the AP and any automatic channel planning done by the switch.</p> <p>Note: For radios that use 802.11a and/or 5-GHz 802.11n mode, some countries have a regulatory domain that requires radar detection. For these countries (based on the country code setting), the radio automatically uses the 802.11h protocol for selecting the channel if radar is detected on the statically assigned channel.</p>
Power	<p>The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range.</p> <p>The default value of 0 indicates that the AP uses the power level set in the AP profile.</p> <p>Note: The power level you set for an AP in the valid AP database is fixed and takes precedence over any automatic power adjustments done by the AP or the switch.</p>

Standalone APs are managed individually, and not by using a D-Link Unified Switch. By including standalone APs in the Valid AP database and specifying their expected settings, you can help ensure that only legitimate APs are on your network. If any of the expected settings you configure for the standalone AP do not match the settings detected through the RF scan, and the *Standalone AP with unexpected configuration* test is enabled on the **WLAN > Administration > Advanced Configuration > WIDS Security** page, the standalone AP is listed as a Rogue on the **WLAN > Monitoring > Access Point > Rogue/RF Scan** page.

If you select Standalone from the Managed Mode menu on the **Valid Access Point Configuration** page, the screen refreshes, and additional fields appear. The following table describes the additional information you can include about the standalone APs you add to the Valid AP database.

Table 333: Valid AP Configuration (Standalone Mode)

Field	Description
Expected SSID	Enter the SSID that identifies the wireless network on the standalone AP.
Expected Channel	Select the channel that the standalone AP uses. If the AP is configured to automatically select a channel, or if you do not want to specify a channel, select Any.
Expected WDS Mode	Standalone APs can use a Wireless Distribution System (WDS) link to communicate with each other without wires. The menu contains the following options: <ul style="list-style-type: none"> • Bridge: Select this option if the standalone AP you add to the Valid AP database is configured to use one or more WDS links. • Normal: Select this option if the standalone AP is not configured to use any WDS links. • Any: Select this option if the standalone AP might use a WDS link.
Expected Security Mode	Select the option to specify the type of security the AP uses: <ul style="list-style-type: none"> • Any—Any security mode • Open—No security • WEP—Static WEP or WEP 802.1X • WPA/WAP2—WPA and/or WPA2 (Personal or Enterprise)
Expected Wired Network Mode	If the standalone AP is allowed on the wired network, select Allowed. If the AP is not permitted on the wired network, select Not Allowed .

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Delete**—Deletes the AP from the local Valid AP database. Managed APs must be reset to complete their removal from the Valid AP database.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).

Local OUI Database Summary

To help identify AP and Wireless Client adapter manufacturers detected in the wireless network, the wireless switch contains a database of registered Organizationally Unique Identifiers (OUIs). This is a read-only list with over 10,000 registrations. From the **Local OUI Database Summary** page, you can enter up to 64 user-defined OUIs. The local list is searched first, so the same OUI can be located in the local list as well as the read-only list.

Figure 368: Local OUI Database Summary

Table 334: Local OUI Database Summary

Field	Description
OUI Value	Enter the OUI that represents the company ID in the format XX:XX:XX where XX is a hexadecimal number between 00 and FF. The first three bytes of the MAC address represents the company ID assignment. Note: The first byte of the OUI must have the least significant bit set to 0. For example 02:FF:FF is a valid OUI, but 03:FF:FF is not.
OUI Description	Enter the organization name associated with the OUI. The name can be up to 32 alphanumeric characters.

After you enter the OUI value and description, click **Add** to add the OUI to the local database.

Command Buttons

The page includes the following buttons:

- **Add**—Adds the OUI value and description information to the local OUI database.
- **Delete**—Deletes any selected OUI entries from the local OUI database. This button is available if the check box next to at least one OUI entry is selected.
- **Delete All**—Deletes all manually-added entries from the local OUI database.
- **Refresh**—Updates the page with the latest information.

AP Management

The AP Management folder contains links to the following pages that help you manage and maintain the APs on your D-Link Unified Switch network:

- [Reset](#)
- [RF Management](#)
- [Access Point Software Download](#)
- [Managed AP Advanced Settings](#)
- [AP Provisioning](#)

Reset

You can manually reset one or all APs from the DWS-4000 Series switch. When you issue the command to reset an AP, the AP closes the SSL connection to the switch before resetting the hardware.

To reset one or more APs, click **AP Management > Reset**.

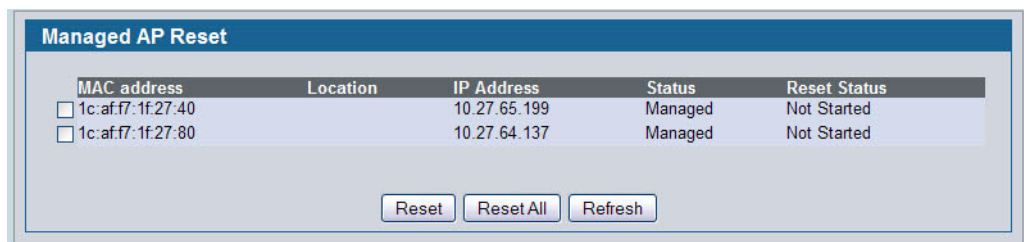


Figure 369: Access Point Reset

Table 335: Reset Fields

Field	Description
MAC Address	The MAC address of the AP
Location	The location of the AP, as specified in the Valid AP or RADIUS database
IP Address	The IP address of the AP
Status	Displays “Managed” to indicate that the AP is managed by the switch.
Reset Status	The status of the reset

Command Buttons

The page includes the following buttons:

- **Reset**—Resets the selected APs. To select an AP, click the check box next to the MAC address.
- **Reset All**—Resets all managed APs listed on the page.
- **Refresh**—Updates the page with the latest information.

The APs might take several minutes to reset and re-establish communication with the switch. While the AP is resetting, the status changes to failed, and then back to managed once the AP is back online.

RF Management

The radio frequency (RF) broadcast channel defines the portion of the radio spectrum that the radio on the access point uses for transmitting and receiving. The range of available channels for an access point is determined by the IEEE 802.11 mode (also referred to as band) of the access point.

The DWL-8600AP and DWL-6600AP are dual-band systems capable of operating in the 2.4 GHz and 5 GHz frequencies. The DWL-3600 is a single-band system and operates in the 2.4 GHz frequency. Multiple operating modes are available within each frequency. Configuration options for the IEEE 802.11a/n (5 GHz) modes do not apply to the DWL-3600AP.

IEEE 802.11b and 802.11g modes (802.11 b/g) operate in the 2.4-GHz RF frequency and support use of channels 1 through 11. IEEE 802.11a mode operates in the 5 GHz frequency and supports a larger set of non-consecutive channels (36,40,44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165). IEEE 802.11n mode can operate in either the 2.4 GHz or 5 GHz frequency.



Note: The available channels depends on the country in which the APs operate. The channels described in this section are valid for the United States.

Interference can occur when multiple access points within range of each other are broadcasting on the same or overlapping channels. The impact of this interference on network performance can intensify during busy times when a large amount of data and media traffic is competing for bandwidth. For the *b/g* radio band, the classical set of non-interfering channels is 1, 6, 11. Channels 1, 4, 8, 11 produce minimal overlap. A similar set of non-interfering channels is used for the *a* radio band, which includes all channels for that mode since they are not overlapping.

Configuring Channel Plan and Power Settings

The DWS-4000 Series switch software contains a channel plan algorithm that automatically determines which RF channels each AP should use to minimize RF interference. When you enable the channel plan algorithm, the switch periodically evaluates the operational channel on every AP it manages and changes the channel if the current channel is noisy.



Note: The regulation of radio frequencies and channel assignments varies from country to country. In countries that do not support channels 1, 6, and 11 on the 802.11b/g/n radio, the channel plan algorithm is inactive. For the 5-GHz radio, the algorithm is inactive in countries that require 802.11h radar detection, which includes European countries and Japan.

The automatic channel selection algorithm does not affect APs that meet any of the following conditions:

- The channel is statically assigned to the AP in the RADIUS or local AP database.
- The channel has been statically assigned to the AP from the **WLAN > Administration > AP Management > Advanced Settings** page.
- The AP uses a profile that has the Automatic Channel field disabled (Radio Configuration setting).



Note: If the AP is not assigned a fixed channel or is not assigned a specific channel by the automatic channel selection algorithm, the AP channel selection mode is set to best. This means that the AP selects the best channel whenever the radio restarts or if the AP detects a radar signal.

The RF transmission power level affects how far an AP broadcasts its signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range or broadcast the signal beyond the desired physical boundaries, which can create a security risk.

Automatic power uses a proprietary algorithm to automatically adjust the RF signal to broadcast far enough to reach wireless clients, but not so far that it interferes with RF signals broadcast by other APs.

To configure Channel Plan and Power Adjustment settings, click **AP Management > RF Management**.

Configuration	Channel Plan History	Manual Channel Plan	Manual Power Adjustments
RF Configuration			
Channel Plan	<input checked="" type="radio"/> 5 GHz (802.11 a/n) <input type="radio"/> 2.4 GHz (802.11 b/g/n)		
Channel Plan Mode	<input type="radio"/> Fixed Time <input checked="" type="radio"/> Manual <input type="radio"/> Interval		
Channel Plan History Depth	5 (0 to 10)		
Channel Plan Interval (hours)	6 (6 to 24)		
Channel Plan Fixed Time (hh:mm)	0 : 0		
Power Adjustment Mode	<input checked="" type="radio"/> Manual <input type="radio"/> Interval		
Power Adjustment Interval (minutes)	15 (15 to 1440)		
<input type="button" value="Submit"/>			

Figure 370: RF Channel Plan and Power Configuration

[Table 336 on page 565](#) describes the RF Channel Plan and Power Adjustment fields you can configure.



Note: When the AP changes its channel, all associated wireless clients temporarily lose their connection to the AP and must re-associate. The re-association can take several seconds, which can affect time-sensitive traffic such as voice and video.

Table 336: RF Channel Plan and Power Adjustment

Field	Description
Channel Plan	Each AP is dual-band capable of operating in the 2.4 GHz and 5 GHz frequencies. The 802.11a/n and 802.11b/g/n modes use different channel plans. Before you configure channel plan settings, select the mode to configure.
Channel Plan Mode	This field indicates the channel assignment mode. The mode of channel plan assignment can be one of the following: <ul style="list-style-type: none"> • Fixed Time: If you select the fixed time channel plan mode, you specify the time for the channel plan and channel assignment. In this mode the plan is applied once every 24 hours at the specified time. • Manual: With the manual channel plan mode, you control and initiate the calculation and assignment of the channel plan. You must manually run the channel plan algorithm and apply the channel plan to the APs. • Interval: In the interval channel plan mode, the switch periodically calculates and applies the channel plan. You can configure the interval to be from every 6 to every 24 hours. The interval period begins when you click Submit.
Channel Plan History Depth	The channel plan history lists the channels the switch assigns each of the APs it manages after a channel plan is applied. Entries are added to the history regardless of interval, time, or channel plan mode. The number you specify in this field controls the number of iterations of the channel assignment. Note: The APs changed in previous iterations cannot be assigned new channels in the next iteration. This history prevents the same APs from being changed time after time.
Channel Plan Interval	If you select the Interval channel plan mode, you can specify the frequency at which the channel plan calculation and assignment occurs. The interval time is in hours, and you can specify an interval that ranges between every 6 hours to every 24 hours.
Channel Plan Fixed Time	If you select the Fixed Time channel plan mode, you can specify the time at which the channel plan calculation and assignment occurs. The channel plan calculation will occur once every 24 hours at the time you specify.
Power Adjustment Mode	You can set the power of the AP radio frequency transmission in the AP profile, the local database or in the RADIUS server. The power level in the AP profile is the default level for the AP, and the power will not be adjusted below the value in the AP profile. The settings in the local database and RADIUS server always override power set in the profile setting. If you manually set the power, the level is fixed and the AP will not use the automatic power adjustment algorithm. You can configure the power as a percentage of maximum power, where the maximum power is the minimum of power level allowed for the channel by the regulatory domain or the hardware capability. <ul style="list-style-type: none"> • Manual: In this mode, you run the proposed power adjustments manually from the Manual Power Adjustments page. • Interval: In this mode, the switch periodically calculates the power adjustments and applies the power for all APs. The interval period begins when you click Submit. Note: If you set the power level in the local or RADIUS database, the settings override the power level set in the AP profile. Note: This setting gets applied to both radios of the AP. For more information about manually setting the power level, see “Radio Configuration” on page 538 and “Valid Access Point Summary” on page 556 .

Table 336: RF Channel Plan and Power Adjustment (Cont.)

Field	Description
Power Adjustment Interval	This field determines how often the switch runs the power adjustment algorithm. The algorithm runs automatically only if you set the power adjustment mode to Interval . Note: This setting gets applied to both radios of the AP.

Command Buttons

The page includes the following button:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tools > Save Changes).

Viewing the Channel Plan History

The DWS-4000 Series switch stores channel assignment information for the APs it manages. To access the Channel Plan History information, click the **AP Management > RF Management > Channel Plan History** tab.

The Cluster Controller switch that controls the cluster maintains the channel history information for all switches in the cluster. On the Cluster Controller, the page shows information about the radios on all APs managed by switches in the cluster that are eligible for channel assignment and were successfully assigned a new channel.

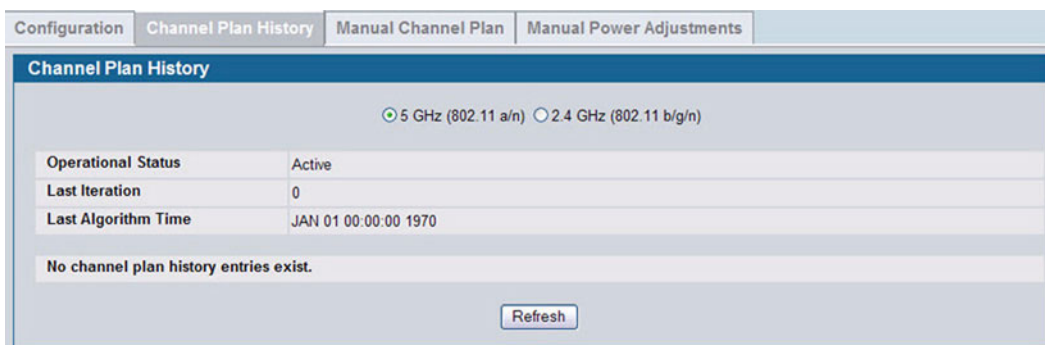
**Figure 371: Channel Plan History**

Table 337 describes the Channel Plan History fields.

Table 337: Channel Plan History

Field	Description
5 GHz (802.11a/n) 2.4 GHz (802.11b/g/n)	The 5 GHz and 2.4 GHz radios use different channel plans, so the switch tracks the channel history separately for each radio. The channel information that displays on the page is only for the radio you select.
Operational Status	This field shows whether the switch is using the automatic channel adjustment algorithm on the AP radios.

Table 337: Channel Plan History (Cont.)

Field	Description
Last Iteration	<p>The number in this field indicates the most recent iteration of channel plan adjustments. The APs that received a channel adjustment in previous iterations cannot be assigned new channels in the next iteration to prevent the same APs from being changed time after time.</p> <p>On the AP Management > RF Management > Configuration tab, you can set the history depth to control the maximum number of iterations stored and displayed in the channel plan history.</p>
Last Algorithm Time	<p>Shows the date and time when the channel plan algorithm last ran.</p> <p>Note: To set the system time on the switch, you must use SNTP, which is disabled by default. From the Web interface, you configure the SNTP client and server information from the pages in the LAN > Administration > System > SNTP folder. From the CLI, use the <code>sntp</code> commands in Global Config mode.</p>
AP MAC Address Location Radio Iteration Channel	This table displays the channel assigned to an AP in an iteration of the channel plan.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Initiating Manual Channel Plan Assignments

If you specify Manual as the Channel Plan Mode on the Configuration tab, the **Manual Channel Plan** page allows you to initiate the channel plan algorithm.

To manually run the channel plan adjustment feature, select the radio to update the channels on (5 GHz or 2.4 GHz) and click **Start**.

**Figure 372: Manual Channel Plan**

To apply proposed channel changes, click **Apply**.

Table 338: Manual Channel Plan

Field	Description
Status	Shows the Current Status of the plan, which is one of the following states: <ul style="list-style-type: none"> • None: The channel plan algorithm has not been manually run since the last switch reboot. • Algorithm In Progress: The channel plan algorithm is running. • Algorithm Complete: The channel plan algorithm has finished running. A table displays to indicate proposed channel assignments. Each entry shows the AP along with the current and new channel. To accept the proposed channel change, click Apply. You must manually apply the channel plan for the proposed assignments to be applied. • Apply In Progress: The switch is applying the proposed channel plan and adjusting the channel on the APs listed in the table. • Apply Complete: The algorithm and channel adjustment are complete.
Proposed Channel Plan Entries	
Note: If no APs appear in the table after the algorithm is complete, the algorithm does not recommend any channel changes.	
Current Channel	Shows the current operating channel for the AP that the algorithm recommends for new channel assignments.
New Channel	Shows the proposed operating channel for the AP.

It is possible for the network configuration to change between the time the automatic channel selection runs and the time you attempt to apply the proposed channel assignments.

The channel will fail to be applied to an AP if one of the following conditions exist:

- The AP has failed.
- The radio on the AP has been disabled through a profile update.
- The channel is not valid for the radio mode.
- The AP has been rebooted since the channel plan was computed and acquires a static channel that has been set statically via local database.
- The channel has been set manually through the advanced page.
- The auto-channel mode has been disabled in the profile for this AP.

Command Buttons

The page includes the following buttons:

- **Apply**—Apply the proposed channel change to the AP and change the current channel to the new channel.
- **Clear**—Clear the proposed channel plan information.
- **Refresh**—Updates the page with the latest information.
- **Start**—Initiate the channel plan algorithm.

Initiating Manual Power Adjustments

If you select Manual as the Power Adjustment Mode on the Configuration tab, you can manually initiate the power adjustment algorithm on the **Manual Power Adjustments** page.

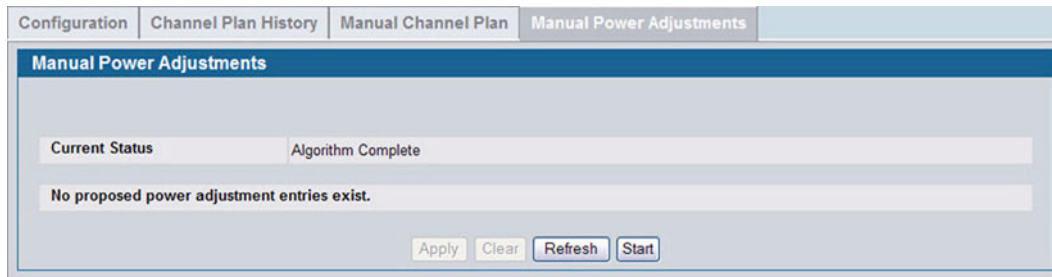


Figure 373: Manual Power Adjustments

Table 339: Manual Power Adjustments

Field	Description
Status	Shows the Current Status of the plan, which is one of the following states: <ul style="list-style-type: none"> • None: The power adjustment algorithm has not been manually run since the last switch reboot. • Algorithm In Progress: The power adjustment algorithm is running. • Algorithm Complete: The power adjustment algorithm has finished running. • A table displays to indicate proposed power adjustments. Each entry shows the AP along with the current and new power levels. To accept the proposed change, click Apply. You must manually apply the power adjustment for the proposed assignments to be applied. • Apply In Progress: The switch is adjusting the power levels that the APs use. • Apply Complete: The algorithm and power adjustment are complete.
AP MAC Address	Identifies the AP MAC address.
Location	Identifies the location of the AP, which is set in the Valid AP database.
Radio	Identifies the radio.
Current Power	Shows the current power level for the AP.
New Power	Shows the proposed power level for the AP.

Command Buttons

The page includes the following buttons:


- **Apply**—Apply the proposed power adjustment to the AP and change the current power level to the new power.
- **Clear**—Clear the proposed power adjustment information.
- **Refresh**—Updates the page with the latest information.
- **Start**—Initiate the power adjustment algorithm.

Access Point Software Download

The DWS-4000 Series switch can upgrade software on the APs that it manages. The Cluster Controller can update code on APs managed by peer wireless switches.

To upgrade one or more AP from the switch that manages it, click the **WLAN > Administration > AP Management > Software Downloads** tab.

Access Point Software Download	
Server Address	0.0.0.0
img_dwl8600	DLink 8600 AP Radios
File Path	
File Name	
img_dwl3600/6600	DLink AP-3600/6600 Radios
File Path	
File Name	
Group Size	10 (1 to 64)
Image Download Type	All images
Managed AP	All 1c:af:f7:1f:27:40 - 10.27.65.199 - 1c:af:f7:1f:27:80 - 10.27.64.137 -

 It may take about 12 minutes for the upgrade process to complete for an AP. After this process is complete, the AP will restart automatically and will become managed again.

Submit Start Refresh

Figure 374: Software Download

After you provide the information about the upgrade file, as described in the following table, click **Start** to begin the upgrade process. Additional fields appear after the download begins and provide information about upgrade status and success.



Note: The APs automatically reset after the code is successfully downloaded and installed.

Table 340 describes the fields you must complete to upgrade APs.

Table 340: Software Download

Field	Description
Server Address	Enter the IP address of the host where the upgrade file is located. The host must have a TFTP server installed and running.
File Path	Enter the file path on the TFTP server where the software is located. You may enter up to 96 characters.
File Name	Enter the name of the upgrade file. You may enter up to 32 characters, and the file extension <i>.tar</i> must be included.
Group Size	When you upgrade multiple APs, each AP contacts the TFTP server to download the upgrade file. To prevent the TFTP server from being overloaded, you can limit the number of APs to be upgraded at a time. In the Group Size field, enter the number of APs that can be upgraded at the same time. When one group completes the upgrade, the next group begins the process.
Image Download Type	Type of the image to be downloaded, which can be one of the following: <ul style="list-style-type: none"> • All images (img_dwl8600 and img_dwl3600/6600) • img_dwl8600 • img_dwl3600/6600 <p>Note: To download all images, make sure you specify the file path and file name for both images in the appropriate File Path and File Name fields.</p>
Managed AP	The list shows all the APs that the switch manages. If the switch is the Cluster Controller, then the list shows the APs managed by all switches in the cluster. Each AP is identified by its MAC address, IP address, and Location in the <MAC - IP - Location> format. To upgrade a single AP, select the AP MAC address from the drop down list. To upgrade all APs, select All from the top of the list. If All is selected, the Group Size field will limit the number of simultaneous AP upgrades in order not to overwhelm the TFTP server. To select multiple APs to upgrade, CTRL + click the APs to upgrade. Note: D-Link recommends that you upgrade all managed APs at the same time.
The following fields display after you click Start:	
Status (Global)	The status of the upgrade process for all APs: <ul style="list-style-type: none"> • Not Started: The DWS-4000 Series switch has not started the download process. • Requested: A request to download AP software has been made, but the switch has not done any downloads. • Code Transfer in Progress: A download is in progress. • Failure: Download failed on all APs. • Aborted: Download was aborted before the AP loaded code from the TFTP server. • NVRAM-Update-in-Progress: Download completed successfully. The reset command has been sent to the AP. • Success: All APs are connected to the DWS-4000 Series switch.

Table 340: Software Download (Cont.)

Field	Description
Status (per-AP)	<p>A table also appears and lists each AP, its download status, and the software version it is downloading. The status for an individual AP can have one of the following values:</p> <ul style="list-style-type: none"> • Requested: A download is planned for this AP, but the AP is not in the current download group, so it hasn't been told to start the download yet. • Code-Transfer-In-Progress: The AP has been told to download the code. • Failure: The AP reported a failing code download. • Aborted: The download was aborted before the AP loaded code from the TFTP server. • Waiting-For-APs-To-Download: A download finished on this AP, and it is waiting for other APs to finish download. Reset command is not sent to the AP in this state. • NVRAM-Update-In-Progress: Download completed successfully. The reset command sent to the AP. • Timed-Out: The AP did not reconnect to the DWS-4000 Series switch in the fixed time interval.
Download Count	The number of managed APs to download software in the current download request. If you selected All for the managed APs to upgrade, the download count shows the number of managed APs at the time the download request was started. The value is 1 if only one AP is being updated.
Success Count	The number of APs that have successfully downloaded the new code. This value starts with 0 at the beginning of the download and increases by one for every AP that successfully downloaded the code.
Failure Count	The number of APs that failed to download the new code starting at 0 and incrementing with each failure.
Abort Count	The number of APs for which the download was aborted, starting at 0 and incrementing each aborted download.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.
- **Start**—Initiate the software download.

Managed AP Advanced Settings

When the AP is in Managed mode, remote access to the AP is disabled. However, you can enable Telnet access by enabling the Debug feature on the **AP Management > Advanced Settings** page. From the **Managed AP Advanced Settings** page, you can also manually change the RF channel and power for each radio on an AP. The manual power and channel changes override the settings configured in the AP profile (including automatic channel selection) and take effect immediately. The manual channel and power assignments are not retained when the AP is reset or if the profile is reapplied to the AP, such as when the AP disassociates and reassociates with the switch.

MAC address	Location	Debug	Radio	Channel	Power (%)
00:22:b0:3a:c1:80		Disabled	1-802.11a/n	149	100
00:22:b0:3a:c9:80		Disabled	2-802.11b/g/n	5	100
			1-802.11a/n	124	100
			2-802.11b/g/n	5	100

Figure 375: Advanced AP Management

Each AP managed by the DWS-4000 Series switch is listed by its MAC address and location. The location is based on the value in the RADIUS or local Valid AP database. [Table 341](#) describes the Advanced features you can configure for the AP.

Table 341: Advanced AP Management

Field	Description
MAC Address	Shows the MAC address of the AP.
Location	Shows the AP location, which is based on the value configured in the RADIUS or local Valid AP database.
Debug	<p>To help you troubleshoot, you can enable Telnet access to the AP so that you can debug the device from the CLI.</p> <p>The Debug field shows the debug status and can be one of the following:</p> <ul style="list-style-type: none"> • Disabled • Set Requested • Set in Progress • Enabled <p>To change the status, click the Debug status link. The Managed AP Debug page appears. Table 342 describes the fields on the new page.</p>
Radio	Identifies the radio to which the channel and power settings apply.
Channel	Click the Channel link to access the Managed AP Channel/Power Adjust page. From that page, you can set a new channel for Radio 1 or Radio 2. The available channels depend on the radio mode and country in which the APs operate. The manual channel change overrides the channel configured in the AP profile and is not retained when the AP reboots or when the AP profile is reapplied. Table 343 on page 576 describes the fields on the new page.

Table 341: Advanced AP Management (Cont.)

Field	Description
Power	Click the Power link to access the Managed AP Channel/Power Adjust page. From that page, you can set a new power level for the AP. The manual power change overrides the power setting configured in the AP profile and is not retained when the AP reboots or when the AP profile is reapplied. Table 343 on page 576 describes the fields on the new page.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Debugging the AP

You can enable debugging on an AP to allow Telnet access to the access point. Once you Telnet to the AP, you can issue commands from the CLI to help you troubleshoot.

The fields in [Table 342 on page 574](#) appear when you click the Debug link for a managed AP on the **Managed AP Advanced** page.

Managed AP Debug	
MAC address	00:22:B0:3A:C1:80
Location	
IP Address	10.27.65.132
Status	None
Password	<input type="text"/>
Confirm Password	<input type="text"/>
Enable Debug	<input type="checkbox"/>
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

Figure 376: Managed AP Debug**Table 342: Managed AP Debug**

Field	Description
MAC Address	Shows the MAC address of the access point.
Location	Shows the location of the access point, as configured in the Valid AP database.
IP Address	Shows the IP address of the AP.
Status	Shows the debug status, which can be one of the following: <ul style="list-style-type: none"> • None: Debugging has not been enabled or disabled. • Set Requested: A request has been made to change the debug status. • Set Complete: Debugging has been enabled or disabled.
Password	Enter the admin password for the AP (the default is admin).

Table 342: Managed AP Debug

Field	Description
Confirm Password	Since the password is encrypted, you must retype the password to confirm the password.
Enable Debug	<p>Select or clear the Enable check box to enable or disable debugging.</p> <p>Once once you Telnet to the AP, you get an AP interface login prompt. The user name is admin. Enter the password you set in the previous field. The default password is admin if you did not specify a new password. From the AP CLI, you can also access the standard Linux prompt by typing the '!' character.</p> <p>You can issue the following debug commands at the Linux OS prompt:</p> <ul style="list-style-type: none"> • <code>get management</code>: Display management interface information • <code>get managed-ap</code>: Display managed AP information <p>You can issue the following debug commands at the Linux OS prompt:</p> <ul style="list-style-type: none"> • <code>ifconfig</code>: display all interfaces. • <code>cat /proc/meminfo</code>: View memory utilization

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Adjusting the Channel and Power

Changes you make to the channel and power are runtime changes only. If you change the channel or power settings, the new settings are lost if the AP or switch is reset.

Managed AP Channel/Power Adjust	
AP MAC Address	1C:AF:F7:1F:27:40
Radio	1-802.11a/n
Channel Status	None
Channel	▼
Power Status	None
Power (%)	0 (1 to 100)
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

Figure 377: Managed AP Debug

The fields in [Table 343 on page 576](#) appear when you click the current channel or power setting for an AP on the **Managed AP Advanced** page.

Table 343: Managed AP Channel/Power Adjust

Field	Description
AP MAC Address	Shows the MAC address of the access point.
Radio	Displays the radio and its mode. The changes apply only to this radio.
Channel Status	The status is one of the following: <ul style="list-style-type: none"> • None • Set Requested • Set Complete
Channel	<p>The Channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface.</p> <p>In the United States, IEEE 802.11b, 802.11g, and 2.4 GHz 802.11n modes (802.11 b/g/n) support the use of channels 1 through 11 inclusive, while IEEE 802.11a and 5-GHz 802.11n modes supports a larger set of non-consecutive channels (36,40,44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165).</p> <p>Note: The available channels depends on the country in which the APs operate.</p> <p>Note: For radios that use 5 GHz modes, some countries have a regulatory domain that requires radar detection. For these countries (based on the country code setting), the radio automatically uses the 802.11h protocol for selecting the channel if radar is detected on the statically assigned channel.</p> <p>Interference can occur when multiple access points within range of each other are broadcasting on the same or overlapping channels. The impact of this interference on network performance can intensify during busy times when a large amount of data and media traffic is competing for bandwidth.</p> <p>If you select auto, the AP scans the RF area for occupied channels and selects a channel from the available non-interfering, or clear channels.</p> <p>If you specify a channel, make sure that the channel does not interfere with the channel that neighbor APs use.</p>
Power Status	The status is one of the following: <ul style="list-style-type: none"> • None • Set Requested • Set Complete
Power	The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range.

Command Buttons

The page includes the following buttons:

- **Cancel**—Cancels any actions and returns to the previous page.
- **Apply**—Applies the settings to the AP.

AP Provisioning

The AP Provisioning feature helps you add new APs to an existing switch cluster. With AP Provisioning, you can configure the access points with parameters that are needed to connect to the wireless network.



Note: The AP Provisioning Summary and Detail pages display data only when the switch is configured as the Cluster Controller.

Use AP Provisioning to connect devices to a network enabled for mutual authentication. If a network is not enabled for mutual authentication then APs can be attached to the network by properly configuring the local Valid AP database or RADIUS AP database and discovery options. The provisioning feature can optionally be used on networks not enabled for mutual authentication to simplify AP attachment to the cluster.

AP Provisioning Summary Status

Use the **AP Provisioning Summary Status** page to view information about all provisioned APs.

MAC Address (*-Managed)	IP Address	Primary IP Address	Backup IP Address	New Primary IP Address	New Backup IP Address	Status	Age
00:05:5e:56:26:90	10.27.65.109					Not Started	0d:00:00:16
00:22:44:66:88:00	10.27.64.114					Not Started	0d:02:03:10
00:22:44:66:88:80	10.27.65.74					Not Started	0d:00:00:16
* 1c:af:f7:1f:27:40	10.27.65.199					Not Started	0d:00:00:02
* 1c:af:f7:1f:27:80	10.27.64.137					Not Started	0d:00:00:02
5c:d9:98:2f:3f:00	10.27.65.150					Not Started	0d:00:00:16

* - Only Unmanaged APs can be deleted.

Figure 378: AP Provisioning Summary Status

The following table shows the fields available on the **AP Provisioning Summary Status** page.

Table 344: AP Provisioning Summary Status

Field	Description
MAC Address	MAC address of the AP
IP Address	IP Address of the AP.
Primary IP Address	The IP address of the primary provisioned switch as reported by the AP.
Backup IP Address	The IP address of the backup provisioned switch as reported by the AP.
New Primary IP Address	Enter the IP address of primary switch to which the AP should try to connect.
New Backup IP Address	Enter the IP address of switch to which the AP should try to connect if it is unable to connect to the primary switch.

Table 344: AP Provisioning Summary Status (Cont.)

Field	Description
Status	Status of the most recently issued AP provisioning command, which has one of the following values: <ul style="list-style-type: none"> • Not Started—Provisioning has not been done for this AP. • Success—Provisioning finished successfully for this switch. The AP Provisioning Status table should reflect the latest provisioning configuration. • In Progress—Provisioning is executing for this AP. • Invalid Switch IP Address—Either primary or backup switch IP address is not in the cluster or the mutual authentication mode is enabled and the primary switch IP address is not specified. • Provisioning Rejected—AP is not managed and is configured not to accept provisioning data in unmanaged mode. • Timed Out—The last provisioning request timed out.
Age	Amount of time since the AP last sent an update.

Command Buttons

The page includes the following buttons:

- **Delete**—Remove the selected AP from the AP provisioning list.
- **Delete All**—Remove all APs from the AP provisioning list.
- **Provision**—Initiate provisioning for the selected AP. You can provision an AP only from the cluster controller. After the AP is provisioned, it should become managed by the switch with the configured Primary IP Address and appear in the AP provisioning database as a managed AP.
- **Refresh**—Updates the page with the latest information.

Detailed AP Provisioning Status

Use the **AP Provisioning Status** (detail) page to view detailed provisioning information about an AP and to specify the IP address of the primary or backup switch that provides provisioning information for the AP.



Note: The AP Provisioning Detail page displays data only when the switch is configured as the Cluster Controller.

Select the MAC address of the AP from the drop-down menu to view provisioning information about that AP.

AP Provisioning Status			
00:05:5E:56:26:90 ▼			
IP Address	10.27.65.109	Time Since Last Update	0d:00:00:01
Primary IP Address	0.0.0.0	Backup IP Address	0.0.0.0
Mutual Authentication Mode	Disable	Unmanaged AP Reprovisioning Mode	Disable
AP Provisioning Status	Not Started	AP Certificate and Profile Transmit Status	Not Started
New Primary IP Address	<input type="text" value="0.0.0.0"/>	New Backup IP Address	<input type="text" value="0.0.0.0"/>
Profile	1-Default ▼		

Figure 379: AP Provisioning Status—Detail

The following table shows the fields available on the **AP Provisioning Status** page.

Table 345: AP Provisioning Status

Field	Description
IP Address	IP Address of the AP.
Time Since Last Update	Time since any information has been received from this access point.
Primary IP Address	The IP address of the primary provisioned switch as reported by the AP.
Backup IP Address	The IP address of the backup provisioned switch as reported by the AP.
Mutual Authentication Mode	Shows whether the Mutual Authentication mode is currently enabled.
Unmanaged AP Reprovisioning Mode	The configured re-provisioning mode in the AP, which is one of the following: <ul style="list-style-type: none"> • Enable—The AP can be reprovisioned when it is not managed. • Disable—The AP cannot be reprovisioned when it is not managed.
AP Provisioning Status	Status of the most recently issued AP provisioning command, which is one of the following: <ul style="list-style-type: none"> • Not Started—Provisioning has not been done for this AP. • Success—Provisioning finished successfully for this switch. The AP Provisioning Status Table should reflect the latest provisioning configuration. • In Progress—Provisioning is executing for this AP. • Invalid Switch IP Address—Either primary or backup switch IP address is not in the cluster or the mutual authentication mode is enabled and the primary switch IP address is not specified. • Provisioning Rejected—AP is not managed and is configured not to accept provisioning data in unmanaged mode. • Timed Out—The last provisioning request timed out.

Table 345: AP Provisioning Status (Cont.)

Field	Description
AP Certificate and Profile Transmit Status	<p>Status of the last AP profile and X.509 Certificate distribution to the Primary and Backup switches. This status is changed as a result of the AP provisioning command. The X.509 certificate is sent to the primary and backup switches only if mutual authentication is enabled.</p> <p>The status is one of the following:</p> <ul style="list-style-type: none"> • Not Started—No information for this AP has been sent to the primary and backup switch. • Success—AP Profile and X.509 Certificate is sent to Primary and Backup Switches. • Failed—The primary or backup switch wasn't in the cluster when this switch attempted to send the information.
New Primary IP Address	Enter the IP address of the switch that should manage the AP.
New Backup IP Address	Enter the IP address of switch to which the AP should try to connect if it is unable to connect to the primary switch.
Profile	Select the AP profile that the AP should use.

Command Buttons

The page includes the following buttons:

- **Delete**—Remove the AP from the AP provisioning list.
- **Provision the AP**—Initiate provisioning for the AP. After the AP is provisioned, it should become managed by the switch with the configured Primary IP Address and appear in the AP provisioning database as a managed AP.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.

Configuring Advanced Settings

The Advanced Configuration folder contains links to the following pages:

- [Advanced Global Settings](#)
- [Known Client](#)
- [Wireless Network List](#)
- [AP Profiles](#)
- [Peer Switch](#)
- [WIDS Security](#)
- [Known Client](#)
- [Switch Provisioning](#)

This section also describes the Unified Wired and Wireless Access System support for the AeroScout™ engine in “Enabling AeroScout™ Engine Support” on page 626.

Advanced Global Settings

The fields on the advanced **Wireless Global Configuration page** are settings that apply to the DWS-4000 Series switch.

Wireless Global Configuration		
Peer Group ID	1	(1 to 255)
Client Roam Timeout (secs)	30	(1 to 120)
Ad Hoc Client Status Timeout (hours)	24	(0 to 168)
AP Failure Status Timeout (hours)	24	(0 to 168)
MAC Authentication Mode	white-list	
RF Scan Status Timeout (hours)	24	(0 to 168)
Detected Clients Status Timeout (hours)	24	(0 to 168)
AP Provisioning Database Age Time(hours)	72	(0 to 240)
Tunnel IP MTU Size	1500	
Cluster Priority	1	(0 to 255,0-Disable)
AP Client QoS	Disable	
TSPEC Violation Report Interval (secs)	300	(0 to 900, 0 - Disable)
Base IP Port	57775	(1 to 65000)

Figure 380: Global Configuration

Table 346 describes the fields on the **Wireless Global Configuration** page.

Table 346: General Global Configurations

Field	Description
Peer Group ID	In order to support larger networks, you can configure wireless switches as peers, with up to 8 switches in a cluster (peer group). Peer switches share some information about APs and allow L3 roaming among them. Peers are grouped according to the Group ID.
Client Roam Timeout	This value determines how long to keep an entry in the Associated Client Status list after a client has disassociated. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.
Ad Hoc Client Status Timeout	This value determines how long to keep an entry in the Ad Hoc Client Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.
AP Failure Status Timeout	This value determines how long to keep an entry in the AP Authentication Failure Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.
MAC Authentication Mode	Select the global action to take on wireless clients in the <ul style="list-style-type: none"> • white-list: Select this option to specify that any wireless clients with MAC addresses that are specified in the Known Client database, and are not explicitly denied access, are granted access. If the MAC address is not in the database then the access to the client is denied. • black-list: Select this option to specify that any wireless clients with MAC addresses that are specified in the Known Client database, and are not explicitly granted access, are denied access. If the MAC address is not in the database then the access to the client is granted. <p>MAC Authentication is enabled at the network level. The network configuration also defines whether MAC addresses are looked up on the local database or on the RADIUS server.</p>
RF Scan Status Timeout	This value determines how long to keep an entry in the RF Scan Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.
Detected Clients Status Timeout	This value determines how long to keep an entry in the Detected Client Status list. Each entry in the status list shows an age, and when the age reaches the value you configure in the timeout field, the entry is deleted.

Table 346: General Global Configurations

Field	Description
Tunnel IP MTU Size	<p>Select the maximum size of an IP packet handled by the network. The MTU is enforced only on tunneled VAPs.</p> <p>When IP packets are tunneled between the APs and the DWS-4000 Series switch, the packet size is increased by 20 bytes during transit. This means that clients configured for 1500 byte IP MTU size may exceed the maximum MTU size of existing network infrastructure which is set up to switch and route 1518 (1522-tagged) byte frames. If you increase the tunnel IP MTU size, you must also increase the physical MTU of the ports on which the traffic flows.</p> <p>Note: If any of the following conditions are true, you do not need to increase the tunnel IP MTU size:</p> <ul style="list-style-type: none"> • The wireless network does not use L3 tunneling. • The tunneling mode is used only for voice traffic, which typically has small packets. • The tunneling mode is used only for TCP based protocols, such as HTTP. This is because the AP automatically reduces the maximum segment size for all TCP connections to fit within the tunnel.
Cluster Priority	<p>Specify the priority of this switch for the Cluster Controller election.</p> <p>The switch with highest priority in a cluster becomes the Cluster Controller. If the priority is the same for all switches, then the switch with lowest IP address becomes the Cluster Controller. A priority of 0 means that the switch cannot become the Cluster Controller. The highest possible priority is 255.</p>
AP Client QoS	<p>Enable or disable the client QoS feature. If AP Client QoS is disabled, the Client QoS configuration remains in place, but any ACLs or DiffServ policies applied to wireless traffic are not enforced.</p> <p>The Client QoS feature extends the primary QoS capabilities of the DWS-4000 Series switch to the wireless domain. More specifically, access control lists (ACLs) and differentiated service (DiffServ) policies are applied to wireless clients associated to the AP.</p>
TSPEC Violation Report Interval	<p>A TSPEC is a traffic specification that is sent from a QoS-capable wireless client to an AP requesting a certain amount of network access for the traffic stream (TS) it represents.</p> <p>The TSPEC Violation Report Interval specifies the normal frequency with which wireless clients detected as using admission-controlled resources without proper TSPEC authorization are reported through system logging and SNMP traps.</p> <p>If a violating client disassociates before the next reporting interval, it is reported upon disassociation.</p> <p>Setting this parameter to 0 disables TSPEC violation reporting.</p>
Base IP Port	<p>Sets the first IP port number within the range that the wireless system uses to send and receive IP traffic.</p> <p>By default the Wireless system uses the IP ports 57775 to 57784.</p> <p>If you change the base IP port, the wireless feature is automatically disabled and re-enabled. The default Wireless IP port is not sent as part of the global switch configuration in the cluster configuration distribution command, so every switch in the cluster must be configured independently with the new IP port number.</p> <p>If the Wireless IP port number is changed from its default value on the switch, then it must also be changed on the Access Points. The port can be set on the AP via an AP administrative command, or DHCP option 43, sub-option 3. If the port is set via DHCP then the DHCP setting supersedes the configured setting.</p>

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.

Wireless SNMP Trap Configuration

If you use Simple Network Management Protocol (SNMP) to manage the DWS-4000 Series switch, you can configure the SNMP agent on the switch to send traps to the SNMP manager on your network from the **Administration > Advanced Configuration > Global > SNMP Traps** tab.

Wireless SNMP Trap Configuration	
AP Failure Traps	Disable ▼
AP State Change Traps	Disable ▼
Client Failure Traps	Disable ▼
Client State Change Traps	Disable ▼
Peer Switch Traps	Disable ▼
RF Scan Traps	Disable ▼
Rogue AP Traps	Disable ▼
TSPEC Traps	Disable ▼
WIDS Status Traps	Disable ▼
Wireless Status Traps	Disable ▼

Figure 381: SNMP Trap Configuration

When an AP is managed by a switch, it does not send out any traps. The switch generates all SNMP traps based on its own events and the events it learns about through updates from the APs it manages.



Note: You can configure the Wireless traps only if the Wireless Trap Mode is enabled, which you configure on the LAN > Administration > SNMP Manager > Trap Flags page.

All Wireless SNMP traps are disabled by default. [Table 347](#) describes the events that generate SNMP traps. All traps are disabled by default.

The traps specified in [Table 347](#) below are generated only by the Cluster Controller unless otherwise specified.

Table 347: SNMP Traps

Field	Description
AP Failure Traps	If you enable this field, the SNMP agent sends a trap if an AP fails to associate or authenticate with the switch.
AP State Change Traps	If you enable this field, the SNMP agent sends a trap for one of the following reasons: <ul style="list-style-type: none"> • Managed AP Discovered • Managed AP Failed • Managed AP Unknown Protocol Discovered • Managed AP Load Balancing Utilization Exceeded
Client Failure Traps	If you enable this field, the SNMP agent sends a trap if a wireless client fails to associate or authenticate with an AP that is managed by the switch.
Client State Change Traps	If you enable this field, the SNMP agent sends a trap for one of the following reasons associated with the wireless client: <ul style="list-style-type: none"> • Client Association Detected • Client Disassociation Detected • Client Roam Detected
Peer Switch Traps	If you enable this field, the SNMP agent sends a trap for one of the following reasons associated with a peer switch <ul style="list-style-type: none"> • Peer Switch Discovered • Peer Switch Failed • Peer Switch Unknown Protocol Discovered • Configuration command received from peer switch. (The switch need not be Cluster Controller for generating this trap.)
RF Scan Traps	If you enable this field, the SNMP agent sends a trap when the RF scan detects a new AP, wireless client, or ad-hoc client.
Rogue AP Traps	If you enable this field, the SNMP agent sends a trap when the switch discovers a rogue AP. The agent also sends a trap every Rogue Detected Trap Interval seconds if any rogue AP continues to be present in the network.
TSPEC Traps	If you enable this field, the SNMP agent sends a trap when the following TSPEC-related events occur: <ul style="list-style-type: none"> • An authorized WMM client is repeatedly using more bandwidth than was allocated for its traffic stream. • A WMM-enabled client is sending prioritized traffic without authorization to use admission controlled resources.
WIDS Status Traps	If you enable this field, the SNMP agent sends a trap for one of the following reasons: <ul style="list-style-type: none"> • This switch has become Cluster Controller • Rogue Client detected • Rogue Client(s) continue to exist, after every Rogue Detected Trap Interval seconds • Maximum number of Managed APs in the peer group exceeded

Table 347: SNMP Traps (Cont.)

Field	Description
Wireless Status Traps	<p>If you enable this field, the SNMP agent sends a trap if the operational status of the DWS-4000 Series switch (it need not be Cluster Controller for this trap) changes. It sends a trap if the Channel Algorithm is complete or the Power Algorithm is complete. It also sends a trap if any of the following databases or lists has reached the maximum number of entries:</p> <ul style="list-style-type: none">• Managed AP database• AP Neighbor List• Client Neighbor List• AP Authentication Failure List• RF Scan AP List• Client Association Database• Ad Hoc Clients List• Detected Clients List

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.

Distributed Tunneling Configuration

The Distributed Tunneling mode, also known as AP-AP tunneling mode, is used to support L3 roaming for wireless clients without forwarding any data traffic to the wireless switch.

In the AP-AP tunneling mode, when a client first associates with an AP in the wireless system the AP forwards its data using the VLAN forwarding mode. The AP to which the client initially associates is the *Home AP*. The AP to which the client roams is the *Association AP*.

When a client roams to another AP in a different subnet the Association AP tunnels all traffic from the client to the Home AP using a CAPWAP L2 tunnel. The Home AP injects the traffic received over the tunnel into the wired network. If a client roams to another AP in the same subnet then the tunnel is not created, and the new AP becomes the Home AP for the client.

Distributed Tunneling Configuration	
Distributed Tunnel Clients	128 (1 to 8000)
Distributed Tunnel Idle Timeout	120 (30 to 3600)
Distributed Tunnel Timeout	7200 (30 to 86400)
Distributed Tunnel Max Multicast Replications Allowed	128 (1 to 1024)

Submit Refresh

Figure 382: Distributed Tunneling Configuration

Table 348 shows the fields on the Distributed Tunneling Configuration page.

Table 348: Distributed Tunneling Configuration

<i>Field</i>	<i>Description</i>
Distributed Tunnel Clients	Specify the maximum number of distributed tunneling clients that can roam away from the Home AP at the same time.
Distributed Tunnel Idle Timeout	Specify the number of seconds of no activity by the client before the tunnel to that client is terminated and the client is forced to change its IP address.
Distributed Tunnel Timeout	Specify the number of seconds before the tunnel to the roamed client is terminated and the client is forced to change its IP address.
Distributed Tunnel Max Multicast Replications Allowed	Specify the maximum number of tunnels to which a multicast frame is copied on the Home AP.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.

Device Location Configuration

The Device Location feature can help you physically locate APs and other WLAN devices in different buildings and on multiple floors of a building. You can configure the information manually or use the WLAN Visualization tool to place the managed APs on floor plans, and then import the Building Floor objects with their associated APs from the WLAN Visualization tool to the switch. The location computation is performed by the Cluster Controller switch. You can use the WLAN Visualization tool to trigger the location search and to display the computed probability map.

Use the **Device Location Configuration** page to configure settings for the Device Location feature.

Figure 383: Device Location Configuration

The following table shows the fields on the **Device Location Configuration** page.

Table 349: Device Location Configuration

<i>Field</i>	<i>Description</i>
Measurement System	Specify the units of measure to use for device location: <ul style="list-style-type: none"> Metric — Measures distances in meters English — Measures distances in feet
RF Scan Mode	Specify whether the switch computes the location of a device from RF-Scan reports for the device. When this mode is enabled the location is stored in the Device Triangulation table.
RF Scan Interval	Specify the number of seconds between the iterations of the triangulation table device location protocol.

Command Buttons

The page includes the following buttons:

- Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- Refresh**—Updates the page with the latest information.

Wireless Network List

The wireless network list shows all the wireless networks configured on the switch. The first 16 networks are created by default. You can modify the default networks, but you cannot delete them. You can add and configure up to 48 additional networks for a total of 64 wireless networks. Multiple networks can have the same SSID.

Table 350: Wireless Network List

Field	Description
ID	Shows an automatically generated unique identifier for the network. IDs up to 16 are assigned to the 16 networks created by default. The switch supports up to 64 networks.
SSID	Identifies the name of the network. The SSID is a hyperlink to the Wireless Network Configuration page for the network.
VLAN	Shows the VLAN ID the wireless network uses.
Hide SSID	Shows whether the network broadcasts the SSID. If enabled, the SSID for this network is not included in AP beacons. To change this setting, click Edit .
L3 Tunnel	Shows whether L3 Tunneling is enabled on the network. Note: When L3 tunneling is enabled, the VLAN ID configured above is not used. In fact, the switch puts the management VLAN ID, if any, on the tunneled packets destined to the AP.
Security	Shows the current security settings for the network.
Redirect	Shows whether HTTP redirect is enabled. The possible values for the field are as follows: <ul style="list-style-type: none"> • HTTP: HTTP Redirect is enabled • None: HTTP Redirect is disabled

Command Buttons

The page includes the following buttons:

- **Add** — Add a new network. Enter the SSID in the field below the Wireless Network List, and then click Add. The Wireless Network Configuration page for the new network appears.
- **Refresh**—Updates the page with the latest information.
- **Delete** — Delete a network. Select the check box next to the network ID, and then click **Delete**. You cannot delete networks 1–16.

Configuring Networks

For information about the fields available on the **Advanced > Networks** page, see [“Configuring the Default Network” on page 545](#).

AP Profiles

Access point configuration profiles are a useful feature for large wireless networks with APs that serve a variety of different users. You can create multiple AP profiles on the DWS-4000 Series switch to customize APs based on location, function, or other criteria. Profiles are like templates, and once you create an AP profile, you can apply that profile to any AP that the DWS-4000 Series switch manages.

For each AP profile, you can configure the following features:

- Profile settings (Name, Hardware Type ID, Wired Network Discovery VLAN ID)
- Radio settings
- SSID settings
- QoS configuration

[Figure 384](#) shows ten APs that are managed by a DWS-4000 Series switch in a campus network. Each building has multiple APs, and the users in one building have different network requirements than the users in other buildings. The administrator of this WLAN has created two AP profiles on the switch in addition to the default profile.

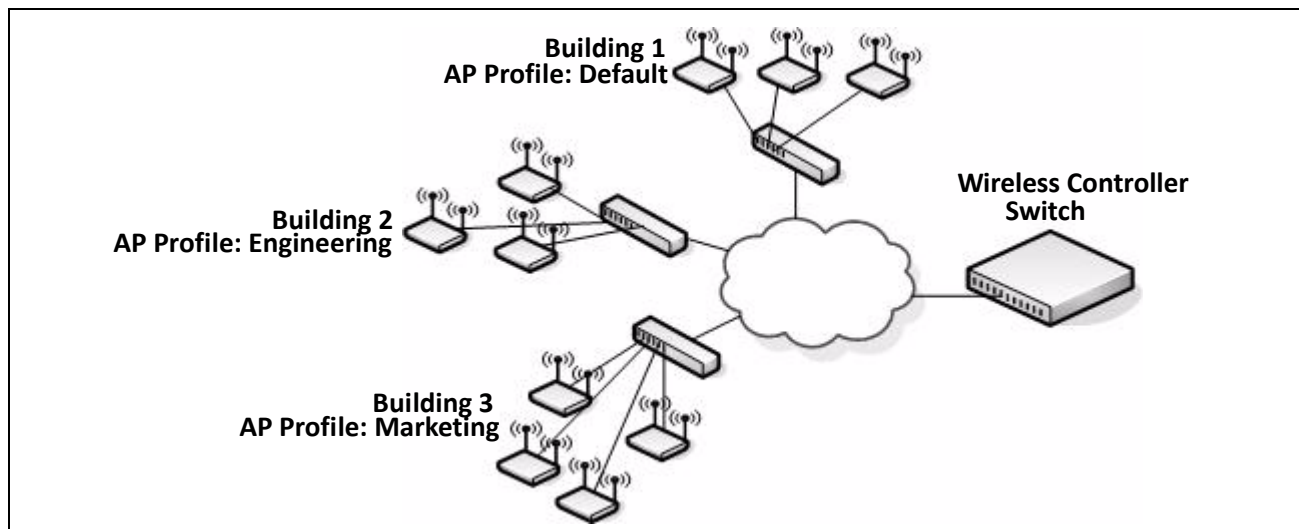


Figure 384: Multiple AP Profiles

Building 1 contains the main lobby and several conference rooms. The WLAN users in this location are primarily non-employees and guests. The APs in Building 1 use the default AP profile with no additional networks and no security.

Building 2 is the engineering building. The Building 2 APs use a profile called “Engineering.” The Engineering profile has three different VAPs that each have a unique SSID: Hardware, Software and Test.

Building 3 is the Sales and Marketing building. The Building 3 AP uses a profile called “Marketing.” The Marketing AP Profile has three VAPs. The SSIDs for the VAPs are: Sales, Marketing, and Program Management.

If the network administrator adds another AP to Building 2, she assigns the Engineering profile to the AP during the AP validation process.



Note: It is recommended that in a switch cluster, the profiles should be synchronized on all the switches in the cluster in order to get consistent information from the wireless system.

Creating, Copying, and Deleting AP Profiles

From the **WLAN > Administration > Advanced Configuration > AP Profile > Access Point Profile Summary** page, you can create, copy, or delete AP profiles. You can create up to 16 AP profiles on the DWS-4000 Series switch. To create a new profile, enter the name of the profile in the **Profile Name** field, and then click **Add**.

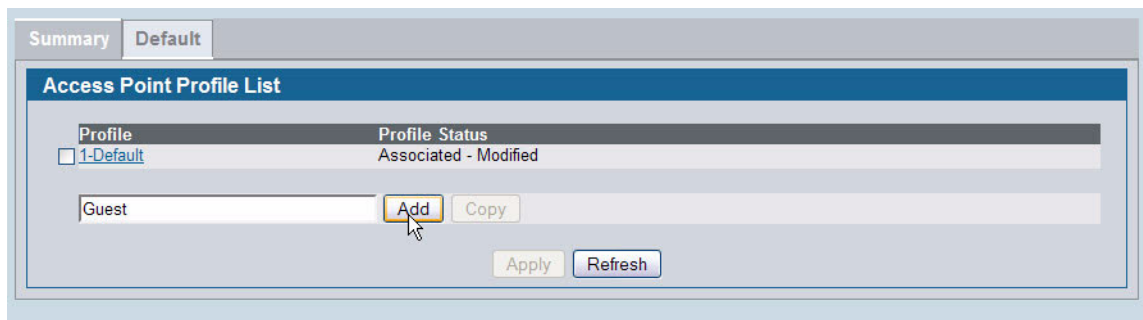


Figure 385: Adding a Profile

After you add the profile, the **Global Configuration** page for the profile appears, and a new tab with the name of the profile appears at the top of the page. When you add a new profile, it has the default AP settings.

[Figure 386](#) shows the layout for AP Profile configuration.

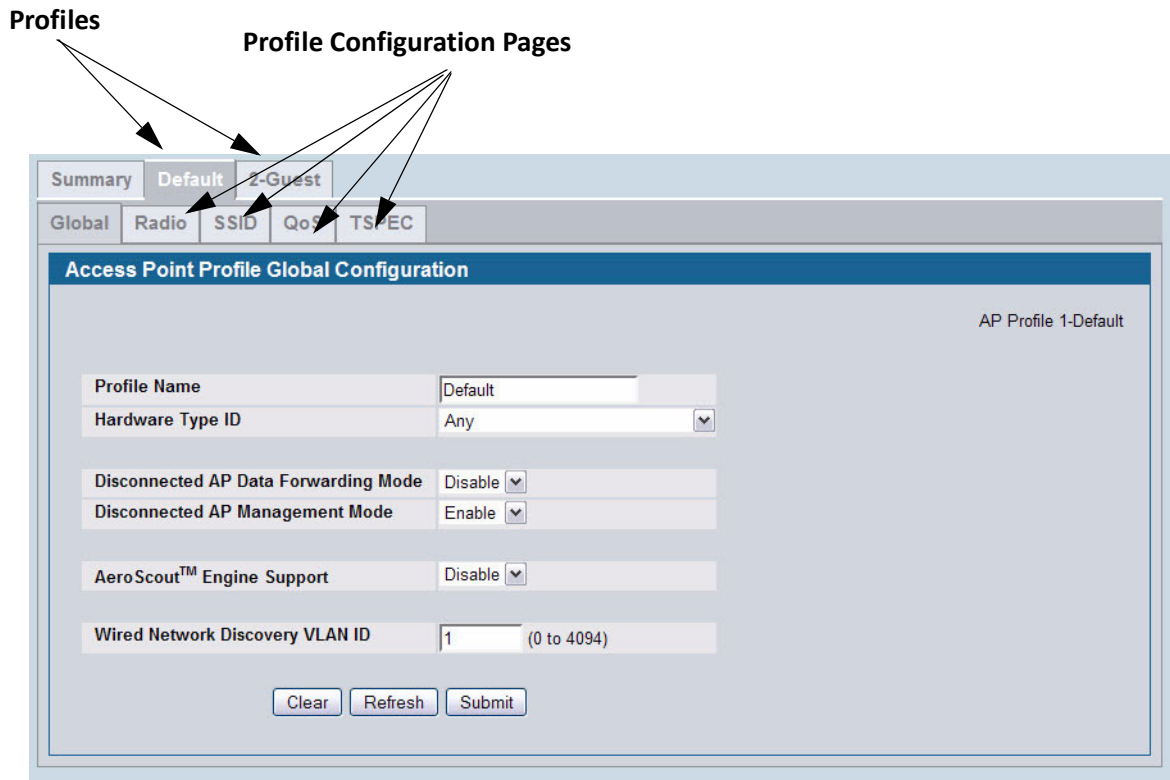


Figure 386: Configuring an AP Profile

Table 351: Access Point Profile Summary

Field	Description
Profile	Identifies the name of the configured profile.
Profile Status	<p>Indicates whether a profile is applied to one or more managed APs and shows the status for a request to re-apply the profile to its associated managed APs. The status is one of the following:</p> <ul style="list-style-type: none"> • Associated: The profile is configured, and one or more APs managed by the switch are associated with this profile. • Associated-Modified: The profile has been modified since it was applied to one or more associated APs; the profile must be re-applied for the changes to take effect. • Apply Requested: After you select a profile and click Apply, the screen refreshes and shows that an apply has been requested. • Apply In Progress: The profile is being applied to all APs that use this profile. During this process the APs reset, and all wireless clients are disassociated from the AP. • Configured: The profile is configured, but no APs managed by the switch currently use this profile.

Command Buttons

The page includes the following buttons:

- **Add**— Adds a profile with the name you enter in the associated field. The Access Point Profile Global Configuration page for the new profile appears after you click **Add**.
- **Copy**—Copies the selected profile and adds it with the name you enter in the associated field.
- **Delete**—Removes the selected profile. You can rename the default profile, but you cannot delete it.
- **Refresh**—Updates the page with the latest information.

Click the **Radio**, **SSID**, **QoS**, or **TSPEC** tabs to configure additional features for the profile.

To copy an existing profile and all of its configurations to a new profile, select the profile with the configuration to copy, enter a name for the new profile, and click **Copy**.

To delete a profile, select the profile and click **Delete**.

To access an existing profile, click the tab with the name of the profile. When you add a new profile, it has the default AP settings. When you copy a profile, it has the AP settings configured in the original profile.

To modify any settings within a profile, click the Global, Radio, Network or QoS settings for the profile you select and update the appropriate fields.

- For more information about the fields on the Global page, see [“Profile” on page 537](#).
- For more information about the fields on the Radio page, see [“Radio Configuration” on page 538](#).
- For more information about the fields on the Network page, see [“Wireless Default VAP Configuration” on page 543](#).
- For more information about the fields on the QoS page, see [“Access Point Profile QoS Configuration” on page 606](#).

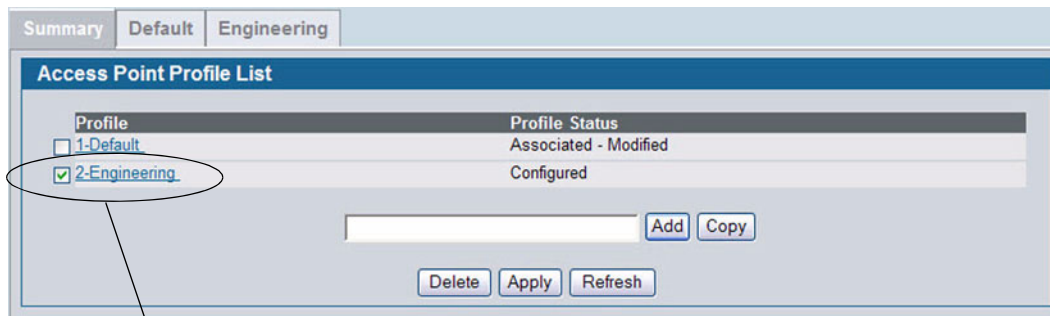
Applying an AP Profile

After you update an AP Profile on the DWS-4000 Series switch, the changes are not applied to the access points that use that profile until you explicitly apply the profile on the **WLAN> Administration > Advanced Configuration > AP Profile > Access Point Profile Summary** page or reset the APs that use the profile.



Note: When you change the VLAN ID for a wireless network, the AP might temporary lose its DHCP-assigned IP address when you apply the updated profile. If this occurs, the AP goes into Standalone mode. As soon as the AP regains its IP address from the DHCP server on your network, it resumes normal operation as a managed AP. You might also see this behavior when you enable or disable a VAP (SSID) and re-apply the AP profile.

To apply the profile changes to all access points that use a profile, select the profile and click **Apply**, as the following figure shows.



Selected Profile to Apply

Figure 387: Applying the AP Profile



Note: When you apply new AP Profile settings to an AP, the access point stops and restarts system processes. If this happens, wireless clients will temporarily lose connectivity. D-Link recommends that you change access point settings when WLAN traffic is low.

The Profile Status field can have one of the following values:

- **Associated:** The profile is configured, and one or more APs managed by the switch are associated with this profile.
- **Associated-Modified:** The profile has been modified since it was applied to one or more associated APs; the profile must be re-applied for the changes to take effect.
- **Apply Requested:** After you select a profile and click **Apply**, the screen refreshes and shows that an apply has been requested.
- **Apply In Progress:** The profile is being applied to all APs that use this profile. During this process the APs reset, and all wireless clients are disassociated from the AP.
- **Configured:** The profile is configured, but no APs managed by the switch currently use this profile.



Note: You associate a profile with an AP in the Valid AP database.

Configuring the AP Profile Global Settings

From the **WLAN > Administration > Advanced Configuration > AP Profile > Access Point Profile Summary** page, you can create, copy, or delete AP profiles. You can create up to 16 AP profiles on the DWS-4000 Series switch. To create a new profile, enter the name of the profile in the **Profile Name** field, and then click **Add**.

The screenshot shows the 'Access Point Profile Global Configuration' page for 'AP Profile 1-Default'. The page has tabs for 'Summary', 'Default', and '2-Guest'. Under the 'Default' tab, there are sub-tabs for 'Global', 'Radio', 'SSID', 'QoS', and 'TSPEC'. The 'Global' sub-tab is active, showing the following configuration fields:

- Profile Name:** Default
- Hardware Type ID:** Any
- Disconnected AP Data Forwarding Mode:** Disable
- Disconnected AP Management Mode:** Enable
- AeroScout™ Engine Support:** Disable
- Wired Network Discovery VLAN ID:** 1 (0 to 4094)

At the bottom of the form are three buttons: 'Clear', 'Refresh', and 'Submit'.

Figure 388: AP Profile Global Configuration

Use the **Access Point Profile Global Configuration** page to configure a variety of global settings for a new or existing AP profile. When you add a new profile, this page automatically appears and is populated with the default AP settings.

Table 352: Access Point Profile Global Configuration

Field	Description
Profile Name	The Access Point profile name you added. Use 0 to 32 characters. Only alphanumeric characters are allowed. No special characters are allowed.
Hardware Type ID	Select the hardware type for the APs that use this profile. The hardware type is determined, in part, by the number of radios the AP supports (single or dual) and the IEEE 802.11 modes that the radio supports (a/b/g or a/b/g/n). The available options are: <ul style="list-style-type: none"> Any DWL-X600AP Dual Radio a/b/g/n DWL-3600AP Single Radio b/g/n DWL-6600AP Dual Radio a/b/g/n
Disconnected AP Data Forwarding Mode	Specify whether the managed AP should allow clients that are already associated to continue forwarding traffic when the AP loses connection with the Wireless Switch. If the field is disabled, the AP will not allow clients to forward data if the AP loses its connection with the switch that is managing it.

Table 352: Access Point Profile Global Configuration

Field	Description
Disconnected AP Management Mode	Specify whether the managed AP should enable stand-alone management functionality when it loses connection with the wireless switch. If this field is disabled, the AP will not allow CLI, web, or SNMP access to the stand-alone management interface.
AeroScout™ Engine Support	AeroScout Engine support provides location-based services for wireless networks. Specify whether to enable support for the AeroScout protocol. For more information about the AeroScout protocol, see “Enabling AeroScout™ Engine Support” on page 626 .
Wired Network Discovery VLAN ID	Enter the VLAN ID that the switch uses to send tracer packets in order to detect APs connected to the wired network. The tracer packets help the switch identify unauthorized APs that do not belong to the Unified Wired and Wireless Access System but are connected to the wired network.

Command Buttons

The page includes the following buttons:

- **Clear**—Resets the profile configuration settings to the default values. The Profile Name is not cleared.
- **Delete**—Deletes the profile. This button is not available on the configuration page for the Default profile. You can rename the Default profile, but you cannot delete it.
- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).

Access Point Profile Radio Configuration

To accommodate a broad range of wireless clients and wireless network requirements, the AP can support up to two radios. By default, Radio 1 operates in the IEEE 802.11b/g/n mode, and Radio 2 operates in the IEEE 802.11a/n mode. The difference between these modes is the frequency in which they operate. IEEE 802.11b/g/n operates in the 2.4 GHz frequency, and IEEE 802.11a/n operates in the 5 GHz frequency of the radio spectrum.



Note: The DWL-3600AP is a single-radio AP. Only the settings you configure for Radio 2 (802.11b/g/n) are applied to the DWL-3600AP.

The **Access Point Profile Radio Configuration** page contains several fields that are not available on the **Basic Setup > Radio** page for the default AP Profile.

Summary
Default

Global
Radio
SSID
QoS
TSPEC

Access Point Profile Radio Configuration
AP Profile 1-Default

1-802.11a/n 2-802.11b/g/n

State	<input checked="" type="radio"/> On <input type="radio"/> Off	Mode	IEEE 802.11a/n ▾
RTS Threshold (bytes)	2347 (0 to 2347)	DTIM Period (# beacons)	10 (1 to 255)
Load Balancing	<input type="checkbox"/>	Beacon Interval (msecs)	100 (20 to 2000)
Load Utilization (%)	60 (1 to 100)	Automatic Channel	<input checked="" type="checkbox"/>
Maximum Clients	200 (0 to 200)	Automatic Power	<input checked="" type="checkbox"/>
RF Scan Other Channels	<input checked="" type="checkbox"/>	Initial Power (%)	100 (1 to 100)
RF Scan Sentry	<input type="checkbox"/>	APSD Mode	Disable ▾
RF Scan Interval (secs)	60 (30 to 120)	Frag Threshold (bytes)	2346 (256 to 2346)
RF Scan Sentry Channels	<input checked="" type="checkbox"/> 802.11a <input checked="" type="checkbox"/> 802.11b/g	Short Retries	7
RF Scan Duration (msecs)	10 (10 to 2000)	Long Retries	4
Rate Limiting	<input type="checkbox"/>	Transmit Lifetime (msecs)	512
Rate Limit (pkts/sec)	50 (1 to 50)	Receive Lifetime (msecs)	512
Rate Limit Burst (pkts/sec)	75 (1 to 75)	Station Isolation	<input type="checkbox"/>
Channel Bandwidth	40 MHz ▾	Primary Channel	Lower ▾
Protection	Auto ▾	Short Guard Interval	Enable ▾
Space Time Block Code	Enable ▾	Radio Resource Management	Enable ▾
No ACK	Disable ▾	Multicast Tx Rate (Mbps)	Auto ▾
Supported Channels	36 44 149 157		
Auto Eligible	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		
Available MCS Indices	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15		
	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		
Rate Sets (Mbps)	6 9 12 18 24 36 48 54		
Basic	<input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		
Supported	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		

Figure 389: AP Profile Radio Settings

To change the settings for a radio, you must first select the radio you want to configure (1 or 2). After you change the settings, click **Submit** to apply the settings. Changes to the settings apply only to the selected radio.

Table 353: Radio Settings

Field	Description
1-802.11a/n 2-802.11b/g/n	<p>From this field, you can select the radio that you want to configure. By default, Radio 1 operates in IEEE 802.11b/g/n mode, and Radio 2 operates in IEEE 802.11a/n mode. If you change the mode, the labels for the radios change accordingly. Changes to the settings apply only to the selected radio.</p> <p>The DWL-3600AP is a single-radio AP. Any settings you configure for Radio 1 (802.11a/n) are not applied to the DWL-3600AP. If the selected Hardware Type ID for the AP profile is DWL-3600AP, the radio selectors are not available.</p>
State	<p>Specify whether you want the radio on or off by clicking On or Off.</p> <p>If you turn off a radio, the AP sends disassociation frames to all the wireless clients it is currently supporting so that the radio can be gracefully shutdown and the clients can start the association process with other available APs.</p>
Mode	<p>The Mode defines the Physical Layer (PHY) standard the radio uses.</p> <p>Select one of the following modes for each radio interface:</p> <ul style="list-style-type: none"> • IEEE 802.11a is a PHY standard that specifies operating in the 5 GHz U-NII band using orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 6 to 54 Mbps. • IEEE 802.11b/g operates in the 2.4 GHz ISM band. IEEE 802.11b is an enhancement of the initial 802.11 PHY to include 5.5 Mbps and 11 Mbps data rates. It uses direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) as well as complementary code keying (CCK) to provide the higher data rates. It supports data rates ranging from 1 to 11 Mbps. IEEE 802.11g is a higher speed extension (up to 54 Mbps) to the 802.11b PHY. It uses orthogonal frequency division multiplexing (OFDM). It supports data rates ranging from 1 to 54 Mbps. • IEEE 802.11a/n operates in the 5 GHz ISM band and includes support for both 802.11a and 802.11n devices. IEEE 802.11n is an extension of the 802.11 standard that includes multiple-input multiple-output (MIMO) technology. IEEE 802.11n supports data ranges of up to 248 Mbps and nearly twice the indoor range of 802.11 b, 802.11g, and 802.11a. • IEEE 802.11b/g/n operates in the 2.4 GHz ISM band and includes support for 802.11b, 802.11g, and 802.11n devices. • 5 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 5 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a). • 2.4 GHz IEEE 802.11n is the recommended mode for networks with 802.11n devices that operate in the 2.4 GHz frequency that do not need to support 802.11a or 802.11b/g devices. IEEE 802.11n can achieve a higher throughput when it does not need to be compatible with legacy devices (802.11b/g or 802.11a).

Table 353: Radio Settings (Cont.)

Field	Description
RTS Threshold	<p>Specify a Request to Send (RTS) Threshold value between 0 and 2347.</p> <p>The RTS threshold indicates the number of octets in an MPDU, below which an RTS/CTS handshake is not performed.</p> <p>Changing the RTS threshold can help control traffic flow through the AP, especially one with a lot of clients. If you specify a low threshold value, RTS packets will be sent more frequently. This will consume more bandwidth and reduce the throughput of the packet. On the other hand, sending more RTS packets can help the network recover from interference or collisions which might occur on a busy network, or on a network experiencing electromagnetic interference.</p>
Load Balancing	If you enable load balancing, you can control the amount of traffic that is allowed on the AP.
Load Utilization	This field allows you to set a threshold for the percentage of network bandwidth utilization allowed on the radio. Once the level you specify is reached, the AP stops accepting new client associations. Enter a percentage of utilization from 1 to 100.
Maximum Clients	<p>Specify the maximum number of stations allowed to associate with this access point at any one time.</p> <p>You can enter a value between 0 and 200.</p>
RF Scan Other Channels	<p>The access point can perform RF scans to collect information about other wireless devices within range and then report this information to the DWS-4000 Series switch.</p> <p>If you select the Scan Other Channels option, the radio periodically moves away from the operational channel to scan other channels.</p> <p>Enabling this mode causes the radio to interrupt user traffic, which may be noticeable with voice connections.</p> <p>When the Scan Other Channels option is cleared, the AP scans only the operating channel.</p>
RF Scan Sentry	<p>Select this option to allow the radio to operate in sentry mode.</p> <p>When the RF Scan Sentry option is selected, the radio primarily performs dedicated RF scanning. The radio passively listens for beacons and traffic exchange between clients and other access points but does not accept connections from wireless clients. In sentry mode, all VAPs are disabled. Networks that deploy sentry APs or radios can detect devices on the network quicker and perform more thorough security analysis. In this mode, the radio switches from one channel to the next. The length of time spent on each channel is controlled by the scan duration. The default scan duration is 10 milliseconds.</p>
RF Scan Interval	This field controls the length of time between channel changes during the RF Scan.
RF Scan Sentry Channels	<p>The radio can scan channels in the radio frequency used by the 802.11b/g band (2.4 GHz), the 802.11a band (5 GHz), or both bands. Select the channel band for the radio to scan.</p> <p>Note: The band selection applies only to radios in sentry mode and is dependent upon the capabilities of the radio.</p>
RF Scan Duration	This field controls the amount of time the radio spends scanning the other channel (in milliseconds) during an RF scan.

Table 353: Radio Settings (Cont.)

Field	Description
Rate Limiting	<p>Enabling multicast and broadcast rate limiting can improve overall network performance by limiting the number of packets transmitted across the network. This feature is disabled by default.</p> <p>Note: The available rate limit values are very low for most environments, so enabling this feature is not recommended.</p> <ul style="list-style-type: none"> • To enable Multicast and Broadcast Rate Limiting, click Enabled. • To disable Multicast and Broadcast Rate Disabled, click Disabled.
Rate Limit	<p>Enter the rate limit you want to set for multicast and broadcast traffic. The limit should be greater than 1, but less than 50 packets per second. Any traffic that falls below this rate limit will always conform to and be transmitted to the appropriate destination.</p> <p>The default and maximum rate limit setting is 50 packets per second. This field is disabled if Rate Limiting is disabled.</p>
Rate Limit Burst	<p>Setting a rate limit burst determines how much traffic bursts can be before all traffic exceeds the rate limit. This burst limit allows intermittent bursts of traffic on a network above the set rate limit.</p> <p>The default and maximum rate limit burst setting is 75 packets per second. This field is disabled if Rate Limiting is disabled.</p>
Channel Bandwidth	<p>The 802.11n specification allows the use of a 40-MHz-wide channel in addition to the legacy 20-MHz channel available with other modes. The 40-MHz channel enables higher data rates but leaves fewer channels available for use by other 2.4 GHz and 5 GHz devices. The 40-MHz option is enabled by default for 802.11a/n modes and 20 MHz for 802.11b/g/n modes. You can use this setting to restrict the use of the channel bandwidth to a 20-MHz channel.</p>
Protection	<p>The protection feature contains rules to guarantee that 802.11 transmissions do not cause interference with legacy stations or applications. By default, these protection mechanisms are enabled (Auto). With protection enabled, protection mechanisms will be invoked if legacy devices are within range of the AP.</p> <p>You can disable (Off) these protection mechanisms; however, when 802.11n protection is off, legacy clients or APs within range can be affected by 802.11n transmissions. 802.11 protection is also available when the mode is 802.11b/g. When protection is enabled in this mode, it protects 802.11b clients and APs from 802.11g transmissions.</p>
Space Time Block Code	<p>Space Time Block Coding (STBC) is an 802.11n technique intended to improve the reliability of data transmissions. The data stream is transmitted on multiple antennas so the receiving system has a better chance of detecting at least one of the data streams.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> • Enable — The AP transmits the same data stream on multiple antennas at the same time. • Disable — The AP does not transmits the same data on multiple antennas.
No ACK	<p>Select Enable to specify that the AP should not acknowledge frames with QoSNoAck as the service class value.</p>

Table 353: Radio Settings (Cont.)

Field	Description
DTIM Period	<p>The Delivery Traffic Information Map (DTIM) message is an element included in some Beacon frames. It indicates which client stations, currently sleeping in low-power mode, have data buffered on the access point awaiting pick-up.</p> <p>The DTIM period you specify indicates how often the clients served by this access point should check for buffered data still on the AP awaiting pickup.</p> <p>Specify a DTIM period within the given range (1–255).</p> <p>The measurement is in beacons. For example, if you set this field to 1, clients will check for buffered data on the AP at every beacon. If you set this field to 10, clients will check on every 10th beacon.</p>
Beacon Interval	<p>Beacon frames are transmitted by an access point at regular intervals to announce the existence of the wireless network. The default behavior is to send a beacon frame once every 100 milliseconds (or 10 per second).</p> <p>The Beacon Interval value is set in milliseconds. Enter a value from 20 to 2000.</p>
Automatic Channel	<p>The channel defines the portion of the radio spectrum that the radio uses for transmitting and receiving. The range of channels and the default channel are determined by the Mode of the radio interface.</p> <p>When the AP boots, the AP scans the RF area for occupied channels and selects a channel from the available non-interfering or clear channels. However, channel conditions can change during operation.</p> <p>Enabling the Automatic Channel makes APs assigned to this profile eligible for auto-channel selection. You can automatically or manually run the auto-channel selection algorithm to allow the DWS-4000 Series switch to adjust the channel on APs as WLAN conditions change.</p> <p>By default, the global auto-channel mode is set to manual. To enable the automatic channel selection mode, go to the AP Management > RF Management page and select Fixed or Interval for the Channel Plan mode. You can also run the automatic channel selection algorithm manually from the Manual Channel Plan page.</p> <p>Note: If you assign a static channel to an AP in the Valid AP database or on the Advanced AP Management page, the AP will not participate in the auto-channel selection.</p>
Automatic Power	<p>The power level affects how far an AP broadcasts its RF signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range.</p> <p>Automatic power uses a proprietary algorithm to automatically adjust the RF signal to broadcast far enough to reach wireless clients, but not so far that it interferes with RF signals broadcast by other APs. The power level algorithm increases or decreases the power level in 10% increments based on presence or absence of packet retransmission errors.</p>
Default Power	<p>The automatic power algorithm will not reduce the power below the number you set in the default power field. By default, the power level is 100%. Therefore, even if you enable the automatic power, the power of the RF signal will not decrease.</p> <p>The power level is a percentage of the maximum transmission power for the RF signal.</p>
APSD Mode	<p>Select Enable to enable Automatic Power Save Delivery (APSD), which is a power management method. APSD is recommended if VoIP phones access the network through the AP.</p>

Table 353: Radio Settings (Cont.)

Field	Description
Frag Threshold	The fragmentation threshold limits the size of packets transmitted over the network. Acceptable values are <i>even</i> numbers from 256-2345. Packets that are under the configured size are not fragmented. A value of 2346 means that packets are not fragmented.
Short Retries	The value in this field indicates the maximum number of transmission attempts on frame sizes less than or equal to the RTS Threshold. The range is 1-255.
Long Retries	The value in this field indicates the maximum number of transmission attempts on frame sizes greater than the RTS Threshold. The range is 1-255.
Transmit Lifetime	Shows the number of milliseconds to wait before terminating attempts to transmit the MSDU after the initial transmission.
Receive Lifetime	Shows the number of milliseconds to wait before terminating attempts to reassemble the MMPDU or MSDU after the initial reception of a fragmented MMPDU or MSDU.
Station Isolation	When this option is selected, the AP blocks communication between wireless clients. It still allows data traffic between its wireless clients and wired devices on the network, but not among wireless clients. This feature is disabled by default. <ul style="list-style-type: none"> To enable Multicast and Broadcast Rate Limiting, click Enabled. To disable Multicast and Broadcast Rate Disabled, click Disabled.
Primary Channel	This setting is editable only when a channel is selected and the channel bandwidth is set to 40 MHz. A 40-MHz channel can be considered to consist of two 20-MHz channels that are contiguous in the frequency domain. These two 20-MHz channels are often referred to as the Primary and Secondary channels. The Primary Channel is used for 802.11n clients that support only a 20-MHz channel bandwidth and for legacy clients. Use this setting to set the Primary Channel as the upper or lower 20-MHz channel in the 40-MHz band.
Short Guard Interval	The guard interval is the dead time, in nanoseconds, between OFDM symbols. The guard interval prevents Inter-Symbol and Inter-Carrier Interference (ISI, ICI). The 802.11n mode allows for a reduction in this guard interval from the a and g definition of 800 nanoseconds to 400 nanoseconds. Reducing the guard interval can yield a 10% improvement in data throughput. Select one of the following options: <ul style="list-style-type: none"> Enable — The AP transmits data using a 400 ns guard Interval when communicating with clients that also support the 400 ns guard interval. Disable — The AP transmits data using an 800 ns guard interval.
Radio Resource Management	Radio Resource Measurement (RRM) mode requires the Wireless System to send additional information in beacons, probe responses, and association responses. Enable or disable the support for radio resource measurement feature in the AP profile. The feature is set independently for each radio and is enabled by default.
Multicast Tx Rate (Mbps)	Select the 802.11 rate at which the radio transmits multicast frames. The rate is in Mbps. The lowest rate in the 5 GHz band is 6 Mbps.
Supported Channels	This field displays the channels that are supported for the radio mode currently selected on the page and for the country configured on the Global Wireless Settings page.
Auto Eligible	Select the Auto Eligible option beneath each channel to include the channel in the automatic channel assignment process.

Table 353: Radio Settings (Cont.)

Field	Description
Available MCS Indices	This field shows the Modulation and Coding Scheme (MCS) index values supported by the radio. Each index can be enabled and disabled independently.
Rate Sets	Select the transmission rate sets you want the access point to support and the basic rate sets you want the access point to advertise. Rates are expressed in megabits per second.
Basic	These numbers indicate the data rates that all stations associating with the AP must support.
Supported	These numbers indicate rates that the access point supports. You can select multiple rates. The AP automatically chooses the most efficient rate based on factors like error rates and distance of client stations from the AP.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Clear**—Resets the settings on the page to the default values.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).

Access Point Profile VAP Configuration

The **Access Point Profile VAP Configuration** page displays the virtual access point (VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier (SSID). You can configure and enable up to 16 VAPs per radio on each physical access point.

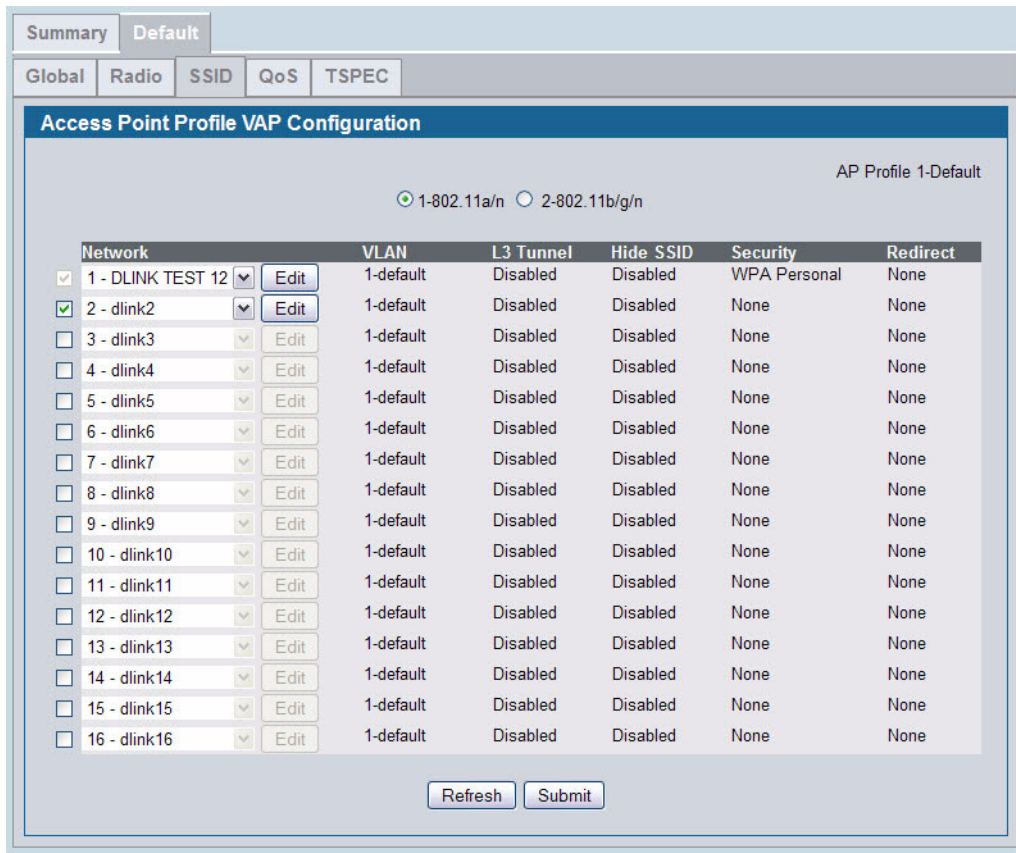


Figure 390: AP Profile VAP Configuration

The following table describes the fields on the **Access Point Profile VAP Configuration** page.

Table 354: Default VAP Configuration

Field	Description
1-802.11a/n	From this field, you can select the radio with the settings to configure. Settings for each radio are configured separately.
2-802.11b/g/n	
	By default, Radio 1 operates in IEEE 802.11a/n mode, and Radio 2 operates in IEEE 802.11b/g/n mode. If you change the mode, the labels for the radios change accordingly. Changes to the settings apply only to the selected radio.
	The DWL-3600AP is a single-radio AP. Any settings you configure for Radio 1 (802.11a/n) are not applied to the DWL-3600AP. If the selected Hardware Type ID for the AP profile is DWL-3600AP, the radio selectors are not available.

Table 354: Default VAP Configuration (Cont.)

Field	Description
Network	<p>Use the option to the left of the network to enable or disable the corresponding VAP on the selected radio.</p> <p>When enabled, use the menu to select a networks to assign to the VAP. You can configure up to 64 separate networks on the switch and apply them across multiple radio and VAP interfaces. By default, 16 networks are pre-configured and applied in order to the VAPs on each radio.</p> <p>Enabling a VAP on one radio does not automatically enable it on the other radio.</p> <p>Note: You cannot disable the default VAP, VAP0.</p> <p>To configure additional networks, click Advanced Configuration > Networks.</p>
Edit	<p>Click Edit to modify settings for the corresponding network.</p> <p>When you click Edit, the Wireless Network Configuration page appears.</p>
VLAN	Shows the VLAN ID of the VAP. To change this setting, click Edit .
L3 Tunnel	<p>Shows whether L3 Tunneling is enabled on the network.</p> <p>Note: When L3 tunneling is enabled, the VLAN ID configured above is not used. In fact, the switch puts the management VLAN ID, if any, on the tunneled packets destined to the AP.</p>
Hide SSID	Shows whether the VAP broadcasts the SSID. If enabled, the SSID for this network is not included in AP beacons. To change this setting, click Edit .
Security	Shows the current security settings for the VAP. To change this setting, click Edit .
Redirect	<p>Shows whether HTTP redirect is enabled. The possible values for the field are as follows:</p> <ul style="list-style-type: none"> • HTTP: HTTP Redirect is enabled • None: HTTP Redirect is disabled

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).

Access Point Profile QoS Configuration

Quality of Service (QoS) provides you with the ability to specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic like Voice-over-IP (VoIP), other types of audio, video, and streaming media as well as traditional IP data over the D-Link Unified Switch.

To display the QoS Configuration page for an AP profile, click **WLAN > Advanced Configuration > AP Profiles**, select the tab corresponding to the profile, and click the **QoS** tab. Click the radio button corresponding to the radio interface you want to configure (QoS is configured per radio interface).

Summary Default

Global Radio SSID QoS TSPEC

Access Point Profile QoS Configuration

AP Profile 1-Default

1-802.11a/n 2-802.11b/g/n

Template: Custom

AP EDCA Parameters				
Queue	AIFS (msecs)	cwMin (msecs)	cwMax (msecs)	Max. Burst (usecs)
Data 0 (Voice)	1	3	7	1500
Data 1 (Video)	1	7	15	3000
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

WMM Mode

Station EDCA Parameters				
Queue	AIFS (msecs)	cwMin (msecs)	cwMax (msecs)	TXOP Limit (32 usec units)
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

Refresh Submit

Figure 391: QoS Configuration

Configuring Quality of Service (QoS) on the D-Link Unified Switch consists of setting parameters on existing queues for different types of wireless traffic, and effectively specifying minimum and maximum wait times (through Contention Windows) for transmission. The settings described here apply to data transmission behavior on the access point only, not to that of the client stations.

AP Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the access point to the client station. Station Enhanced Distributed Channel Access (EDCA) Parameters affect traffic flowing from the client station to the access point.

You can specify custom QoS settings, or you can select a template that configures the AP profile with pre-defined settings that are optimized for data traffic or voice traffic.

Table 355 describes the QoS settings you can configure.

Table 355: QoS Settings

Field	Description
1-802.11a/n 2-802.11b/g/n	<p>From this field, you can select the radio for which you want to configure QoS settings. Settings for each radio are configured separately.</p> <p>By default, Radio 1 operates in IEEE 802.11a/n mode, and Radio 2 operates in IEEE 802.11b/g/n mode. If you change the mode, the labels for the radios change accordingly. Changes to the settings apply only to the selected radio.</p> <p>The DWL-3600AP is a single-radio AP. Any settings you configure for Radio 1 (802.11a/n) are not applied to the DWL-3600AP. If the selected Hardware Type ID for the AP profile is DWL-3600AP, the radio selectors are not available.</p>
Template	Select the QoS template to apply to the AP profile. If you select Custom, you can change the AP and station parameters. If you select Voice or Factory Defaults, the switch will use the pre-defined settings for the template you select.
AP EDCA Parameters	
Queue	<p>Queues are defined for different types of data transmitted from AP-to-station:</p> <ul style="list-style-type: none"> • Data 0 (Voice)—High priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. • Data 1 (Video)—High priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. • Data 2 (best effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. • Data 3 (Background)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Inter-Frame Space)	The Arbitration Inter-Frame Spacing (AIFS) specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255.
cwMin (Minimum Contention Window)	<p>This parameter is input to the algorithm that determines the initial random backoff wait time (window) for retry of a transmission.</p> <p>The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.</p> <p>The first random number generated will be a number between 0 and the number specified here.</p> <p>If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window.</p> <p>Valid values for the cwmin are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwmin must be lower than the value for cwmax.</p>

Table 355: QoS Settings (Cont.)

Field	Description
cwMax (Maximum Contention Window)	<p>The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.</p> <p>Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached.</p> <p>Valid values for the cwmax are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for cwmax must be higher than the value for cwmin.</p>
Max. Burst Length	<p>AP EDCA Parameter Only (The Max. Burst Length applies only to traffic flowing from the access point to the client station.)</p> <p>This value specifies (in milliseconds) the Maximum Burst Length allowed for packet bursts on the wireless network. A <i>packet burst</i> is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance.</p> <p>Valid values for maximum burst length are 0.0 through 999.</p>
General Parameters	
WMM Mode	<p>Wi-Fi MultiMedia (WMM) is enabled by default. With WMM enabled, QoS prioritization and coordination of wireless medium access is on. With WMM enabled, QoS settings on the D-Link Unified Switch control <i>downstream</i> traffic flowing from the access point to client station (AP EDCA parameters) and the <i>upstream</i> traffic flowing from the station to the access point (station EDCA parameters).</p> <p>Disabling WMM deactivates QoS control of station EDCA parameters on <i>upstream</i> traffic flowing from the station to the access point</p> <p>With WMM disabled, you can still set some parameters on the downstream traffic flowing from the access point to the client station (AP EDCA parameters). To disable WMM extensions, click Disabled.</p> <p>To enable WMM extensions, click Enabled.</p>
Station EDCA Parameters	
Queue	<p>Queues are defined for different types of data transmitted from station-to-AP:</p> <ul style="list-style-type: none"> • Data 0 (Voice)—Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue. • Data 1 (Video)—Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue. • Data 2 (best effort)—Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue. • Data 3 (Background)—Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AIFS (Inter-Frame Space)	<p>The Arbitration Inter-Frame Spacing (AIFS) specifies a wait time for data frames. The wait time is measured in slots. Valid values for AIFS are 1 through 255.</p>

Table 355: QoS Settings (Cont.)

Field	Description
cwMin (Minimum Contention Window)	<p>This parameter is used by the algorithm that determines the initial random backoff wait time (window) for data transmission during a period of contention for</p> <p>The value specified in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.</p> <p>The first random number generated will be a number between 0 and the number specified here.</p> <p>If the first random backoff wait time expires before the data frame is sent, a retry counter is incremented and the random backoff value (window) is doubled. Doubling will continue until the size of the random backoff value reaches the number defined in the Maximum Contention Window.</p>
cwMax (Maximum Contention Window)	<p>The value specified in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached.</p> <p>Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached.</p>
TXOP Limit	<p>Station EDCA Parameter Only (The TXOP Limit applies only to traffic flowing from the client station to the access point.)</p> <p>The Transmission Opportunity (TXOP) is an interval of time when a WME client station has the right to initiate transmissions onto the wireless medium (WM).</p> <p>This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for client stations; that is, the interval of time when a WMM client station has the right to initiate transmissions on the wireless network.</p>

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.

Access Point Profile TSPEC Configuration

From the **Access Point Profile TSPEC Configuration** page, you can configure traffic specification (TSPEC) settings for the access points that use this profile.

TSPEC incorporates QoS features into the wireless network to help wireless clients make sure time- and delay-sensitive network traffic, such as video and voice, have priority over other type of traffic. Examples of wireless clients that might use this feature include a Wi-Fi Certified telephone handset that marks its codec-generated data packets as voice priority traffic, or a video player application on a wireless laptop that prioritizes a video conference feed from a corporate server.

Configure the settings on the **Access Point Profile TSPEC Configuration** page to determine how an AP handles the TSPEC sent from a QoS-capable wireless client.



Caution! If you change any of the settings on the TSPEC Configuration page, the AP radios will restart when this profile is applied.

Figure 392: AP Profile TSPEC Configuration

The following table describes the fields on the **Access Point Profile TSPEC Configuration** page.

Table 356: TSPEC Configuration

Field	Description
Radio 1 Radio 2	You configure the TSPEC settings for Radio 1 and Radio 2 separately. Use the radio button to select the desired radio.
TSPEC Mode	Enable or disable TSPEC operation on this radio.
Voice ACM Mode	Regulates mandatory admission control (ACM) for the voice access category. The options are: <ul style="list-style-type: none"> • Enabled—A station is required to send a TSPEC request for bandwidth to the AP before sending or receiving a voice traffic stream. The AP responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted. • Disabled—A station can send and receive voice priority traffic without requiring an admitted TSPEC; the AP ignores voice TSPEC requests from client stations.

Table 356: TSPEC Configuration (Cont.)

Field	Description
Video ACM Mode	Regulates mandatory admission control for the video access category. The options are: <ul style="list-style-type: none"> • Enabled—A station is required to send a TSPEC request for bandwidth to the AP before sending or receiving a video traffic stream. The AP responds with the result of the request, which includes the allotted medium time if the TSPEC was admitted. • Disabled—A station can send and receive video priority traffic without requiring an admitted TSPEC; the AP ignores video TSPEC requests from client stations.
Voice ACM Limit	Defines the maximum portion of bandwidth utilization to admit for the voice access category. TSPEC requests that would cause this limit to be exceeded are rejected.
Video ACM Limit	Defines the maximum portion of bandwidth utilization to admit for the video access category. TSPEC requests that would cause this limit to be exceeded are rejected.
Roam Reserve Limit	Defines the portion of bandwidth in the Voice ACM Limit and Video ACM Limit parameters to hold in reserve for roaming clients only. If this value exceeds the Voice ACM limit or Video ACM limit, respectively, then that entire ACM limit is used exclusively for roaming clients. Setting this value to 0% causes none of the voice or video ACM limit values to be reserved for roaming clients; they compete equally with non-roaming clients for wireless network bandwidth.
AP Inactivity Timeout	Specifies the amount of time that an active traffic stream from the AP to the wireless client (downlink) may be idle before it is deleted by the AP. If set to 0, this timeout is disabled, and a downlink or bidirectional traffic stream will not time out.
STA Inactivity Timeout	The amount of time that an active traffic stream from the wireless client to the AP may be idle before it is deleted by the AP. If set to 0, this timeout is disabled, and an uplink or bidirectional traffic stream will not time out.
Legacy WMM Queue Map Mode	When enabled, the AP allows intermixing of non-WMM legacy traffic with WMM traffic on access category queues that are operating according to ACM rules.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).

Peer Switch

The Peer Switch Configuration feature allows you to send a variety of configuration information from one switch to all other switches. In addition to keeping the switches synchronized, this function allows you to manage all wireless switches in the cluster from one switch. The **Peer Switch Configuration Request Status** page provides information about the status of the configuration upgrade on the switches in the cluster.

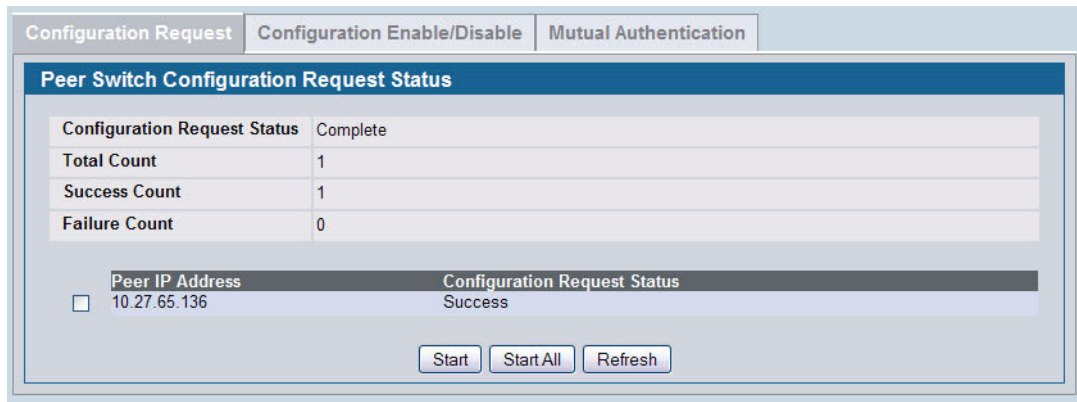


Figure 393: Peer Switch Configuration Request Status

To initiate a configuration update on a specific peer switch, select the box next to the IP address of the peer switch to update, and then click **Start**. To update all peer switches, click **Start All**.

The following table describes the fields on the **Peer Switch Configuration Request Status** page.

Table 357: Peer Switch Configuration Request Status

Field	Description
Configuration Request Status	Indicates the global status for a configuration push operation to one or more peer switches. The status can be one of the following: <ul style="list-style-type: none"> • Not Started • Receiving Configuration • Saving Configuration • Success • Failure—Invalid Code Version • Failure—Invalid Hardware Version • Failure—Invalid Configuration
Total Count	Indicates the number of peer switches included at the time a configuration download request is started, the value is 1 if a download request is for a single switch.
Success Count	Indicates the total number of peer switches that have successfully completed a configuration download.
Failure Count	Indicates the total number of peer switches that have failed to complete a configuration download.
Peer IP Address	Lists the IP address of each switch in the cluster and indicates the configuration request status of that switch.

Peer Switch Configuration Enable/Disable

You can copy portions of the switch configuration from one switch to another switch in the cluster. The **Peer Switch Configuration Enable/Disable** page allows you to select which parts of the configuration to copy to one or more peer switches in the group.

Peer Switch Configuration Enable/Disable	
Global	Enable
Discovery	Disable
Channel/Power	Enable
AP Database	Enable
AP Profiles	Enable
Known Client	Enable
Captive Portal	Enable
RADIUS Client	Enable
QoS ACL	Enable
QoS DiffServ	Enable
WDS Group	Enable
Device Location	Enable

Figure 394: Peer Switch Configuration Enable/Disable

You can make changes to a configuration that has been sent to one or more peer switches, and you can make changes to a configuration received from a peer switch. No changes automatically propagate from one switch to the cluster; you must manually initiate a request on one switch in order to copy any configuration to its peers.

The following table shows the fields on the detail page for **Peer Switch Configuration Enable/Disable** page.

Table 358: Peer Switch Configuration Enable/Disable

Field	Description
Global	<p>Enable this field to include the basic and advanced global settings in the configuration that the switch pushes to its peers. The configuration does not include the switch IP address since that is a unique setting.</p> <p>To view current basic global settings, click the WLAN > Administration > Basic Setup > Global tab. To view current advanced global settings, click the WLAN > Advanced Configuration > Global page.</p>
Discovery	<p>Enable this field to include the L2 and L3 discovery information, including the VLAN list and IP list, in the configuration that the switch pushes to its peers.</p> <p>To view the discovery settings on the local switch, click the WLAN > Administration > Basic Setup > Discovery tab.</p>

Table 358: Peer Switch Configuration Enable/Disable (Cont.)

Field	Description
Channel/Power	<p>Enable this field to include the RF management information in the configuration that the switch pushes to its peers.</p> <p>To view the channel and power settings on the local switch, click the WLAN > Administration > AP Management > RF Management tab.</p>
AP Database	<p>Enable this field to include the AP Database in the configuration that the switch pushes to its peers.</p> <p>To view the contents of the local AP Database, click the WLAN > Administration > Basic Setup > Valid AP tab.</p>
AP Profiles	<p>Enable this field to include all AP profiles in the configuration that the switch pushes to its peers. The AP profile includes the global AP settings, such as the hardware type, Radio settings, VAP and Wireless Network settings, and QoS settings.</p> <p>To view the local AP Profile settings, click the WLAN > Administration > Advanced Configuration > AP Profile tab.</p>
Known Client	<p>Enable this field to include the Known Client Database in the configuration that the switch pushes to its peers.</p> <p>To view the contents of the local AP Database, click the WLAN > Administration > Advanced Configuration > Clients > Known Client page.</p>
Captive Portal	<p>Enable this field to include the Captive Portal information in the configuration that the switch pushes to its peers.</p> <p>To view the Captive Portal settings on the local switch, click the pages available in the Security > Captive Portal folder.</p> <p>Note: You can access the Captive Portal pages from either the LAN or WLAN tabs.</p>
RADIUS Client	<p>Enable this field to include the Client RADIUS information in the configuration that the switch pushes to its peers.</p> <p>To view the Client RADIUS settings on the local switch, click the pages available in the LAN > Security > RADIUS folder.</p>
QoS ACL	<p>Enable this field to include the QoS ACLs in the configuration that the switch pushes to its peers.</p> <p>To view the ACL settings on the local switch, click the pages available in the LAN > Access Control Lists folder.</p>
Qos DiffServ	<p>Enable this field to include the Diffserv classes, services, and policies in the configuration that the switch pushes to its peers.</p> <p>To view the DiffServ settings on the local switch, click the pages available in the LAN > QoS > Differentiated Services folder.</p>
WDS Group	<p>Enable this field to include WDS AP group information in the configuration that the switch pushes to its peers.</p>
Device Location	<p>Enable this field to include AP and Client location information in the configuration that the switch pushes to its peers.</p>

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.

Mutual Authentication

Mutual Authentication provides security when adding switches and APs to the wireless network. If Mutual Authentication mode is enabled, the APs and switches perform X.509 Mutual Certificate exchanges. Each device compares the certificate received from the remote end-point with the local copy of the remote device's certificate. If the certificates don't match then the Transport Layer Security (TLS) connection is dropped.

Figure 395: Mutual Authentication

The following table shows the fields on the **Mutual Authentication** page.

Table 359: Mutual Authentication

Field	Description
Switch Provisioning Mode	When this field is enabled, switches can send and receive provisioning messages. As a security feature, you can disable switch provisioning. When switch provisioning mode is disabled the switch does not accept provisioning messages.
Network Mutual Authentication Mode	Select Enable to require mutual authentication on the wireless network. When Disable is selected, mutual authentication is not required. Changing this parameter on one switch automatically updates the configuration on all other switches in the cluster and all managed APs in the cluster. When this field is enabled, switch provisioning must be enabled in order for new switches to be added to the cluster. If switch provisioning is disabled, the cluster will not accept certificates from a new switch.
Unmanaged AP Reprovisioning Mode	When this field is enabled, the AP can be re-provisioned when it is not managed. Changing this parameter on one switch automatically updates the configuration on all other switches. This parameter is only applicable if mutual authentication is enabled.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.

WIDS Security

The D-Link Unified Switch Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network.

WIDS AP Configuration

The **WIDS AP Configuration** page allows you to activate or deactivate various threat detection tests and set threat detection thresholds in order to help detect rogue APs on the wireless network. These changes can be done without disrupting network connectivity. Since some of the work is done by access points, the switch needs to send messages to the APs to modify its WIDS operational properties.



Note: The classification settings on the WIDS AP Configuration page are part of the global configuration on the switch and must be manually pushed to other switches in order to synchronize that configuration.

Many of the tests are focused on identifying APs that are advertising managed SSIDs, but are not in fact managed APs. Detecting such an AP means that a network is either miss-configured or that a hacker set up a honeypot AP in the attempt to collect passwords or other secure information.

Although operational mode radios can detect most threats, the sentry radios detect the threats faster, especially when a potential rogue is operating on a different channel from any of the managed AP radios. The number of deployed sentry radios should be sufficient to provide coverage by one sentry radio in every geographical location within the network. A denser sentry deployment may be desirable in order to improve rogue or interferer signal triangulation.

WIDS AP Configuration	
Administrator configured rogue AP	Enable ▾
Managed SSID from an unknown AP	Enable ▾
Managed SSID from a fake managed AP	Enable ▾
AP without an SSID	Enable ▾
Fake managed AP on an invalid channel	Enable ▾
Managed SSID detected with incorrect security	Enable ▾
Invalid SSID from a managed AP	Enable ▾
AP is operating on an illegal channel	Enable ▾
Standalone AP with unexpected configuration	Enable ▾
Unexpected WDS device detected on network	Enable ▾
Unmanaged AP detected on wired network	Enable ▾
Rogue Detected Trap Interval (seconds)	300 (60 to 3600, 0 - Disable)
Wired Network Detection Interval (seconds)	60 (1 to 3600, 0 - Disable)
AP De-Authentication Attack	Disable ▾

Figure 396: WIDS AP Configuration

Table 360 shows the fields on the WIDS Security AP Configuration page.

Table 360: WIDS AP Configuration

Field	Description
Administrator configured rogue AP	If the source MAC address is in the valid-AP database on the switch or on the RADIUS server and the AP type is marked as <i>Rogue</i> , then the AP state is Rogue.
Managed SSID from an unknown AP	This test checks whether an unknown AP is using the managed network SSID. A hacker may set up an AP with managed SSID to fool users into associating with the AP and revealing password and other secure information. Administrators with large networks who are using multiple clusters should either use different network names in each cluster or disable this test. Otherwise, if an AP in the first cluster detects APs in the second cluster transmitting the same SSID as APs in the first cluster then these APs are reported as rogues.
Managed SSID from a fake managed AP	A hacker may set up an AP with the same MAC address as one of the managed APs and configure it to send one of the managed SSIDs. This test checks for a vendor field in the beacons which is always transmitted by managed APs. If the vendor field is not present, then the AP is identified as a fake AP.
AP without an SSID	SSID is an optional field in beacon frames. To avoid detection a hacker may set up an AP with the managed network SSID, but disable SSID transmission in the beacon frames. The AP would still send probe responses to clients that send probe requests for the managed SSID fooling the clients into associating with the hacker's AP. This test detects and flags APs that transmit beacons without the SSID field. The test is automatically disabled if any of the radios in the profiles are configured not to send SSID field, which is not recommended because it does not provide any real security and disables this test.
Fake managed AP on an invalid channel	This test detects rogue APs that transmit beacons from the source MAC address of one of the managed APs, but on different channel from which the AP is supposed to be operating.
Managed SSID detected with incorrect security	During RF Scan the AP examines beacon frames received from other APs and determines whether the detected AP is advertising an open network, WEP, or WPA. If the SSID reported in the RF Scan is one of the managed networks and its configured security not match the detected security then this test marks the AP as rogue.
Invalid SSID from a managed AP	This test checks whether a known managed AP is sending an unexpected SSID. The SSID reported in the RF Scan is compared to the list of all configured SSIDs that are used by the profile assigned to the managed AP. If the detected SSID doesn't match any configured SSID then the AP is marked as rogue.
AP is operating on an illegal channel	The purpose of this test is to detect hackers or incorrectly configured devices that are operating on channels that are not legal in the country where the wireless system is set up. Note: In order for the wireless system to detect this threat, the wireless network must contain one or more radios that operate in sentry mode.

Table 360: WIDS AP Configuration (Cont.)

Field	Description
Standalone AP with unexpected configuration	<p>If the AP is classified as a known standalone AP, then the switch checks whether the AP is operating with the expected configuration parameters. You configure the expected parameters for the standalone AP in the local or RADIUS Valid AP database.</p> <p>This test may detect network misconfiguration as well as potential intrusion attempts. The following parameters are checked:</p> <ul style="list-style-type: none"> • Channel Number • SSID • Security Mode • WDS Mode • Presence on a wired network
Unexpected WDS device detected on network	<p>If the AP is classified as a Managed or Unknown AP and wireless distribution system (WDS) traffic is detected on the AP, then the AP is considered to be Rogue.</p> <p>Only stand-alone APs that are explicitly allowed to operate in WDS mode are not reported as rogues by this test.</p>
Unmanaged AP detected on wired network	<p>This test checks whether the AP is detected on the wired network. If the AP state is Unknown, then the test changes the AP state to Rogue. The flag indicating whether AP is detected on the wired network is reported as part of the RF Scan report. If AP is managed and is detected on the network then the switch simply reports this fact and doesn't change the AP state to Rogue.</p> <p>In order for the wireless system to detect this threat, the wireless network must contain one or more radios that operate in sentry mode.</p>
Rogue Detected Trap Interval	<p>Specify the interval, in seconds, between transmissions of the SNMP trap telling the administrator that rogue APs are present in the RF Scan database. If you set the value to 0, the trap is never sent.</p>
Wired Network Detection Interval	<p>Specify the number of seconds that the AP waits before starting a new wired network detection cycle. If you set the value to 0, wired network detection is disabled.</p>
AP De-Authentication Attack	<p>Enable or disable the AP de-authentication attack.</p> <p>The wireless switch can protect against rogue APs by sending de-authentication messages to the rogue AP. The de-authentication attack feature must be globally enabled in order for the wireless system to do this function. Make sure that no legitimate APs are classified as rogues before enabling the attack feature. This feature is disabled by default.</p>

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.

WIDS Client Configuration

The D-Link Unified Switch Wireless Intrusion Detection System (WIDS) can help detect intrusion attempts into the wireless network and take automatic actions to protect the network. The settings you configure on the **WIDS Client Configuration** page help determine whether a detected client is classified as a rogue. Clients classified as rogues are considered to be a threat to network security.



Note: The classification settings on the WIDS Client Configuration page are part of the global configuration on the switch and must be manually pushed to other switches in order to synchronize that configuration.

As part of the general association and authentication process, wireless clients send 802.11 management messages to APs. The WIDS feature tracks the following types of management messages that each detected client sends:

- Probe Requests
- 802.11 Authentication Requests.
- 802.11 De-Authentication Requests.

In order to help determine whether a client is posing a threat to the network by flooding the network with management traffic, the system keeps track of the number of times the AP received each message type and the highest message rate detected in a single RF Scan report. On the **WIDS Client Configuration** page, you can set thresholds for each type of message sent, and the APs monitor whether any clients exceed those thresholds or tests.

WIDS Client Configuration	
Not Present in OUI Database Test	Disable
Known Client Database Test	Disable
Configured Authentication Rate Test	Enable
Configured Probe Requests Rate Test	Enable
Configured De-Authentication Requests Rate Test	Enable
Maximum Authentication Failures Test	Enable
Authentication with Unknown AP Test	Disable
Client Threat Mitigation	Disable
Known Client Database Lookup Method	Local
Known Client Database Radius Server Name	Default-RADIUS-Server
Rogue Detected Trap Interval (seconds)	300 (60 to 3600, 0 - Disable)
De-Authentication Requests Threshold Interval (seconds)	60 (1 to 3600)
De-Authentication Requests Threshold Value	10 (1 to 99999)
Authentication Requests Threshold Interval (seconds)	60 (1 to 3600)
Authentication Requests Threshold Value	10 (1 to 99999)
Probe Requests Threshold Interval (seconds)	60 (1 to 3600)
Probe Requests Threshold Value	120 (1 to 99999)
Authentication Failure Threshold Value	5 (1 to 99999)

Figure 397: WIDS Client Configuration

Table 361 describes the fields on the **WIDS Client Configuration** page.

Table 361: WIDS Client Configuration

Field	Description
Not Present in OUI Database Test	This test checks whether the MAC address of the client is from a registered manufacturer identified in the OUI database.
Known Client Database Test	This test checks whether the client, which is identified by its MAC address, is listed in the Known Client Database and is allowed access to the AP either through the Authentication Action of Grant or through the White List global action. If the client is in the Known Client Database and has an action of Deny, or if the action is Global Action and it is globally set to Black List, the client fails this test.
Configured Authentication Rate Test	This test checks whether the client has exceeded the configured rate for transmitting 802.11 authentication requests.
Configured Probe Requests Rate Test	This test checks whether the client has exceeded the configured rate for transmitting probe requests.
Configured De-Authentication Requests Rate Test	This test checks whether the client has exceeded the configured rate for transmitting de-authentication requests.
Maximum Authentication Failures Test	This test checks whether the client has exceeded the maximum number of failed authentications.
Authentication with Unknown AP Test	This test checks whether a client in the Known Client database is authenticated with an unknown AP.
Client Threat Mitigation	Select enable to send de-authentication messages to clients that are in the Known Clients database but are associated with unknown APs. The Authentication with Unknown AP Test must also be enabled in order for the mitigation to take place. Select disable to allow clients in the Known Clients database to remain authenticated with an unknown AP.
Known Client Database Lookup Method	When the switch detects a client on the network it performs a lookup in the Known Client database. Specify whether the switch should use the local or RADIUS database for these lookups.
Known Client Database RADIUS Server Name	If the known client database lookup method is RADIUS then this field specifies the RADIUS server name.
Rogue Detected Trap Interval	Specify the interval, in seconds, between transmissions of the SNMP trap telling the administrator that rogue APs are present in the RF Scan database. If you set the value to 0, the trap is never sent.
De-Authentication Requests Threshold Interval	Specify the number of seconds an AP should spend counting the de-authentication messages sent by wireless clients.
De-Authentication Requests Threshold Value	If switch receives more than specified messages during the threshold interval the test triggers.
Authentication Requests Threshold Interval	Specify the number of seconds an AP should spend counting the authentication messages sent by wireless clients.
Authentication Requests Threshold Value	If switch receives more than specified messages during the threshold interval the test triggers.

Table 361: WIDS Client Configuration (Cont.)

Field	Description
Probe Requests Threshold Interval	Specify the number of seconds an AP should spend counting the probe messages sent by wireless clients.
Probe Requests Threshold Value	Specify the number of probe requests a wireless client is allowed to send during the threshold interval before the event is reported as a threat.
Authentication Failure Threshold Value	Specify the number of 802.1X authentication failures a client is allowed to have before the event is reported as a threat.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).
- **Refresh**—Updates the page with the latest information.

Known Client

The Known Client Summary shows the wireless clients currently in the Known Client Database and allows you to add new clients to the database. The database contains wireless client MAC addresses and names. The database is used to retrieve client descriptive names from the RADIUS server as well as implement MAC Authentication.



Figure 398: Known Client Summary

Table 362 describes the fields on **Known Client Summary** page.

Table 362: Known Client Summary

Field	Description
MAC Address	Shows the MAC address of the known client.
Name	Shows the descriptive name configured for the client when it was added to the Known Client database.
Authentication Action	When MAC authentication is enabled on the network, this field shows the action to take on a wireless client. The following options are available: <ul style="list-style-type: none"> • Grant—Allow the client with the specified MAC address to access the network. • Deny—Prohibit the client with the specified MAC address from accessing the network. • Global Action—Use the global white-list or black-list action configured on the Advanced Global Configuration page to determine how to handle the client.

To add a client to the Known Client database, enter the MAC address of the client in the available field and click **Add**. To remove a client from the Known Client database, select the check box next to the client MAC address and click **Delete**. To remove all clients from the database, click **Delete All**. To view or configure information about an existing client, click the MAC address of the client.

Command Buttons

The page includes the following buttons:

- **Add**—Adds a client with the MAC address you enter in the field to the Known Client database.
- **Delete**—Removes the selected client from the Known Client database.
- **Delete All**—Removes all clients in the list from the Known Client database.
- **Refresh**—Updates the page with the latest information.

Known Client Configuration

The Known Client Configuration page allows you to add wireless clients to the Known Client Database and specify the authentication action to take on the client when it attempts to access the network. The database contains wireless client MAC addresses and names. The database is used to retrieve client descriptive names from the RADIUS server as well as implement MAC Authentication.

Figure 399: Known Client Configuration

Table 363 describes the fields on **Known Client Configuration** page.

Table 363: Known Client Configuration

Field	Description
MAC Address	Shows the MAC address of the client. To view or configure the name or authentication action for another client in the Known Client database, select its MAC address from the menu.
Name	Enter a descriptive name for the client, which can contain up to 32 alphanumeric characters. This field is optional.
Authentication Action	Specify the action to take on a wireless client when MAC authentication is enabled on the network. The following options are available: <ul style="list-style-type: none"> • Grant—Allow the client with the specified MAC address to access the network. • Deny—Prohibit the client with the specified MAC address from accessing the network. • Global Action—Use the global white-list or black-list action configured on the Advanced Global Configuration page to determine how to handle the client.

Command Buttons

The page includes the following buttons:

- **Refresh**—Updates the page with the latest information.
- **Submit**—Updates the switch with the values you enter. To retain the new values across a power cycle, you must perform a save (Tool > Save Changes).

Switch Provisioning

Use the **Switch Certificate Request** page to request a X.509 certificate from the cluster controller. The X.509 mutual certificate exchange is the only mechanism for peer switches to authenticate with each other because switches do not support pass-phrase authentication.

The X.509 certificate is automatically generated by the switch, so it does not communicate with any trusted certificate authority, and there are no certificate maintenance fees.

Figure 400: Switch Certificate Request

The following table shows the fields available on the **Switch Certificate Request** page.

Table 364: Switch Certificate Request

<i>Field</i>	<i>Description</i>
Switch IP Address	Enter the IP address of the wireless switch from which this switch requests an X.509 certificate.
Switch Certificate Request Status	Shows the status of the request, which is one of the following: <ul style="list-style-type: none"> • Not Started—Certificate exchange has not started. • Invalid IP address—IP address specified in the Switch IP Address field is not valid. • In Progress—Certificate request is in progress. • Success—Certificate has been obtained and added to the certificate file. • Timed Out—Certificate request timed out without getting a certificate.

Command Buttons

The page includes the following buttons:

- **Start**—Initiates the X.509 certificate request.
- **Refresh**—Updates the page with the latest information.

Provisioning

Use the **Switch Provisioning** page to request provisioning information from a switch in the cluster. After the new switch receives the provisioning information, it can join the cluster.

Figure 401: Switch Provisioning

The following table shows the fields available on the **Switch Provisioning** page.

Table 365: Switch Provisioning

Field	Description
Switch IP Address	Enter the IP address of the switch in a cluster to which a new switch establishes a connection to obtain provisioning information. The provisioning information enables the new switch to join the cluster.
Switch Provisioning Status	Shows the status of the provisioning, which is one of the following: <ul style="list-style-type: none"> • Not Started • Success—The provisioning sequence completed successfully. • Connection Failed—Can't establish TLS connection with the cluster switch. • Provisioning Failed—The switch in the cluster did not respond with expected messages. This can happen if the switch is running code that does not support switch provisioning or the switch provisioning mode is disabled on the switch in the cluster.

Command Buttons

The page includes the following buttons:

- **Start**—Initiates the provisioning request for the switch.
- **Refresh**—Updates the page with the latest information.

Enabling AeroScout™ Engine Support

The AeroScout Engine (AE) is a software platform produced by AeroScout Inc. for location-based services. The AE can determine the physical location of 802.11-capable AeroScout devices. The AE communicates with APs that have the AE protocol enabled in order to collect information about the RF devices detected by the APs.

The DWS-4000 Series switch supports only direct communication between the AE and the APs. When operating in managed mode, the AE is configured with the IP address of the managed access points from which it collects information. The DWS-4000 Series switch does not communicate with the AE.

AeroScout tags operate only in 802.11b/g mode. Therefore, network administrators who use the AeroScout tags must configure at least one radio on APs that are expected to detect tags in either 802.11b/g or 802.11b/g/n mode. The radios configured in 2.4 GHz IEEE 802.11n mode or any of the 5 GHz modes cannot detect AeroScout tags.

To enable AeroScout support, see [“Configuring the AP Profile Global Settings” on page 595](#).



Note: The following notes apply to AeroScout product and protocol support:

- D-Link does not sell AeroScout products. Contact AeroScout for AeroScout hardware, software or deployment information.
- The AE protocol does not support any authentication or encryption between the AE server and the access point.
- The AE protocol requires radios to operate in promiscuous mode. This means that the AP receives and processes all packets detected by the radios, as opposed to processing only packets destined to the APs BSSID. This can affect AP throughput.

Configuring the Wireless Distribution System

The Wireless Distribution System (WDS)-Managed AP feature allows you to add managed APs to the cluster using over-the-air WDS links through other managed APs. This capability is critical in providing a seamless experience for roaming clients and for managing multiple wireless networks. It can also simplify the network infrastructure by reducing the amount of cabling required. With WDS, APs may be located outdoors where wired connection to the data network is unavailable, or in remote buildings that are not connected to the main campus with a wired network.

The WDS AP group consists of two types of APs: root APs and satellite APs. A root AP acts as a bridge or repeater on the wireless medium and communicates with the switch via the wired link. A satellite AP communicates with the switch via a WDS link to the root AP. The WDS links are secured using WPA2 Personal authentication and AES encryption.

Support for the WDS-managed AP feature within the Unified Wired and Wireless Access System includes the following:

- The wireless system can contain up to two WDS-managed AP groups.
- Each WDS-managed AP group can contain up to four APs.
- An AP can be a member of only one WDS AP group.
- Each satellite AP can have only one WDS link on the satellite APs. This means that a satellite AP must be connected to a root AP. A satellite AP cannot be connected to another satellite AP.

The following image shows a WDS group with one root AP and two satellite APs. Dashed lines represent wireless connections.

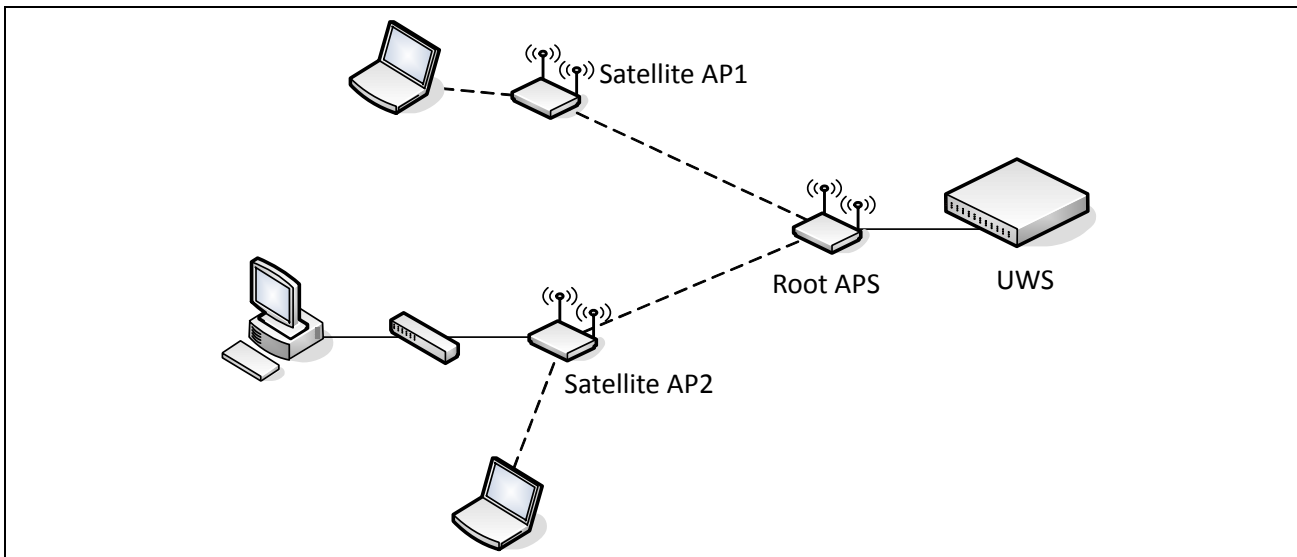


Figure 402: WDS-Managed AP Group

The WDS group in [Figure 402](#) has the following characteristics:

- All three APs are managed by the Unified Wired and Wireless Access System.
- The group has two WDS AP links: one link is between the Root AP and Satellite AP1, and one link is between the Root AP and Satellite AP2.
- The Ethernet port on Satellite AP2 is enabled to allow wired LAN access to remote office PCs.

By default, an AP is configured as a root AP. For an AP to be attached to the Wireless System as a satellite AP, configure the following settings on the AP while it is in stand-alone mode:

- **Satellite AP mode.** This setting enables the satellite AP to discover and establish WDS link with the root AP. By default, the WDS Managed Mode is *Root AP*.
- **Password for WPA2 Personal authentication** used to establish the WDS links. Only the satellite APs need this configuration. The root APs get the password from the switch when they become managed.
- **Static Channel.** The APs on each end of a WDS link must use the same radio and channel to communicate. Configure the satellite AP to use a static channel. For a root AP, set the static channel when you add the AP to the Valid AP database on the switch.
- **Optionally, to allow the Ethernet port on a satellite AP to provide wired access to the LAN, you must set the WDS Managed Ethernet Port to Enabled.** It is disabled by default.

For information about configuring the stand-alone AP by using the web-based interface, see the *Administrator's Guide* for the UAP.



Caution! Certain topologies for WDS managed APs can result in unpredictable behavior. For example, if a satellite AP has the Ethernet port enabled and has a wired connection to a switch that manages the same WDS group, the satellite AP cannot determine which path to establish a management connection on because spanning tree is not yet functional. A satellite AP, by definition, should have a connection to the managed switch only over the air. Otherwise, it is considered a root AP (if it is part of a WDS managed group). If there are multiple wireless paths from an AP to the managed switch, spanning tree for the WDS group must be enabled to prevent loops.

To configure a WDS managed group and its links, use the following general steps:

1. Configure the satellite APs by connecting to the AP management interface while the AP is in stand-alone mode. Set the WDS Managed Mode to Satellite AP and configure the WDS Group Password.
2. From the switch CLI or web-based interface, create a WDS group.
3. Configure the WDS group password. The password you configure on the switch should be the same as the password you configure on each satellite AP.
4. Add the MAC address of each AP to the WDS group.
5. Configure the WDS links by specifying the MAC address and radio of the AP on each end of the link.

Keep the following considerations in mind when you configure and manage a WDS group:

- Make sure the radios that participate in the WDS link use the same channel. Use one of the following methods to control the channel:
 - When you configure the satellite AP in stand-alone mode, use the Radio page to set a static channel.
 - When you configure the AP in the Valid AP database, specify the channel that the radio must use. By default, the channel is set to Auto.
 - On the Radio page for the AP profile, select only one channel in the list of Auto Eligible channels. By default, multiple channels are enabled.
- D-Link recommends that satellite APs do not have wired connectivity to the wireless switch.
- A configuration push to WDS APs may take up to three minutes to complete.

WDS Managed AP Group Configuration

Use the **WDS Managed AP Group Configuration** page to add or delete WDS-Managed AP groups and to configure group settings. Changes to the WDS AP group do not take effect on the APs until the WDS AP group database is pushed to the cluster. Use the **Push Config** button to ensure the changes you make are applied to the switches and APs in the cluster. APs that become managed after the WDS AP group database is pushed to the cluster pick up the configuration.



Note: To ensure that the network is operating as intended, always push the configuration after making all desired changes to the WDS AP group.

Figure 403: WDS Managed AP Group Configuration

The following table shows the fields available on the **WDS Managed AP Group Configuration** page.

Table 366: WDS Managed AP Group Configuration

<i>Field</i>	<i>Description</i>
ID	This field appears after at least one WDS group has been created. The ID is a number from 1–8 that identifies the WDS AP group. This number is automatically assigned when you create the group.
Group Name	A descriptive name of the WDS AP group, which can contain up to 32 characters.

Command Buttons

The page includes the following buttons:

- **Add**—Adds the group with the name entered into the field.
- **Delete**— Deletes the selected group.
- **Refresh**—Updates the page with the latest information.
- **Push Config**—Push the WDS-Managed AP group information to all switches that are members of the cluster.

When you add a new WDS-Managed AP group or click the group name, the page refreshes and fields to configure the group setting appear.



Note: After you change WDS-Managed AP group settings, make sure you push the configuration to other switches in the cluster.

Figure 404: Edit WDS Managed AP Group Settings

The following table shows the fields available to configure a WDS managed AP group.

Table 367: Edit WDS Managed AP Group Settings

Field	Description
WDS Group Name	A descriptive name of the WDS AP group. From this field, you can modify the name of an existing group, if desired.
Spanning Tree	Specifies whether to enable spanning tree on all APs in this WDS AP group. Spanning tree must be enabled if there are any potential loops in the network. For example if a satellite AP has links to two root APs then spanning tree must be enabled. Note: The spanning tree protocol running on the APs interacts with the spanning tree protocol running on the edge switches to which the APs are connected.
WDS Group Password	Password used for securing the WPA2-Personal security on the WDS Link. Range: 8–63 ASCII characters. To create or change the password, select the Edit checkbox and type a password in the available field. This password must match the passwords set on the satellite APs in this group. By default, the password is AP-Group- <i>n</i> , where <i>n</i> is the AP group ID.

Command Buttons

The page includes the following buttons:

- **Submit**—Updates the switch with the values you enter.

WDS Managed AP Configuration

After you create a WDS-Managed AP group, use the **WDS Managed AP Configuration** page to view the APs that are members of the group, add new members, and change STP Priority values for existing members.



Note: After you change WDS-Managed AP group settings, make sure you push the configuration to other switches in the cluster.

Figure 405: WDS Managed AP Configuration

The following table shows the fields available on the **WDS Managed AP Summary** page.

Table 368: WDS Managed AP Summary

<i>Field</i>	<i>Description</i>
WDS Group ID	Select the ID associated with the group to configure.
AP MAC Address	MAC Address of the AP.
STP Priority	Spanning Tree Priority for this AP. The STP priority is used only when spanning tree mode is enabled. The STP priority determines which AP is selected as the root of the spanning tree and which AP has preference over another AP when multiple equal cost paths exist in the topology. The lower value for the spanning tree priority means that the AP is more likely to be used for bridging data into the campus network. You should assign a lower priority to the APs connected to the wired network than to the satellite APs. The STP priority value is rounded down to a multiple of 4096. The range is 0–61440, and the default value is 36864.

Command Buttons

The page includes the following buttons:

- **Add**—Allows you to configure a new AP for the selected group. When you click **Add**, the **WDS Managed AP Group Configuration** page displays.
- **Submit**—Select the checkbox associated with an AP to modify the STP Priority value for the AP. Click **Apply** to update the switch with the values you enter.
- **Delete**—Deletes the selected AP.
- **Refresh**—Updates the page with the latest information.



Note: If no APs have been added to the selected WDS group, only the **Add** and **Refresh** buttons display.

When you click **Add** from the WDS Managed AP Summary page, the page refreshes and displays fields to configure the WDS Managed AP settings.



Note: After you change WDS-Managed AP group settings, make sure you push the configuration to other switches in the cluster.

Figure 406: WDS Managed AP Settings

The following table shows the fields available to configure the WDS Managed AP settings.

Table 369: WDS Managed AP Group Configuration

Field	Description
AP MAC Address	MAC Address of the AP.
STP Priority	Spanning Tree Priority for this AP. The STP priority is used only when spanning tree mode is enabled. The STP priority determines which AP is selected as the root of the spanning tree and which AP has preference over another AP when multiple equal cost paths exist in the topology. The lower value for the spanning tree priority means that the AP is more likely to be used for bridging data into the campus network. You should assign a lower priority to the APs connected to the wired network than to the satellite APs. The STP priority value is rounded down to a multiple of 4096. The range is 0–61440, and the default value is 36864.

Command Buttons

The page includes the following buttons:

- **Submit**—Update the switch with the values you enter.

WDS Link Configuration

After you create a WDS-Managed AP group, use the **WDS AP Link Configuration** page to configure the WDS links between the APs that are members of the group.



Note: After you change WDS-Managed AP group settings, make sure you push the configuration to other switches in the cluster.

Source AP MAC Address	Source Radio	Dest AP MAC Address	Dest AP Radio	STP Link Cost
<input type="checkbox"/> 1C:AF:F7:1F:27:80	1	00:12:C9:3E:36:BA	1	100

Figure 407: WDS AP Link Configuration

The following table shows the fields available on the **WDS AP Link Configuration** page.

Table 370: WDS AP Link Configuration

Field	Description
WDS Group ID	Select the ID associated with the group to configure.
Source AP MAC Address	MAC Address of the source AP. The AP must be included in the selected WDS group. Note: The WDS links are bidirectional. The terms <i>Source</i> and <i>Destination</i> simply reflect the WDS link endpoints specified when the WDS link is created.
Source Radio	The radio number of the WDS link endpoint on the source AP.
Dest AP MAC Address	The MAC address of the destination AP in the group.
Destination Radio	The radio number of the WDS link endpoint on the destination AP.
STP Link Cost	Spanning Tree Path cost for the WDS link. The range is 0–255. When multiple alternate paths are defined in the WDS group, the link cost is used to indicate which links are the primary links and which links are the secondary links. The spanning tree selects the path with the lowest link cost.

Command Buttons

The page includes the following buttons:

- **Add**—Allows you to configure a new WDS link for the selected group. When you click **Add**, the **WDS Link Create** page displays.
- **Submit**—Select the checkbox associated with a link to modify the STP Link Cost value. Click **Apply** to update the switch with the value you enter.
- **Delete**—Deletes the selected WDS link.
- **Refresh**—Updates the page with the latest information.



Note: If no links have been configured for the selected WDS group, only the **Add** and **Refresh** buttons display.

WDS Link Create

When you click **Add** from the WDS AP Link Configuration page, the **WDS Link Create** page displays. From this page, you can create WDS links between APs in the WDS group.



Note: After you change WDS-Managed AP group settings, make sure you push the configuration to other switches in the cluster.

Figure 408: WDS Link Create

The following table shows the fields available on the **WDS Link Create** page.

Table 371: WDS Link Create

Field	Description
Source AP MAC Address	MAC Address of the source AP. Note: The WDS links are bidirectional. The terms <i>Source</i> and <i>Destination</i> simply help to differentiate between the WDS link endpoints.
Source AP Radio	The radio number of the WDS link endpoint on the source AP.
Destination AP MAC Address	The MAC address of the destination AP in the group.
Destination Radio	The radio number of the WDS link endpoint on the destination AP.
STP Link Cost	Spanning Tree Path cost for the WDS link. The range is 0–255. When multiple alternate paths are defined in the WDS group, the link cost is used to indicate which links are the primary links and which links are the secondary links. The spanning tree selects the path with the lowest link cost.

Command Buttons

The page includes the following button:

- **Submit**—Update the switch with the values you enter.

Locating WLAN Devices

The Device Location feature can help you physically locate APs and other WLAN devices within the wireless system. The feature can help locate devices that are in different buildings within a campus environment and on multiple floors within a building. To compute the probable location of a device within the wireless network, the wireless system uses a triangulation algorithm. The location computation is performed by the Cluster Controller switch.

You can configure floor and building information by using the pages within the Device Location folder or by using the WLAN Visualization tool. By default, the WLAN Visualization tool continuously polls the switch to maintain an up-to-date view of the wireless network and pushes any configuration changes to the switch.



Note: D-Link recommends that you do not attempt to configure location information by using the switch UI and the WLAN Visualization at the same time.

You can use the WLAN Visualization tool to trigger the location search and to display the computed probability map.

Managed AP Location

The pages available from the Managed AP Location link allow you to define the buildings and floors that make up the wireless network. You can also manually enter coordinates for the AP locations in each building and floor.

Building

Wireless networks are often deployed in campus environments that include multiple buildings. Use the **Building** page to define the buildings where APs are deployed.

Building Number	Building Description	Total Floor Count	Total AP Count
<input type="checkbox"/> 1	100 Corporate Drive	2	0

Building(1 - 8) Description

Figure 409: Building

The following table shows the fields available on the **Building** page.

Table 372: Building

Field	Description
Building Number	Unique number from 1–8 that identifies a building within the wireless system.
Building Description	A description for the building, such as an address or function. The name can be up to 64 characters. The default name is Building- <i>n</i> , where <i>n</i> is the building number.
Total Floor Count	Number of floors configured for the building.
Total AP Count	Number of APs in the building with an administratively-configured physical location.

Command Buttons

The page includes the following buttons:

- **Delete**— Deletes the selected building from the database.
- **Delete All**—Deletes all buildings configured in the database.
- **Refresh**—Updates the page with the latest information.

Building Floor

Use the **Building Floor** page to define the floors within the buildings where APs are deployed.

Floor Number	Floor Description	Total AP Count
<input type="checkbox"/> 1	Admin	0
<input type="checkbox"/> 2	Marketing	0

Figure 410: Building Floor

The following table shows the fields available on the **Building Floor** page.

Table 373: Building Floor

<i>Field</i>	<i>Description</i>
Building Number	Select the number of the building with the floors to define.
Floor Number	Unique number from 1–20 that identifies the floor within the selected building.
Floor Description	A description used to identify the floor. The name can be up to 64 characters. The default description is None.
Total AP Count	Number of APs on the floor with an administratively-configured physical location.

Command Buttons

The page includes the following buttons:

- **Delete**—Deletes the selected floor from the building.
- **Delete All**—Deletes all configured floors from the building.
- **Refresh**—Updates the page with the latest information.

Managed AP Coordinates

Use the **Managed AP Coordinates** page to manually specify where APs are physically located.

Figure 411: Managed AP Coordinates

The following table shows the fields available on the **Managed AP Coordinates** page.

Table 374: Managed AP Coordinates

Field	Description
Building Number	Select the number that identifies the building where the AP is located.
Floor Number	Select the number that identifies the floor where the AP is located.
AP MAC Address	Identifies the MAC address of the AP
Measurement Units	Specify whether the coordinate units are meters or feet.
X-Coordinate	Specify the X axis offset of the managed AP from some arbitrary 0,0 point on the building floor. By convention the X axis is the horizontal axis. The range is –3000 to 3000 feet or –1000 to 1000 meters.
Y-Coordinate	Specify the Y axis offset of the managed AP from some arbitrary 0,0 point on the building floor. By convention the Y axis is the vertical axis. The range is –3000 to 3000 feet or –1000 to 1000 meters.

Command Buttons

The page includes the following buttons:

- **Add**— Adds the AP information defined in the fields to the selected building and floor.
- **Delete**— Removes the selected AP from the database.
- **Delete All**—Removes all APs configured in the database.
- **Refresh**—Updates the page with the latest information.

Managed AP Location Summary

Use the **Managed AP Location Summary** page to view summary information about the location of the APs in the wireless network. The page displays the APs with a location that has been manually configured or imported from the WLAN Visualization tool.

The screenshot shows a web interface with a navigation bar containing 'Building', 'Building Floor', 'Managed AP Coordinates', and 'Managed AP Location Summary'. Below the navigation bar is a section titled 'Managed AP Location Summary' with a dropdown menu for 'Building Number' set to 'All'. A table displays the following data:

Building / Floor Number	AP MAC Address	X-Coordinate(Meters)	Y-Coordinate(Meters)
1 / 2	00:05:5e:56:26:90	169	71
1 / 2	00:10:18:33:fc:00	42	90
1 / 2	1c:af:f7:1f:27:40	29	22
1 / 2	1c:af:f7:1f:27:80	42	83
1 / 2	5c:d9:98:2f:3f:00	35	45

Below the table is a 'Refresh' button.

Figure 412: Managed AP Location Summary

The following table shows the fields available on the **Managed AP Location Summary** page.

Table 375: Managed AP Location Summary

Field	Description
Building/Floor Number	Identifies the building and floor where the AP is located.
AP MAC Address	Identifies the MAC address of the AP
X-Coordinate	Identifies the X axis offset of the managed AP from some arbitrary 0,0 point on the building floor.
Y-Coordinate	Identifies the Y axis offset of the managed AP from some arbitrary 0,0 point on the building floor.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

On-Demand Location Trigger

Use the **On-Demand Location Trigger** page to find the location of an AP or wireless client. You can request the location of an AP or a client which is already detected by the system, or specify a MAC address of the device that has not yet been detected.

Figure 413: On-Demand Location Trigger

The following table shows the fields available on the **On-Demand Location Trigger** page.

Table 376: On-Demand Location Trigger

Field	Description
Building Number	Select the number that identifies the building to be searched for devices. Select All to search all buildings.
Floor Number	Select the number that identifies the floor of the building to be searched for devices. Select All to search all floors within the selected building.
Type of Device	Specify whether to search for APs or wireless clients.
Device MAC	If the checkbox is clear, specify the MAC address of the device to locate in the Target Device MAC Address field. If the checkbox is selected, you can choose the target device MAC address from a list of MAC addresses of devices that have already been detected.
Target Device MAC Address	Specify the MAC address of the device to find.
Use Operational Mode Radios	If the checkbox is clear, only the radios that are configured to be in sentry mode perform the search. If the checkbox is selected, both sentry and operational radios participate in the search.
Number of Locator APs	Identifies the number of managed APs that will participate in the search.
Location Procedure Status	Identifies whether the On-Demand Location procedure is currently running. The status is either Not in Progress or In Progress.

Command Buttons

The page includes the following buttons:

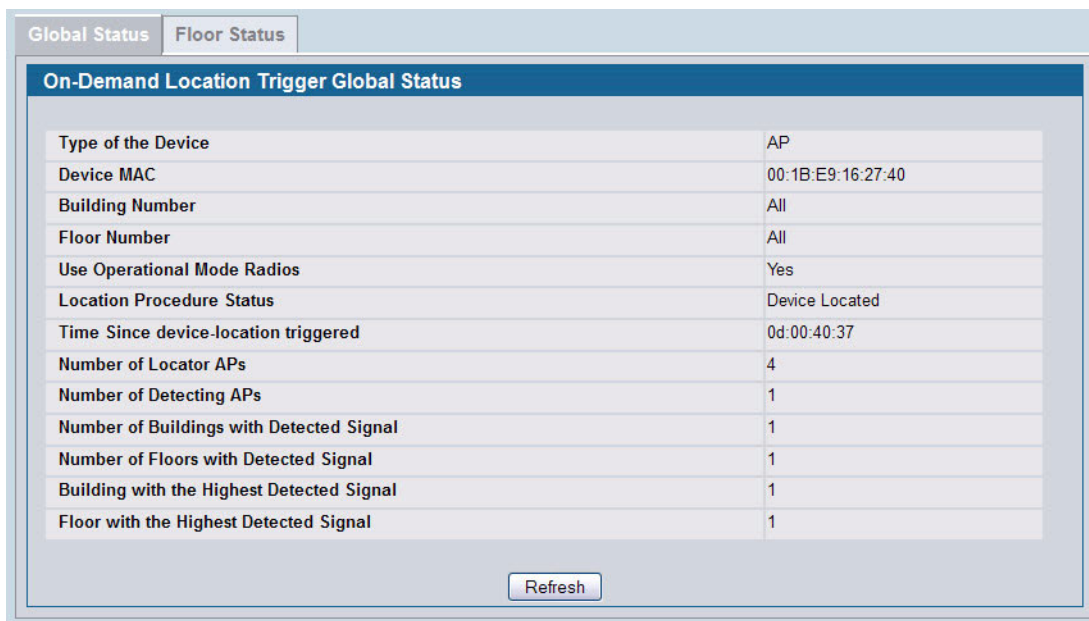
- **Count Search APs**—Recalculates the number of Locator APs. Modifying the building number, floor number, or inclusion of operational mode radios can change the number of APs that participate in the search.
- **Start Search**—Initiates the On-Demand Location process.
- **Refresh**—Updates the page with the latest information.

On-Demand Location Trigger Status

Use the page available from the **On-Demand Location Trigger Status** link to view the results of the On-Demand Location process.

On-Demand Location Trigger Global Status

Use the **On-Demand Location Trigger Global Status** page to view the results of the most recent On-Demand Location procedure. The status information is read-only and is updated by the Cluster Controller after the location procedure completes.



On-Demand Location Trigger Global Status	
Type of the Device	AP
Device MAC	00:1B:E9:16:27:40
Building Number	All
Floor Number	All
Use Operational Mode Radios	Yes
Location Procedure Status	Device Located
Time Since device-location triggered	0d:00:40:37
Number of Locator APs	4
Number of Detecting APs	1
Number of Buildings with Detected Signal	1
Number of Floors with Detected Signal	1
Building with the Highest Detected Signal	1
Floor with the Highest Detected Signal	1

Refresh

Figure 414: On-Demand Location Trigger Global Status

The following table shows the fields available on the **On-Demand Location Trigger Global Status** page.

Table 377: On-Demand Location Trigger Global Status

Field	Description
Type of Device	Indicates whether the most recent On-Demand Location process was invoked to find an AP or a Client.
Device MAC	AP or Client MAC address whose location was requested.
Building Number	Number that identifies the building that was searched for the device.
Floor Number	Number that identifies the floor of the building that was searched for the device.
Use Operational Mode Radios	Indicates whether the network used only sentry radios or both sentry and operational mode radios to perform the search.
Location Procedure Status	Identifies the current status of the On-Demand Location procedure: <ul style="list-style-type: none"> • Not Started • In Progress • Device Located • Device is not located • No APs Available for Locating Device
Time Since Device-Location Triggered	Amount of time in days, hours, minutes, and seconds that has passed since the search was initiated. If the on-demand device location was never triggered, the time stamp is 0d 00:00:00
Number of Locator APs	Number of managed APs that participated in the search.
Number of Detecting APs	Number of managed APs that detected the device.
Number of Buildings with Detected Signal	Number of buildings where managed APs detected the target device.
Number of Floors with Detected Signal	Number of building floors where managed APs detected the target device. Floors from different buildings may be included in this status.
Building with the Highest Detected Signal	Building number in which the target device was detected by a managed AP with the highest RSSI.
Floor with the Highest Detected Signal	Floor number on which the target device was detected by a managed AP with the highest RSSI.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

On-Demand Location Trigger Floor Status

Use the **On-Demand Location Trigger Floor Status** page to view the results of the most recent On-Demand Location procedure for each floor. The page can display entries for each floor, even if the device is not detected on the floor. If a building or floor was not included in the On-Demand search parameters, no data is reported for the floor.

Field	Value
Building Number	1
Floor Number	1
Device Found	Found
Number of Detecting APs	1
Solution Type	Point
X-Coordinate (Meters)	419
Y-Coordinate (Meters)	60
Circle Radius (Meters)	0
Sigma (Meters)	3

Figure 415: On-Demand Location Trigger Floor Status

The following table shows the fields available on the **On-Demand Location Trigger Floor Status** page.

Table 378: On-Demand Location Trigger Floor Status

Field	Description
Building Number	Number that identifies the building that was searched for the device.
Floor Number	Number that identifies the floor of the building that was searched for the device.
Device Found	Indicates whether the device was found on the selected floor.
Number of Detecting APs	Number of managed APs that detected the device.
Solution Type	Indicates whether the probability map is a circle around the managed AP (Circle), or the solution is an X,Y coordinate (Point Solution).
X-Coordinate	Identifies the X axis offset of the managed AP from some arbitrary 0,0 point on the building floor.
Y-Coordinate	Identifies the Y axis offset of the managed AP from some arbitrary 0,0 point on the building floor.
Circle Radius	For the Circle solution this parameter represents the radius from the X,Y coordinate where the device is most likely to be located. For the Point solution this value is not applicable and is set to 0.
Sigma	The standard deviation for the location. The parameter is applicable to Circle and Point solutions. For the Circle solution the Sigma represents the offset from "Circle Radius". For the Point solution the sigma represents the radius from the X,Y coordinate.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

AP Triangulation Location

The Wireless System continually collects detected signal information about APs and records the data in the AP triangulation table. The Cluster Controller periodically iterates through the triangulation tables for all APs in the RF-Scan table and computes the location for each device. The pages available from the **AP Triangulation Location** link provide device location information derived from the AP triangulation tables.

AP Triangulation Summary

Use the **AP Triangulation Summary** page to view a summary of device location information that the Cluster Control computes based on the data in the AP triangulation table. Click the MAC address of a device to view additional location information about the device.

Summary Detail

AP Triangulation Summary

All Located

Device MAC Address	Device Type	Building / Floor Number	Detected XY Coordinate(Meters)	Status
00:05:5e:56:26:a0	Detected AP	0/0	0, 0	Failure
00:10:18:33:fc:00	Detected AP	1/2	35, 45	Success
00:10:18:33:fc:10	Detected AP	1/2	35, 45	Success
00:10:18:33:fc:80	Detected AP	0/0	0, 0	Failure
00:10:18:33:fc:83	Detected AP	0/0	0, 0	Failure
00:10:18:33:fc:8e	Detected AP	0/0	0, 0	Failure
00:10:18:33:fd:50	Detected AP	1/2	35, 45	Success
00:10:18:55:fb:c0	Detected AP	0/0	0, 0	Failure
00:10:18:55:fb:d0	Detected AP	1/2	41, 78	Success
00:10:18:55:fc:00	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:c1	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:c2	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:c3	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:c4	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:c5	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:c6	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:c7	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:c8	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:c9	Detected AP	0/0	0, 0	Failure
00:10:18:55:fc:ca	Detected AP	0/0	0, 0	Failure

1 2 3 4 5 6 7 8 9 10 Next

Refresh

Figure 416: AP Triangulation Summary

The following table shows the fields available on the **AP Triangulation Summary** page.

Table 379: AP Triangulation Summary

Field	Description
Device MAC Address	MAC address of the AP
Device Type	Indicates whether the device is a Managed AP or a Detected AP. If the type of device changes, the change might not be reflected until the device location is next computed.
Building/Floor Number	Number that identifies the building and floor where the device is detected. A value of 0 indicates that no data is available.
Detected XY Coordinate	Identifies the X and Y axis offsets of the AP from some arbitrary 0,0 point on the building floor.
Status	The status of the last iteration of the location computation algorithm: <ul style="list-style-type: none"> • Not Executed • Success • Failure

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Detailed AP Triangulation Status

Use the **AP Triangulation Status** page to view detailed triangulation and location information about a detected or managed AP. To view detailed triangulation information for a specific AP, select its MAC address from the available menu.

The screenshot shows the 'AP Triangulation Status' page. At the top, there are two tabs: 'Summary' and 'Detail'. Below the tabs is a dropdown menu showing the MAC address '00:10:18:33:FC:00'. Below the dropdown is a table with the following data:

Location Data	Present	Device Type	Detected AP
Location Computation Status	Success	Last Successful Computation	0d:00:00:20
Building Number	1	Floor Number	2
Detected X-Coordinate(Meters)	35	Detected Y-Coordinate(Meters)	45

At the bottom of the table is a 'Refresh' button.

Figure 417: Detailed AP Triangulation Status

The following table shows the fields available on the **Detailed AP Triangulation Status** page.

Table 380: Detailed AP Triangulation Status

Field	Description
MAC Address Selector	The menu contains the MAC address of each AP listed on the summary page.
Location Data	Indicates whether location data is available for the AP.
Device Type	Indicates whether the device is a Managed AP or a Detected AP. If the type of device changes, the change might not be reflected until the device location is next computed.
Location Computation Status	The status of the last iteration of the location computation algorithm: <ul style="list-style-type: none"> • Not Executed • Success • Failure
Last Successful Computation	Amount of time in days, hours, minutes, and seconds that has passed since the triangulation information was last computed successfully.
Building Number	Number that identifies the building where the device is detected. A value of 0 indicates that no data is available.
Floor Number	Number that identifies the floor where the device is detected. A value of 0 indicates that no data is available.
Detected X Coordinate	Identifies the X axis offsets of the AP from some arbitrary 0,0 point on the building floor. A value of 0 indicates that no data is available.
Detected Y Coordinate	Identifies the Y axis offsets of the AP from some arbitrary 0,0 point on the building floor. A value of 0 indicates that no data is available.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Client Triangulation Location

The Wireless System continually collects detected signal information about wireless clients and records the data in the Client triangulation tables. The Cluster Controller periodically iterates through the triangulation tables for all clients in the Detected Clients table and computes the location for each device. Use the pages available from the **Client Triangulation Location** link to view device location information derived from the Client triangulation table.

Client Triangulation Summary

Use the **Client Triangulation Summary** page to view a summary of device location information that the Cluster Control computes based on the data in the Client triangulation table. Click the MAC address of a device to view additional location information about the device.

Summary Detail

Client Triangulation Summary

All Located

Device MAC Address	Device Type	Building / Floor Number	Detected XY Coordinate(Meters)	Status
00-01-36-54-3b-f4	Detected Client	0/0	0, 0	Failure
00-10-18-96-3e-d4	Detected Client	0/0	0, 0	Failure
00-11-50-e2-ba-5a	Detected Client	0/0	0, 0	Failure
00-12-f0-e5-61-b5	Detected Client	1/2	35, 45	Success
00-13-02-5c-21-f0	Detected Client	0/0	0, 0	Failure
00-13-46-0e-25-6d	Detected Client	0/0	0, 0	Failure
00-14-6c-59-d1-99	Detected Client	0/0	0, 0	Failure
00-14-a5-4b-05-3e	Detected Client	1/2	35, 45	Success
00-14-a5-4d-5f-87	Detected Client	0/0	0, 0	Failure
00-15-00-32-8a-30	Detected Client	0/0	0, 0	Failure
00-16-01-73-02-be	Detected Client	0/0	0, 0	Failure
00-16-01-73-07-77	Detected Client	1/2	35, 45	Success
00-16-01-73-07-b1	Detected Client	1/2	37, 52	Success
00-16-cf-12-58-ea	Detected Client	0/0	0, 0	Failure
00-16-cf-23-86-65	Detected Client	1/2	35, 45	Success
00-16-cf-bd-29-25	Detected Client	0/0	0, 0	Failure
00-17-ca-89-0a-80	Detected Client	0/0	0, 0	Failure
00-19-7d-1a-f1-94	Detected Client	0/0	0, 0	Failure
00-19-7d-28-1d-11	Detected Client	1/2	35, 45	Success
00-19-7e-44-c3-4d	Detected Client	0/0	0, 0	Failure

1 2 3 4 5 6 7 8 9 10 Next

Refresh

Figure 418: Client Triangulation Summary

The following table shows the fields available on the **Client Triangulation Summary** page.

Table 381: Client Triangulation Summary

Field	Description
Device MAC Address	MAC address of the wireless client.
Device Type	Indicates whether the device is an Associated Client or a Detected Client. If the type of device changes, the change might not be reflected until the device location is next computed.
Building/Floor Number	Number that identifies the building and floor where the device is detected. A value of 0 indicates that no data is available.
Detected XY Coordinate	Identifies the X and Y axis offsets of the wireless client from some arbitrary 0,0 point on the building floor.
Status	The status of the last iteration of the location computation algorithm: <ul style="list-style-type: none"> • Not Executed • Success • Failure

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Detailed AP Triangulation Status

Use the **Client Triangulation Status** page to view detailed triangulation and location information about a detected or managed wireless client. To view detailed triangulation information for a specific client, select its MAC address from the available menu.

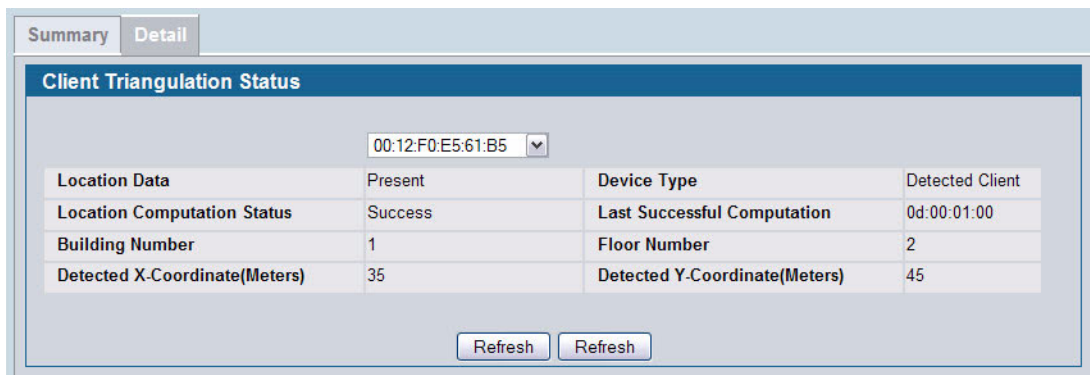


Figure 419: Detailed Client Triangulation Status

The following table shows the fields available on the **Detailed Client Triangulation Status** page.

Table 382: Detailed Client Triangulation Status

Field	Description
MAC Address Selector	The menu contains the MAC address of each wireless client listed on the summary page.
Location Data	Indicates whether location data is available for the client.
Device Type	Indicates whether the device is a Associated Client or a Detected Client. If the type of device changes, the change might not be reflected until the device location is next computed.
Location Computation Status	The status of the last iteration of the location computation algorithm: <ul style="list-style-type: none"> • Not Executed • Success • Failure
Last Successful Computation	Amount of time in days, hours, minutes, and seconds that has passed since the triangulation information was last computed successfully.
Building Number	Number that identifies the building where the device is detected. A value of 0 indicates that no data is available.
Floor Number	Number that identifies the floor where the device is detected. A value of 0 indicates that no data is available.
Detected X Coordinate	Identifies the X axis offsets of the client from some arbitrary 0,0 point on the building floor. A value of 0 indicates that no data is available.
Detected Y Coordinate	Identifies the Y axis offsets of the client from some arbitrary 0,0 point on the building floor. A value of 0 indicates that no data is available.

Command Buttons

The page includes the following button:

- **Refresh**—Updates the page with the latest information.

Visualizing the Wireless Network

The WLAN Visualization component is an optional feature that graphically shows information about the wireless network. WLAN Visualization uses a Java applet to display switches, APs, and associated wireless clients. The WLAN Visualization tool can help you visualize where the APs and clients are in relationship to the building.

This section contains the following subsections to help you manage the WLAN Visualization component of the D-Link Unified Switch:

- [WLAN Visualization Overview](#)
- [Importing and Configuring a Background Image](#)
- [Setting Up the Graph](#)
- [Checking the Location of an AP or Client](#)
- [Understanding the Menu Options and Icons](#)
- [Viewing Component Information](#)

WLAN Visualization Overview

Figure 420 shows an example of a floor plan with a DWS-4000 Series switch that has three managed APs. The figure also shows a peer switch, a rogue AP and client, and several unknown APs. The Device Location feature has been triggered and has located the probable location of a device.

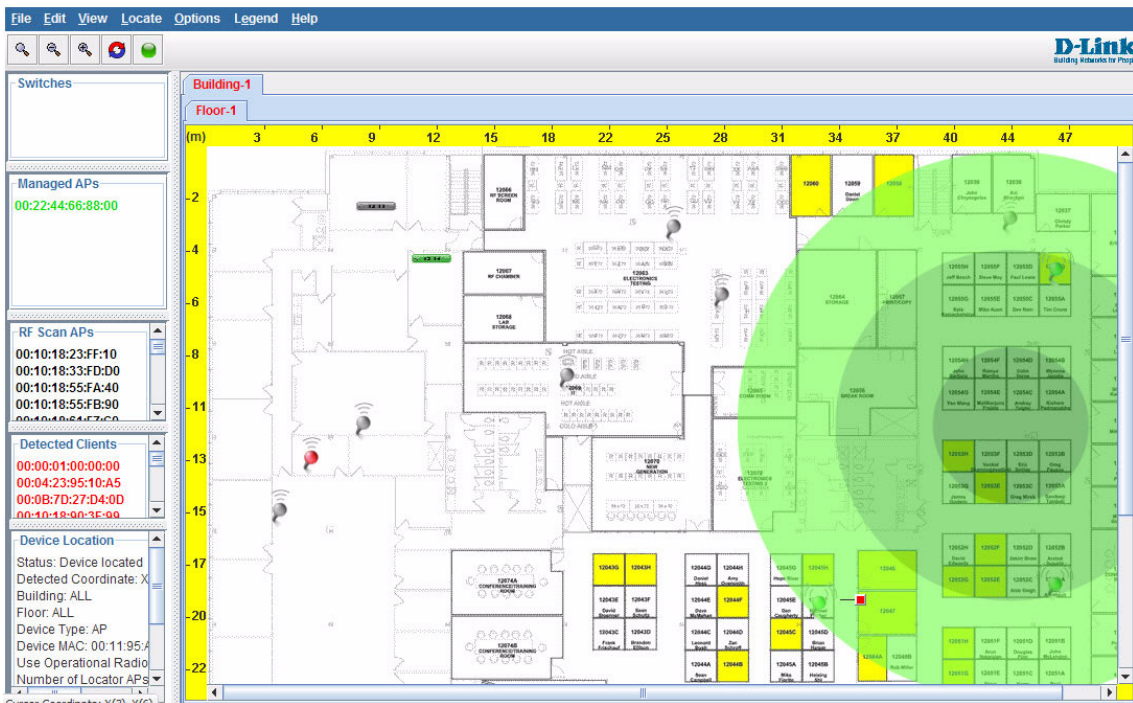


Figure 420: Sample WLAN Visualization



Note: You can launch the WLAN Visualization tool only from the cluster controller.

You can upload one or more custom images to create a background for the graph. Then, you can use the Device Locator feature to check the location of wireless devices and provide the approximate location of the device on the graph. Another option is to manually graph the components by dragging the MAC address of the discovered device from the left side of the window, which contains ungraphed components, to its location on the graph.

Right-clicking an object on the WLAN Visualization graph provides access to information about the object and provides one or more links to configuration pages on the Web interface. The goal of WLAN Visualization is to help provide a realistic representation of your wireless network and allow you to have real-time access to information about discovered devices.

Importing and Configuring a Background Image

By default, the WLAN Visualization graph does not have a background image. You can upload one or more images, such as your office floor plan, to provide a site context and site related information. You can upload up to 16 images with a total size limit of 1 MB.

Images that you upload should be in one of the following two file formats:

- GIF (Graphics Interchange Format)
- JPG (Joint Photographic Experts Group)

Additionally, D-Link recommends that you do not use color images since the WLAN components might not show up as well.

To load an image onto the switch to use as a background for the WLAN Visualization graph, use the following procedures:

1. Click **WLAN Visualization > Download Image**.
2. Click Browse to navigate to the file location.
3. Select the file to upload and click **Start File Transfer**.

Download File To Switch

Image File Selection:

Note: Supported image file types are GIF and JPG. You are encouraged to limit the use of colors as this will improve WLAN component visibility.

Once you upload an image file and save the running configuration, the image remains on the switch and you can assign it to an existing graph using the WLAN Visualization application.

Setting Up the Graph

To start the WLAN Visualization tool, click **WLAN Visualization > Launch...** This opens a new browser window and starts the Java applet.



Note: Your browser must allow pop-up windows to open from the switch.

The first time you launch the WLAN Visualization tool, there is no background image, and all discovered WLAN components are ungraphed. The screen is split into two panes. The left pane has four container views that are used to hold un-graphed components. The right pane is an area where graph definitions are shown. This graph pane is initially blank and must be defined before WLAN components can be placed.

Creating a New Graph

You can create a graph for each floor of each building within the wireless system. Graphs can be created and edited only when Live Visualization is disabled. To disable Live Visualization, click the Live Visualization control button so that it flashes red.

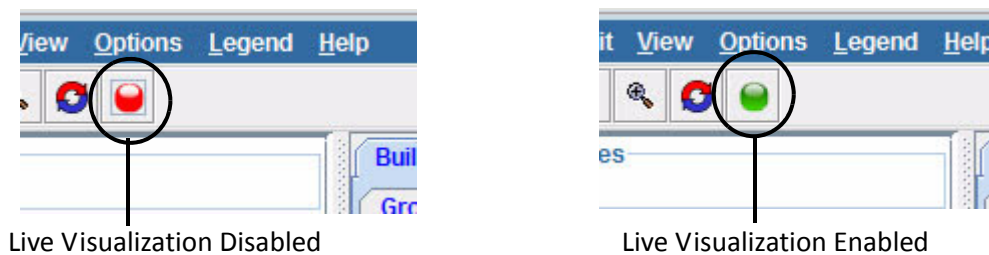


Figure 421: Live Visualization Control

To create a new graph and load the background image, launch the WLAN Visualization tool and use the following steps.

1. Ensure that Live Visualization is disabled (red).
2. From the WLAN Visualization menu bar, click **Edit > New Graph**.
The New Graph Definition dialogue box opens.
3. Enter a name to identify the building and floor, and select the appropriate numbers for the building and floor.
4. Select the image to use as the background.
For information about how to upload an image to use as a graph background, see [“Importing and Configuring a Background Image”](#) on page 651

5. Enter the represented length for one of the graph dimensions (height or width).

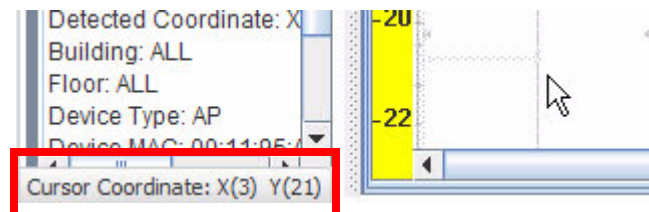
Use the Selection and Measurement drop-down menus to specify whether the length is the height or width, and whether it is in meters or feet. You must use the same unit of measurement for all floors within the building.

The length you enter determines the scale of the background image in relation to the network components. The scale of the background image affects the way the WLAN Visualization tool presents the radio frequency (RF) coverage of the access points, so it is important to be as accurate as possible when you specify the length.

6. Click **Save**.

The WLAN Visualization window refreshes and displays the background image and a yellow ruler along the top and left side. The ruler information is based on the height and width settings specified when defining the graph.

When you move your mouse over the graph, the cursor location is shown in the bottom-left side of the window.



Manually Graphing the Components

You must manually place each Unified Switch on the graph because the switch does not contain any radios. Click the IP address of the switch in the Switches window for ungraphed components and drag it to its approximate location on the graph. When you release the mouse button, an icon that represents the switch appears on the graph.

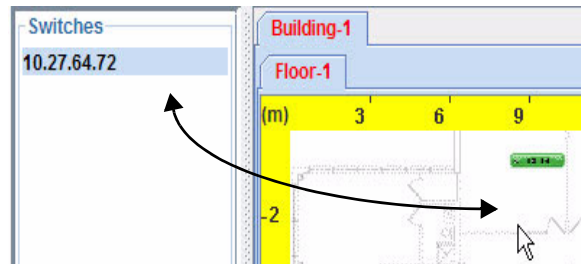


Figure 422: Graphing a Switch

For Managed APs, RF Scan APs, and detected clients, you can manually drag-and-drop each device to its approximate location on the graph, or you can use the Device Locator feature to determine the probable location.

To remove a component from the graph, right-click the component and select **Edit > Un-Graph**. The component returns to the appropriate window in the ungraphed components area.

Checking the Location of an AP or Client

To trigger the On-Demand Location search for a specific device that is located on the graph, right-click the device and select the **Command > Check Location** option. To find the location of an ungraphed device, right-click the MAC address of the device and select the **Command > Check Location** option. You can also use the **Locate > Target Access Point** or **Locate > Target Client** menu options to check the location of a graphed or ungraphed AP or client.

After you specify a device to locate, the On-Demand Location Trigger window appears. If you right-clicked a device or MAC address, the window is prepopulated with the appropriate information, as shown in Figure 423. If you used the **Locate** menu, select the MAC address of the device from the available menu.

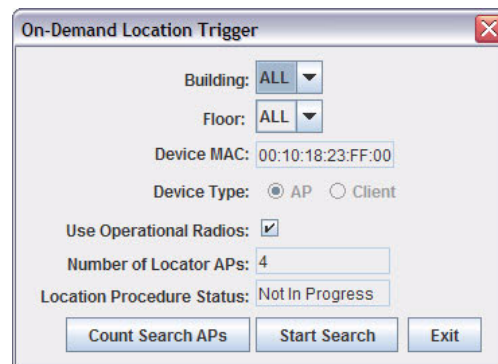


Figure 423: On-Demand Location Search Window

By default, the device search uses operational radios on managed APs use triangulation to try to determine the location of a neighboring device. Traffic for wireless clients associated with the operational radios is disrupted as they perform the search. To use sentry radios only, clear the User Operational Radios option in the On-Demand Location Trigger window.

The search window indicates the number of APs involved in the search. If you clear the Use Operational Radios option, or if additional APs become managed before the search starts, you can recalculate the number of search APs by clicking **Count Search APs**.

Click **Start Search** to initiate the device search. A pop-up window displays and asks you to confirm the search. Click **Yes** to begin the search.

After you start the search, the Device Location feature might take several minutes to locate the device. A Device Location Progress indicator tracks the amount of time, in minutes and seconds, that has passed since the search was initiated.

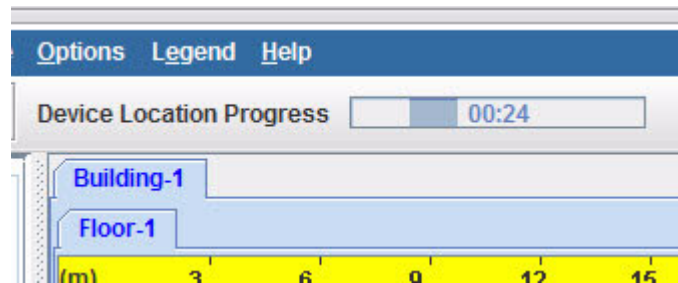


Figure 424: Device Location Progress Timer

The WLAN Visualization feature also includes a Device Location status window that displays information about the search.



Figure 425: Device Location Status

When the device has been located, a location map appears on the map to indicate the probable location of the device. The location map is either a point solution or a circle solution.

The point solution map is shaped as a circle centered on the XY coordinates of the device location. The map is scaled according to the calculated Sigma solution value. The map circle contains shaded colors where the darkest color (center) indicates the greatest probability of the device located. [Figure 426](#) shows an example of a point solution map for a located device.

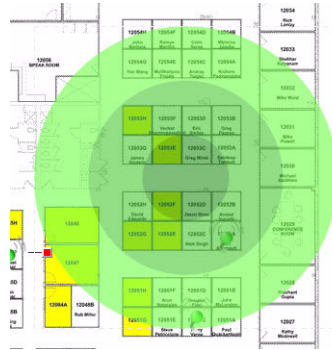


Figure 426: Probable Device Location – Point Solution

Right-click within the target area to access information and commands associated with the located device:

- The Attributes menu identifies the MAC address of the device and its detected XY coordinates.
- The Solution menu provides a textual summary of the device location results.
- The Commands menu provides access to the following actions:
 - To remove the point solution map from the graph, select **Clear this device location icon**.
 - To move the located device from the ungraphed component list or another point on the graph to its detected probable location, select **Graph device to this location**.
 - To move the located device to the cursor coordinates, position the mouse pointer in the desired location on the map and select **Graph located device to the current cursor position**.

The circle solution map is shaped as a circle centered on the XY coordinates of the device location. The map is sized according to the calculated Radius and Sigma solution values. The map circle contains shaded colors where the darkest color indicates the greatest probability of the device located. That the darkest colored ring is not the center of the circle but rather within the middle radius ring. [Figure 427](#) shows an example of a circle solution map for a located device.

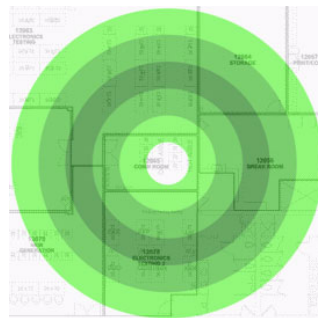


Figure 427: Probable Device Location – Circle Solution

If the locator APs are not able to determine the location of a device, the Device Location status indicates that the device is not located. A device might not be found if, for example, the search APs are unable to triangulate on the target device. The ability to locate a device and the search radius of the probable location are dependent, in part, on the location of the locator APs in relation to each other and to the device to be found.

If a device is located, but it is outside of the graph boundaries, a green arrow appears on the perimeter of the graph. Right-click the arrow to view information about the coordinates of the located device.

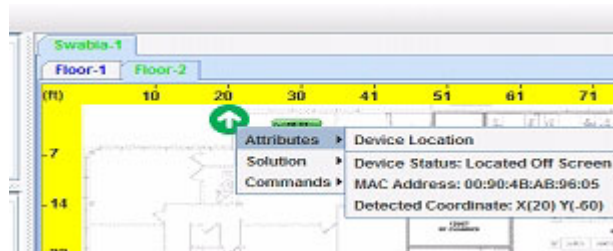


Figure 428: Probable Device Location – Off Screen

Understanding the Menu Options and Icons

The following table provides an overview of the menu items available in the WLAN Visualization tool.

Table 383: WLAN Visualization Menu Bar Options

Menu Item	Description
File	
Force Refresh	Resynchronizes the Java client application. If you edit the graph, you can force a refresh to manually update the view.
Reconnect and Refresh	Disconnects the client application from the switch and re-connects it.
Exit	Exits the WLAN Visualization application.
Edit	
New Graph	Opens a window that allows you to create and configure a new graph, including the name, background image, and scale factor for the graph.
Edit Graph	Opens the window for an existing graph. You can change the background image or graph scale. To change the name of the graph, you must create a new graph.
Delete Graph	Deletes the active graph. When you select this item, a dialogue box appears to confirm that you want to delete the graph.
Image Management	Lists the available background images and allows you to delete any available image.

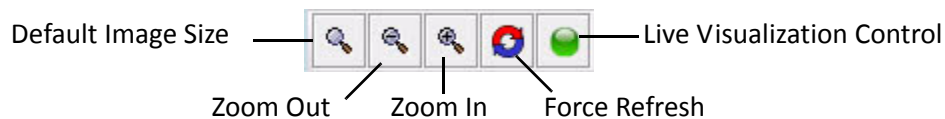
Table 383: WLAN Visualization Menu Bar Options (Cont.)

Menu Item	Description
View	
Ungraphed Components	<p>Allows you to change the view of the ungraphed components in the panel on the left:</p> <ul style="list-style-type: none"> • Tab View: Organizes the component windows and the Device Location window by tabs. One window displays at a time. • List View: Organizes all component windows and the Device Location window vertically in the left panel. This is the default view.
AP Power Display	<p>Select the power range image to display for a managed AP:</p> <ul style="list-style-type: none"> • Disable Power Display: The power range image is not displayed • 5 GHz Band: Shows the transmit power for all managed APs that have a radio operating in 802.11a or 5-GHz 802.11n mode. • 2.4 GHz Band: Shows the transmit power for all managed APs that have a radio operating in 802.11 b/g or 2.4 GHz 802.11n mode. <p>The size of the power range image is based on the transmit power for the radio, which can be low, medium, or high. The size of the power range image also depends on the actual scale factor of the current background image.</p> <p>If the AP has two radios that are configured in the same mode, two power range images are displayed.</p> <p>Note: The color of the power range image is based on the assigned channel of the associated radio.</p> <p>If two APs use the same channel (or channels that are close together) and are within each other's transmission range, the APs will interfere with each other and wireless clients will experience poor WLAN performance. To reduce interference, you can take one of the following steps:</p> <ul style="list-style-type: none"> • Reduce the transmit power on the APs. • Physically place the APs further apart. • Use the automatic channel adjustment algorithm on the APs or statically set the channels so they are non-interfering channels. <p>CAUTION: Power ranges are for illustrative purposes only. The actual power distribution varies based on factors such as office wall propagation and background RF noise.</p>
Options	
Show Managed APs	Controls whether to display AP on the graph. Clearing the check box hides but does not un-graph the objects.
Show RF Scan APs	Controls whether to display the APs detected through the RF scan. Clearing the check box hides but does not un-graph the objects.
Show Managed AP Clients	Controls whether to display wireless clients associated with managed APs. Clearing the check box hides but does not un-graph the objects.
Show Detected Clients	Controls whether to display wireless clients that have been detected by the wireless system. Clearing the check box hides but does not un-graph the objects.
Show Location Results	Display the point or circle solution on the graph. The point and circle solutions show the probable location of a device as a result of a search.

Table 383: WLAN Visualization Menu Bar Options (Cont.)

Menu Item	Description
Locate	
Target Access Point	Select this option to allow the wireless system to search for an AP and update its location based on the received search information. When you select this option, a window opens that allows you to select the MAC address of the AP to search for and to specify the location search parameters.
Target Client	Select this option to allow the wireless system to search for a client and update its location based on the received search information. When you select this option, a window opens that allows you to select the MAC address of the client to search for and to specify the location search parameters.
Legend	
Images	Shows the icons associated with each WLAN component on the graph.
Channel Color	Maps the color of the power transmission image to the channel that the radio is using for transmission.
Help	
Help	Opens a new HTML window to display the WLAN Visualization online help page.

The following figure identifies the toolbar icons directly below the menu bar.

**Figure 429: Toolbar Icons**

Legend Menu

The items in the **Legend** menu contain information about the icons and colors that appear on the graph.

The **Images** menu item shows the icons that represent the WLAN components on the graph.

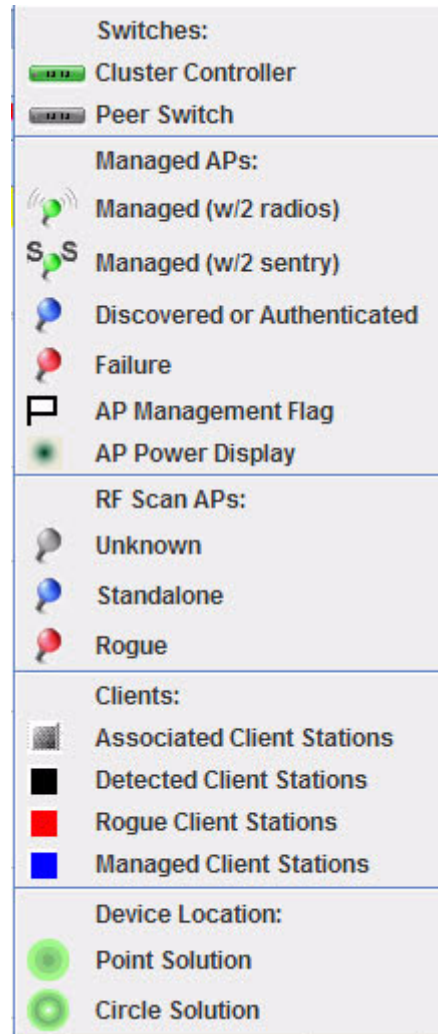


Figure 430: Legend

As the legend shows, the Managed AP icon can be blue, green, or red, depending on the status of the AP:

- Blue: The AP has been discovered and by the switch, but it is in a transitional state. The AP could be waiting to be authenticated, or it has been validated and authenticated but not configured.
- Green: The AP profile configuration has been applied to the AP, and it is operating in managed mode.
- Red: The switch has lost contact with the AP, the AP is being reset, or the AP has experienced an authentication failure.

A radio operating in Sentry Mode displays the letter “S” in place of the antenna on the AP icon, as [Figure 431](#) shows.



Figure 431: Sentry Mode—Detailed View

When the AP Power Display is enabled, radios in sentry mode show a gray AP power display image around the AP.

The Channel Color legend maps the color of the power display image to the channel that the image color represents. The color corresponds to the channel that the radio is using for transmission. The available channels depend on the mode and country of operation.

Viewing Component Information

After you place a component on the graph, you can right-click the component to learn more information about it, ungraph it, or to access a page on the Web UI to manage or monitor the component. You must be logged on to the switch for the links to be active.

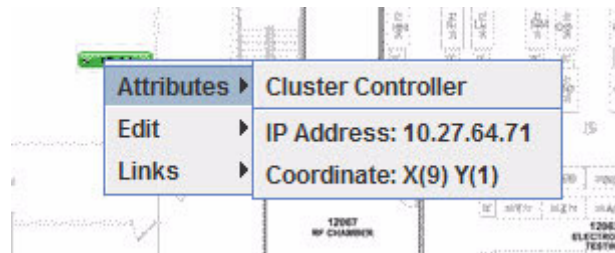


Figure 432: Wireless Component Attributes

Appendix A: Configuration Examples

This appendix contains examples of how to configure selected features available in the Unified Wired and Wireless Access System software. Each example contains procedures on how to configure the feature by using the Web interface, CLI, and SNMP.

This appendix describes how to perform the following procedures:

- [Configuring VLANs](#)
- [Configuring VLAN Routing](#)
- [Configuring Multiple Spanning Tree Protocol](#)
- [Configuring a Virtual Access Point](#)
- [Configuring Differentiated Services for VoIP](#)
- [Configuring a Network with WDS-Managed APs](#)
- [Configuring a Network to Use WPA2-Enterprise and Dynamic VLANs](#)
- [Optimizing WLAN Traffic](#)
- [Detecting and Preventing Wireless Intrusion](#)



Note: Each configuration example starts from a factory-default configuration unless otherwise noted.

Configuring VLANs

The diagram in this section shows a switch with four ports configured to handle the traffic for two VLANs. Port 0/2 handles traffic for both VLANs, while port 0/1 is a member of VLAN 2 only, and ports 0/3 and 0/4 are members of VLAN 3 only.

The following examples show how to create VLANs, assign ports to the VLANs, and assign a VLAN as the default VLAN to a port.

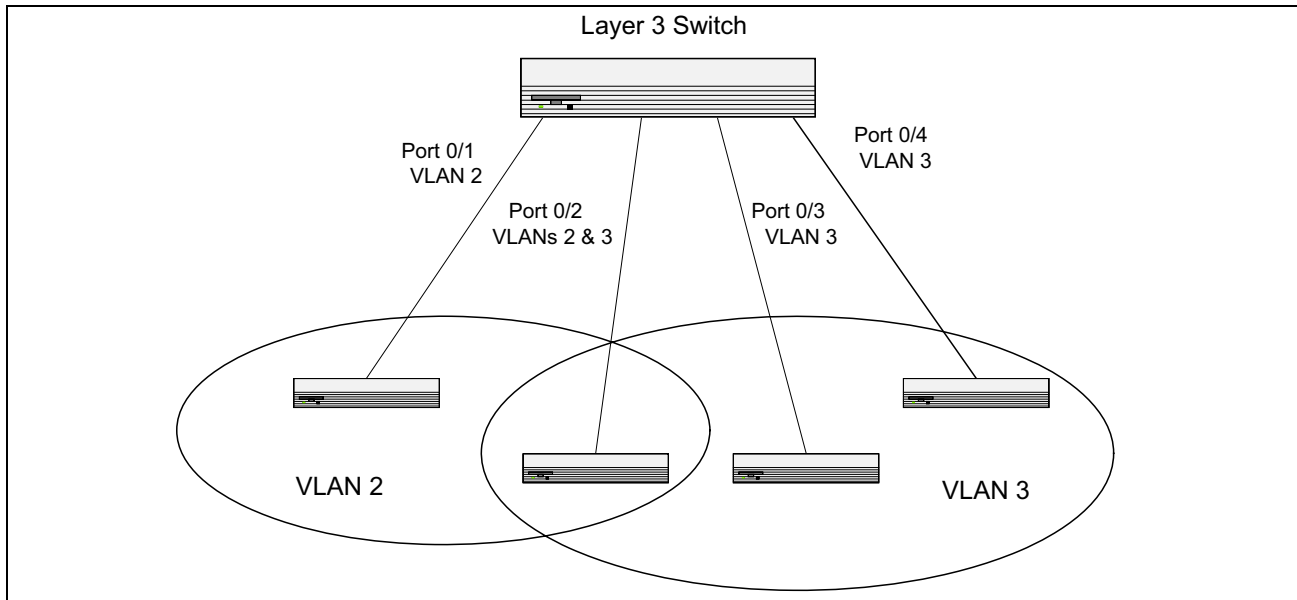
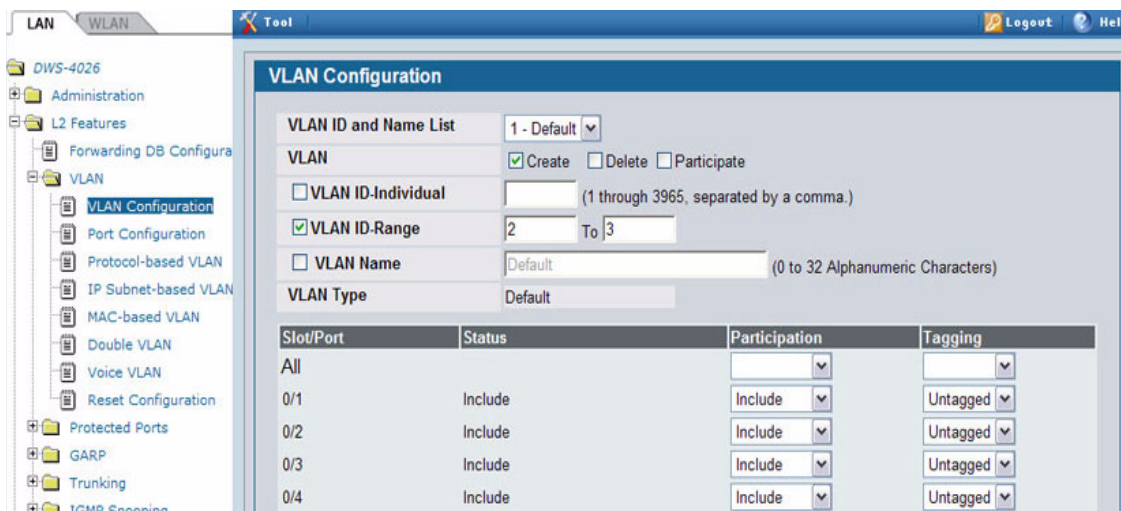


Figure 433: VLAN Example Network Diagram

1. Access the **LAN > L2 Features > VLAN > VLAN Configuration** page.
2. Select the Create option in the VLAN field.
3. Select the VLAN ID-Range option and enter 2 to 3 in the range fields.



4. Click **Submit**.
5. Select VLAN 2 from the VLAN ID and Name List.
6. Select the Participate option in the VLAN field.
7. For ports 0/1 and 0/2, select Include from the Participation menu to specify that these ports are members of VLAN 2.
8. From the Tagging menu, select Tagged in the first row (All) to specify that frames will always be transmitted

tagged from ports that are members of VLAN 2.

Slot/Port	Status	Participation	Tagging
All			Tagged
0/1	Exclude	Include	Untagged
0/2	Exclude	Include	Untagged
0/3	Exclude	Autodetect	Untagged

9. Click **Submit**.

10. Select VLAN 3 from the VLAN ID and Name List.

11. Select the Participate option in the VLAN field.

12. For ports 0/2, 0/3 and 0/4, select Include from the Participation menu to specify that these ports are members of VLAN 3.

13. Click **Submit**.

14. Go to the **LAN > L2 Features > VLAN > Port Configuration** page.

15. From the Slot/Port menu, select 0/1.

16. In the Acceptable Frame Types field, select VLAN Only to specify that untagged frames will be rejected on receipt.

17. Click **Submit**.

18. From the Slot/Port menu, select 0/2.

19. In the Port VLAN ID field, enter 3 to assign VLAN 3 as the default VLAN for the port.

20. In the Acceptable Frame Types field, select VLAN Only to specify that untagged frames will be rejected on receipt.

Slot/Port	All
Port VLAN ID	1 (1 to 3965)
Acceptable Frame Types	Admit All
Ingress Filtering	Disable
Port Priority	0 (0 to 7)

Submit

21. Click **Submit**.

Configuring Multiple Spanning Tree Protocol

This example shows how to enable IEEE 802.1s Multiple Spanning Tree (MST) protocol on the switch and all of the ports and to set the bridge priority.

To make multiple switches be part of the same MSTP region, make sure the Force Protocol Version setting for all switches is IEEE 802.1s. Also, make sure the configuration name, digest key, and revision level are the same for all switches in the region.



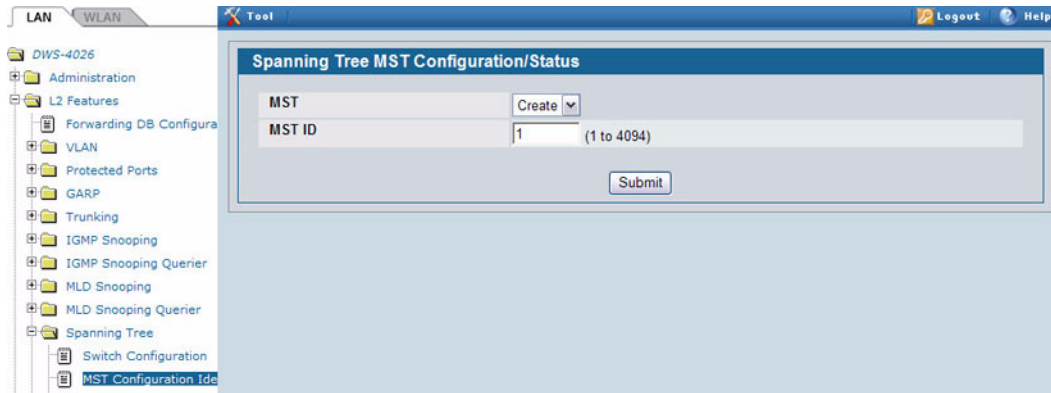
Note: The digest key is generated based on the association of VLANs to different instances. To ensure the digest key is same, the mapping of VLAN to instance must be the same on each switch in the region. For example, if VLAN 10 is associated with instance 10 on one switch, you must associate VLAN 10 and instance 10 on the other switches.

1. Create VLANs 10 and 20.
 - a. Access the **LAN > L2 Features > VLAN > VLAN Configuration** page.
 - b. Select the Create option in the VLAN field.
 - c. Select the VLAN ID-Individual option and enter 10.
 - d. Click **Submit**.
 - e. Repeat the steps to add VLAN 20.
2. Enable MSTP on the switch and change the configuration name.
3. Changing the configuration name allows all the bridges that want to be part of the same region to join.
 - a. Go to the **LAN > L2 Features > Spanning Tree > Switch Configuration/Status** page.
 - b. From the STP Mode menu, select Enable.
 - c. In the Configuration Name field, enter dlink.
 - d. Click **Submit**.

MST ID	VID	FID
CST	1 2 3	1 2 3

4. Create two MST instances.
 - a. Go to the **LAN > L2 Features > Spanning Tree > MST Configuration/Status** page.
 - b. From the MST field, select Create.
 - c. In the MST ID field, enter 10.

- d. Click **Submit**.
 - e. Repeat the steps to create an MST instance with an ID of 20.
5. Associate MST ID 10 with VLAN 10 and assign a bridge priority of 16384
- a. Select MST 10 from the MST menu.
 - b. Enter 16384 in the Bridge Priority field.
 - c. Click VLAN 10 to select it from the VLAN ID field.
 - d. Click **Submit**.



6. Use similar procedures to associate MST instance 20 to VLAN 20 and assign it a bridge priority value of 61440.
- By using a lower priority for MST 20, MST 10 becomes the root bridge.
7. Enable STP on port 0/1.
- a. Go to the **LAN > Administration > Port Configuration > Port Configuration** page.
 - b. From the Slot/Portt mode, select port 0/1.
 - c. From the STP Mode menu, select Enable.
 - d. Click **Submit**.

The screenshot shows the 'Port Configuration' page in the D-Link UWS web interface. The left sidebar contains a tree view with the following items: Administration, System Description, Switch Configuration, Card Configuration, PoE Configuration, Serial Port, IP Address, Network DHCP Client, HTTP Configuration, User Accounts, Authentication List, User Login, Denial Of Service Prot, Multiple Port Mirroring, Telnet Sessions, Outbound Telnet Client, Ping Test, Traceroute, SNMP, Port Configuration (selected), Port Description, Log, and SNMP Manager. The main content area is titled 'Port Configuration' and contains the following fields:

Slot/Port	All	
Port Type		
STP Mode	Disable	
Admin Mode	Enable	
Broadcast Storm Recovery Mode	Disable	
Broadcast Storm Recovery Level	5	percent
Multicast Storm Recovery Mode	Disable	
Multicast Storm Recovery Level	5	percent
Unicast Storm Recovery Mode	Disable	
Unicast Storm Recovery Level	5	percent
LACP Mode	Enable	
Physical Mode	Auto	
Physical Status		
Link Status		
Link Trap	Enable	
Maximum Frame Size	1518	(1518 to 9216)
ifIndex		

A 'Submit' button is located at the bottom of the form.

8. Use similar procedures to enable STP on port 0/2.
9. Force port 0/2 to be the root port for MST 20, which is the non-root bridge.
 - a. Go to the **LAN > L2 Features > Spanning Tree > MST Port Configuration/Status** page.
 - b. From the MST ID menu, select 20.
 - c. From the Slot/Port menu, select 0/2.
 - d. In the Port Priority field, enter 64.
 - e. Click **Submit**.

Configuring VLAN Routing

This section provides an example of how to configure Unified Wired and Wireless Access System software to support VLAN routing. The configuration of the VLAN router port is similar to that of a physical port. The main difference is that, after the VLAN has been created, you must use the **show ip vlan** command to determine the VLAN's interface ID so that you can use it in the router configuration commands.

The diagram in this section shows a Layer 3 switch configured for port routing. It connects two VLANs, with two ports participating in one VLAN, and one port in the other. The script shows the commands you would use to configure Unified Wired and Wireless Access System software to provide the VLAN routing support shown in the diagram.

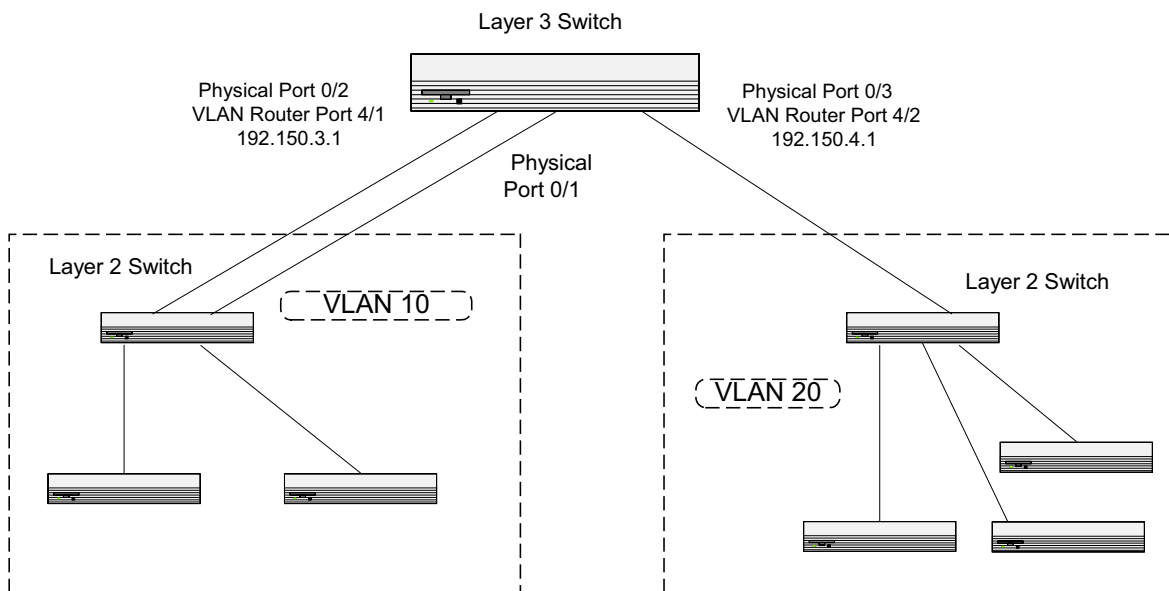
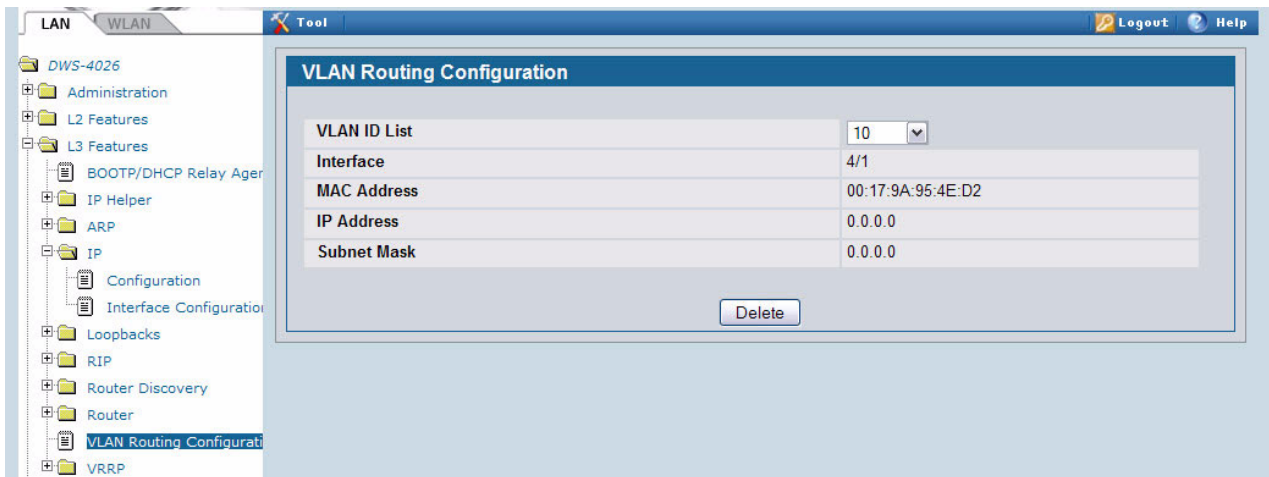


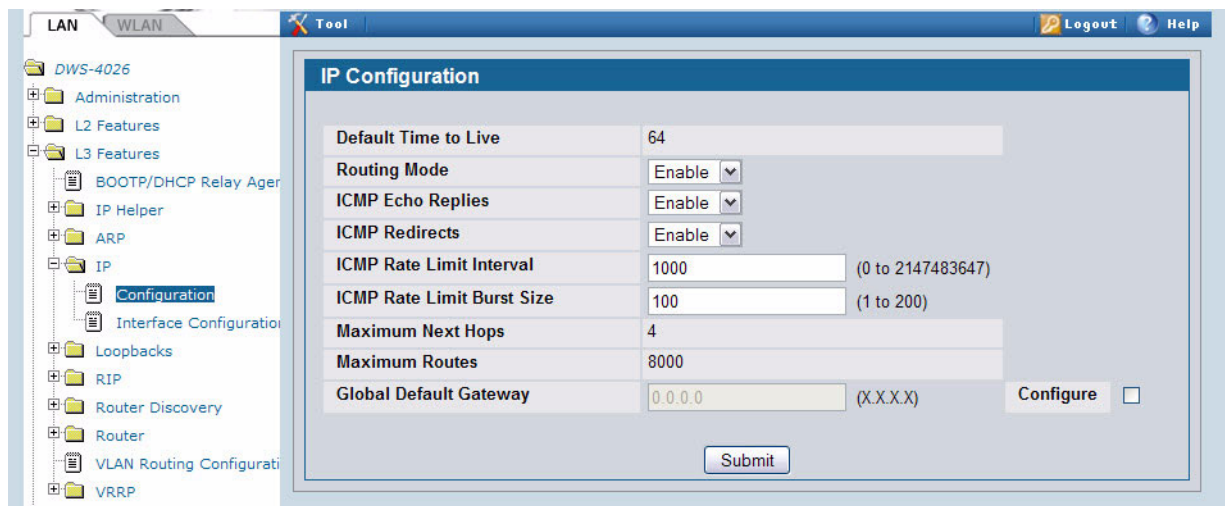
Figure 434: VLAN Routing Example Network Diagram

Use the following screens to perform the same configuration using the Web Interface:

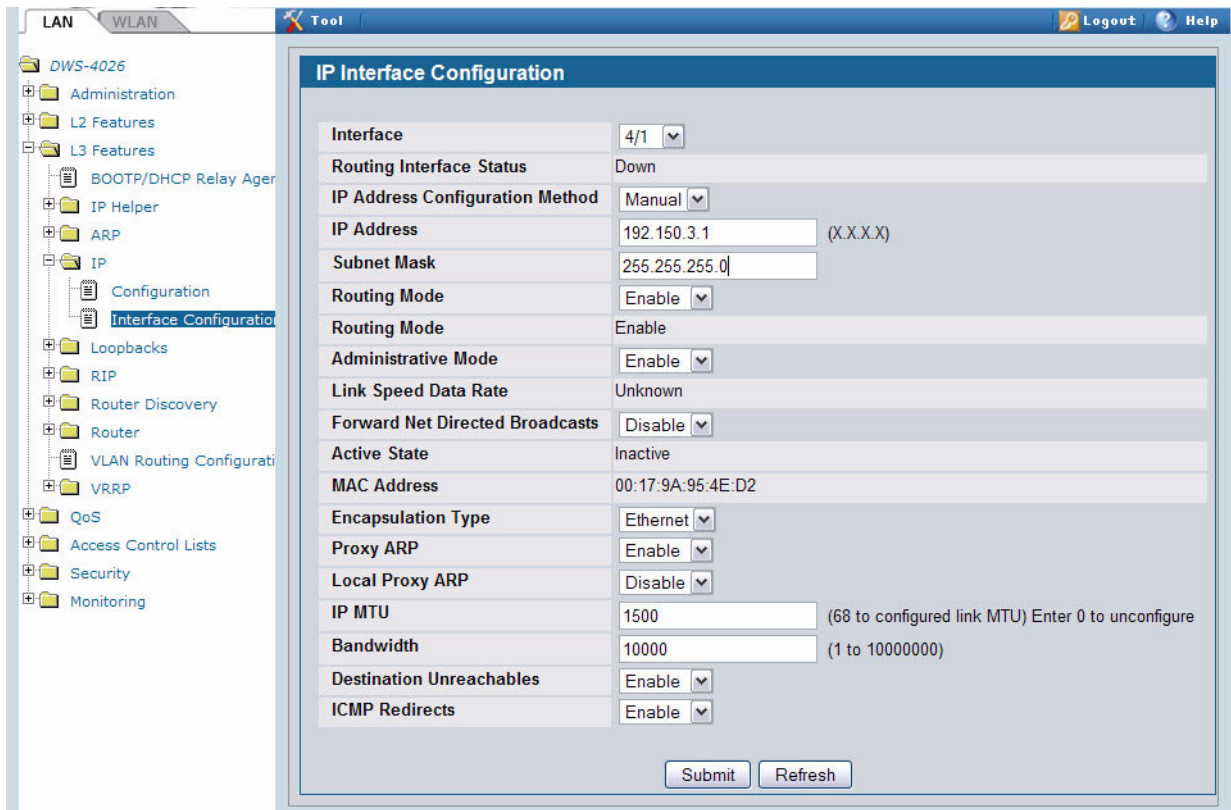
1. From the **LAN > L2 Features > VLAN > VLAN Configuration** page, perform the following configuration:
 - Create VLANs 10 and 20.
 - Include interfaces 0/1 and 0/2 as members of VLAN 10, and set tagging for all interfaces to Tagged.
 - Include interface 0/3 as a member of VLAN 20, and set tagging for all interfaces to Tagged.
2. From the **LAN > L2 Features > VLAN > Port Configuration** page, set the port VLAN ID for interfaces 0/1 and 0/2 to 10 and the port VLAN ID for interface 0/3 to 20.
3. Navigate to the **LAN > L3 Features > VLAN Routing Configuration** page.
4. Enter 10 in the VLAN ID field, and then click **Create**.



5. Note the slot/port ID assigned to the VLAN routing interface, which is 4/1 for VLAN 10 in this example.
6. Enter 20 in the VLAN ID field, and then click **Create**. Note that the VLAN is assigned an interface ID of 4/2.
7. To enable routing on the switch, go to the **LAN > L3 Features > IP > Configuration** page, select Enable from the Routing Mode menu, and click **Submit**.



8. Go to the **LAN > L3 Features > IP > Interface Configuration** page to configure the IP addresses and subnet masks for the virtual router ports.
 - a. From the Interface menu, select 4/1.
 - b. From the IP Address Configuration Method menu, select Manual.
 - c. Enter 192.150.3.1 in the IP Address field.
 - d. Enter 255.255.255.0 in the Subnet Mask field.
 - e. Click **Submit**.



The screenshot displays the 'IP Interface Configuration' page in the D-Link UWS web interface. The left sidebar shows a navigation tree with 'LAN' selected, and 'L3 Features > IP > Interface Configuration' highlighted. The main content area contains the following configuration fields:

Field	Value	Notes
Interface	4/1	
Routing Interface Status	Down	
IP Address Configuration Method	Manual	
IP Address	192.150.3.1	(X.X.X.X)
Subnet Mask	255.255.255.0	
Routing Mode	Enable	
Routing Mode	Enable	
Administrative Mode	Enable	
Link Speed Data Rate	Unknown	
Forward Net Directed Broadcasts	Disable	
Active State	Inactive	
MAC Address	00:17:9A:95:4E:D2	
Encapsulation Type	Ethernet	
Proxy ARP	Enable	
Local Proxy ARP	Disable	
IP MTU	1500	(68 to configured link MTU) Enter 0 to unconfigure
Bandwidth	10000	(1 to 10000000)
Destination Unreachables	Enable	
ICMP Redirects	Enable	

At the bottom of the form, there are 'Submit' and 'Refresh' buttons.

9. Select interface 4/2 from the Interface menu and configure it with an IP address of 192.150.4.1 and subnet mask of 255.255.255.0.

Configuring 802.1X Network Access Control

This example configures a single RADIUS server used for authentication and accounting at 10.10.10.10. The shared secret is configured to be *secret*. The process creates a new authentication list, called radiusList, which uses RADIUS as the authentication method. This authentication list is associated with the 802.1X default login. IEEE 802.1X port-based access control is enabled for the system, and interface 0/1 is configured to be in force-authorized mode because this is where the RADIUS server and protected network resources are located.

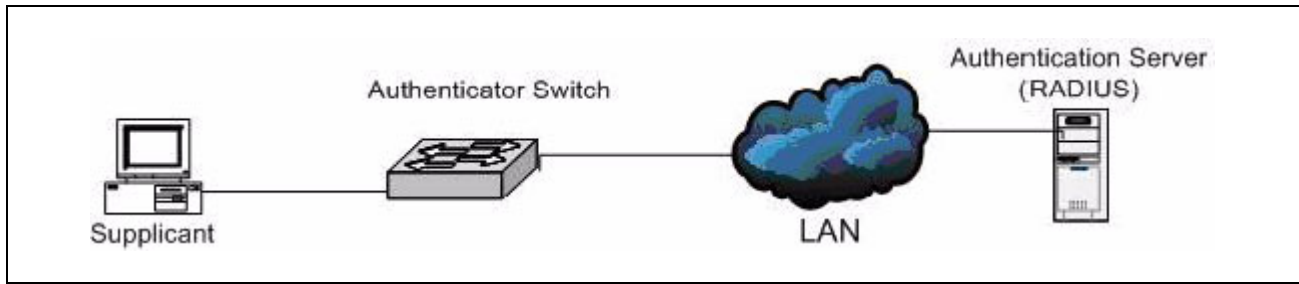
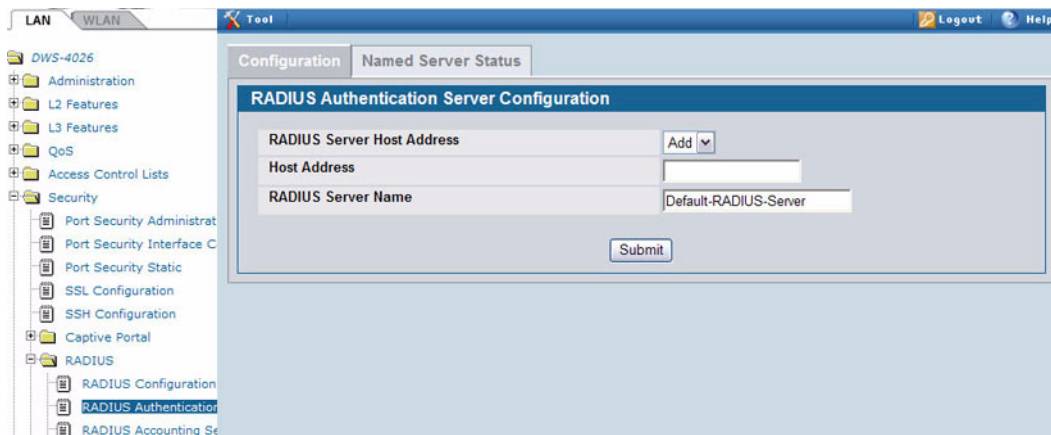


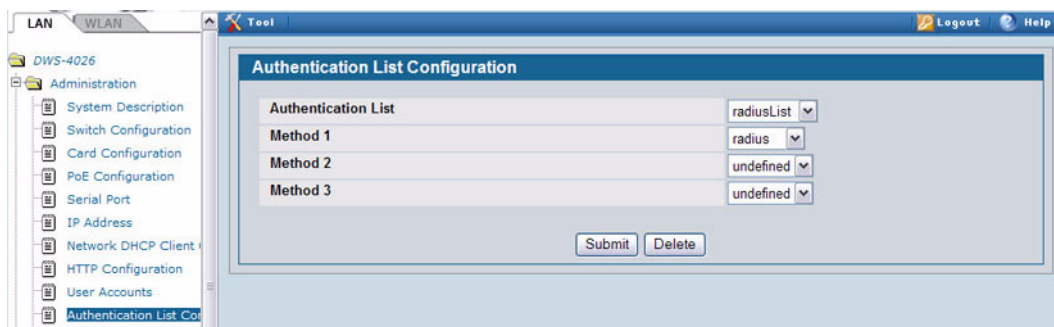
Figure 435: Switch with 802.1X Network Access Control

If a user, or supplicant, attempts to communicate via the switch on any interface except interface 0/1, the system challenges the supplicant for login credentials. The system encrypts the provided information and transmits it to the RADIUS server. If the RADIUS server grants access, the system sets the 802.1X port state of the interface to authorized, and the supplicant is able to access network resources.

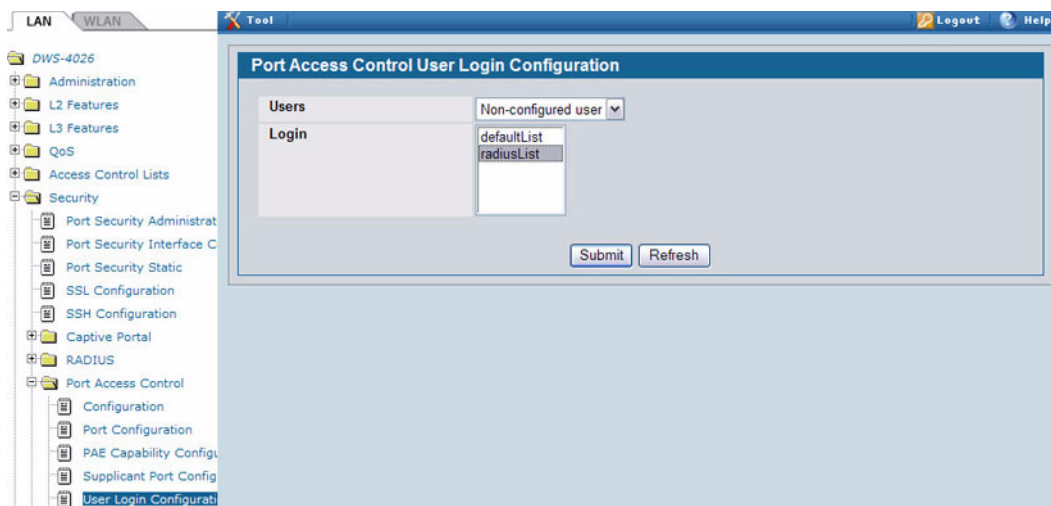
1. To configure the RADIUS Server information in the switch, go to the **LAN > Security > RADIUS > RADIUS Authentication Server Configuration** page.
2. Select Add from RADIUS Server Host Address field.
3. Enter 10.10.10.10 in the Host Address field.
4. Click **Submit**.
The page refreshes, and additional fields appear.
5. in the Secret field, enter secret and select the Apply option.
6. From the Primary Server field, select Yes.



7. Click **Submit** to apply the changes to the system.
8. Configure the RADIUS accounting server information.
 - a. Go to the **LAN > Security > RADIUS > Accounting Server** page.
 - b. Select Add from Accounting Server Host Address field.
 - c. Enter 10.10.10.10 in the Accounting Server Host Address field.
 - d. Click **Submit**.
 - e. in the Secret field, enter secret and select the Apply option.
 - f. Click **Submit**.
9. To enable the RADIUS accounting mode, go to the **LAN > Security > RADIUS > RADIUS Configuration** page, select Enable from the Accounting Mode menu, and then click **Submit**.
10. Create an authentication list.
 - a. Go to the **LAN > Administration > Authentication List Configuration** page.
 - b. Enter radiusList in the Authentication List Name field.
 - c. Click **Submit**.
 - d. Select RADIUS from the Method 1 menu, and then click **Submit**.



11. To set radiusList as the default login list for users that are not configured on the system, go to the **LAN > Security > Port Access Control > Login** page, select radiusList from the Login field, and click **Submit**.



12. To enable IEEE 802.1X authentication on the switch, go to the **LAN > Security > Port Access Control >**

Configuration page, select **Enable** from the **Administrative Mode** menu, and then click **Submit**.

13. To set the 802.1X mode for port 0/1, go to the **LAN > Security > Port Access Control > Port Configuration** page, select **Force Authorized** from the **Control Mode** field, and then click **Submit**.

Configuring a Virtual Access Point

The following example shows how to configure the default virtual access point (VAP) profile on the switch. After the switch authenticates an AP it discovers on the network, it assigns the default profile to the AP. In order for the switch and AP to discover each other, the **WLAN Switch** feature must be enabled on the UWS, and the **Managed Mode** must be enabled on the AP.

The default profile in this example has three enabled VAPs with the following settings:

Table 384: VAP Configuration Example Settings

Network (SSID)	VLAN	Security	Redirect	Client QoS
Visitor	10	None	http://www.dlink.com.tw	http://www.dlink.com.tw Bandwidth Restrictions
Corporate	20	WPA Personal	None	None
Voice	30	WPA Enterprise	None	DiffServ Policy Up

The Voice network uses the default RADIUS server configured on the system to authenticate clients and has the **L2 Distributed Tunneling Mode** enabled.



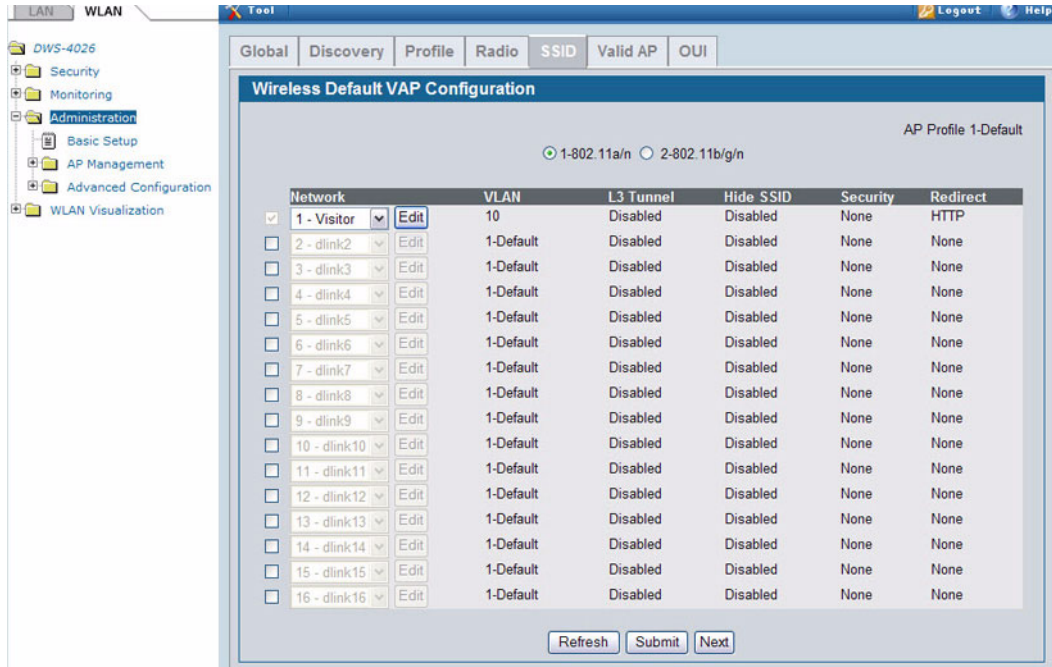
Note: When **L2 Distributed tunneling** is enabled, note the following network considerations:

- If APs are located in different subnets, the client VLANs must also be separated by a router so that the VLANs do not form a single bridge segment.
- If the IP addresses of the APs are on the same subnet, all VLANs used by the wireless clients must also be located in the same bridge segment.

The Voice network also uses a **DiffServ** policy to expedite the voice traffic. The policy must already be configured in order to associate it with the Voice network. You configure the policy by using the pages available from the **LAN > QoS > Differentiated Services** folder. For information about configuring **DiffServ** policies, see [“Configuring Differentiated Services for VoIP” on page 677](#).

1. Access the **WLAN > Administration > Basic Setup** page, and then click the **SSID** tab.
By default, **Network 1** is enabled and uses “**Guest Network**” as the **SSID**.
2. Configure the first VAP.
 - a. Click **Edit** for **Network 1** to access the **Wireless Network Configuration** page for that network.
 - b. Delete the existing **SSID** and enter **Visitor** in the **SSID** field.
 - c. In the **VLAN** field, enter **10**.
 - d. In the **Redirect** field, select the **HTTP** option.

- e. In the Redirect URL field, enter `www.dlink.com.tw`
- f. In the Bandwidth Limit Down field, enter `3000000` to limit the download speed to 3 Mbps for the VAP.
- g. In the Bandwidth Limit Up field, enter `100000` to limit the upload speed to 1 Mbps for the VAP.
- h. Click **Submit** to apply the settings to the switch.



3. Click the **SSID** tab to return to the **Wireless Default VAP Configuration** page.
4. Select the check box next to network 2, and then click **Edit**.
5. Configure the second VAP.
 - a. Delete the existing SSID and enter Corporate in the SSID field.
 - b. In the VLAN field, enter 20.
 - c. From the Security option, select WPA.
Additional security fields appear.
 - d. Clear the WPA option so that only WPA2 clients can connect to the VAP.
 - e. Select the CCMP (AES) option.
 - f. Enter a WPA Key.
 - g. Click **Submit**.
6. Click the **VAP** tab to return to the **Wireless Default VAP Configuration** page.
7. Select the check box next to network 3, and then click **Edit**.

Network	VLAN	L3 Tunnel	Hide SSID	Security	Redirect
<input checked="" type="checkbox"/> 1 - Visitor Edit	10	Disabled	Disabled	None	HTTP
<input type="checkbox"/> 2 - dlink2 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 3 - dlink3 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 4 - dlink4 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 5 - dlink5 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 6 - dlink6 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 7 - dlink7 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 8 - dlink8 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 9 - dlink9 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 10 - dlink10 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 11 - dlink11 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 12 - dlink12 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 13 - dlink13 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 14 - dlink14 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 15 - dlink15 Edit	1-Default	Disabled	Disabled	None	None
<input type="checkbox"/> 16 - dlink16 Edit	1-Default	Disabled	Disabled	None	None

8. Configure the third VAP.



Note: Because this VAP uses WPA Enterprise, wireless clients must authenticate by using an external RADIUS server. Make sure that the RADIUS Authentication Server Configured field shows the status as Configured. For more information about configuring the RADIUS server, see the steps that pertain to setting up the RADIUS server in [“Configuring 802.1X Network Access Control”](#) on page 671.

- a. Delete the existing SSID and enter Voice in the SSID field.
- b. In the VLAN field, enter 30.
- c. From the Security option, select WPA.
Additional security fields appear.
- d. Clear the WPA option so that only WPA2 clients can connect to the VAP.
- e. Select WPA Enterprise
- f. Select the CCMP (AES) option.
- g. From the L2 Distributed Tunneling Mode field, select Enable to allow the clients to roam among APs in different subnets without losing their network connection.
- h. From the DiffServ Policy UP field, select the policy to apply to traffic transmitted from wireless clients to the AP.
- i. Click **Submit**.

The screenshot displays the 'Wireless Network Configuration' page in the D-Link UWS management interface. The left-hand navigation pane shows a tree structure with 'WLAN' selected, containing sub-items like 'Basic Setup', 'AP Management', 'Advanced Configuration', and 'WLAN Visualization'. The main configuration area is titled 'Wireless Network Configuration' and includes the following settings:

SSID	Voice
Hide SSID	<input type="checkbox"/>
Ignore Broadcast	<input type="checkbox"/>
VLAN	30 (1 to 4094)
L3 Tunnel	<input type="checkbox"/>
L3 Tunnel Status	None
L3 Tunnel Subnet	0.0.0.0
L3 Tunnel Mask	255.255.255.0
MAC Authentication	<input type="radio"/> Local <input type="radio"/> RADIUS <input checked="" type="radio"/> Disable
Redirect	<input type="radio"/> None <input checked="" type="radio"/> HTTP
Redirect URL	www.broadcom.ct
Wireless ARP Suppression Mode	Disable
L2 Distributed Tunneling Mode	Enable
RADIUS Authentication Server Name	
RADIUS Authentication Server Name	Default-RADIUS-Server
RADIUS Authentication Server Status	Not Configured
RADIUS Accounting Server Name	
RADIUS Accounting Server Name	Default-RADIUS-Server
RADIUS Accounting Server Status	Not Configured
RADIUS Use Network Configuration	Enable
RADIUS Accounting	<input type="checkbox"/>
Security	
<input type="radio"/> None <input type="radio"/> WEP <input checked="" type="radio"/> WPA/WPA2	
<input type="radio"/> WPA Personal <input checked="" type="radio"/> WPA Enterprise	
WPA Versions	
<input type="checkbox"/> WPA <input checked="" type="checkbox"/> WPA2	

Configuring Differentiated Services for VoIP

One of the most valuable uses of DiffServ is to support Voice over IP (VoIP). VoIP traffic is inherently time-sensitive: for a network to provide acceptable service, a guaranteed transmission rate is vital. This example shows one way to provide the necessary quality of service: how to set up a class for UDP traffic, have that traffic marked on the inbound side, and then expedite the traffic on the outbound side. The configuration script is for Router 1 in the accompanying diagram: a similar script should be applied to Router 2.

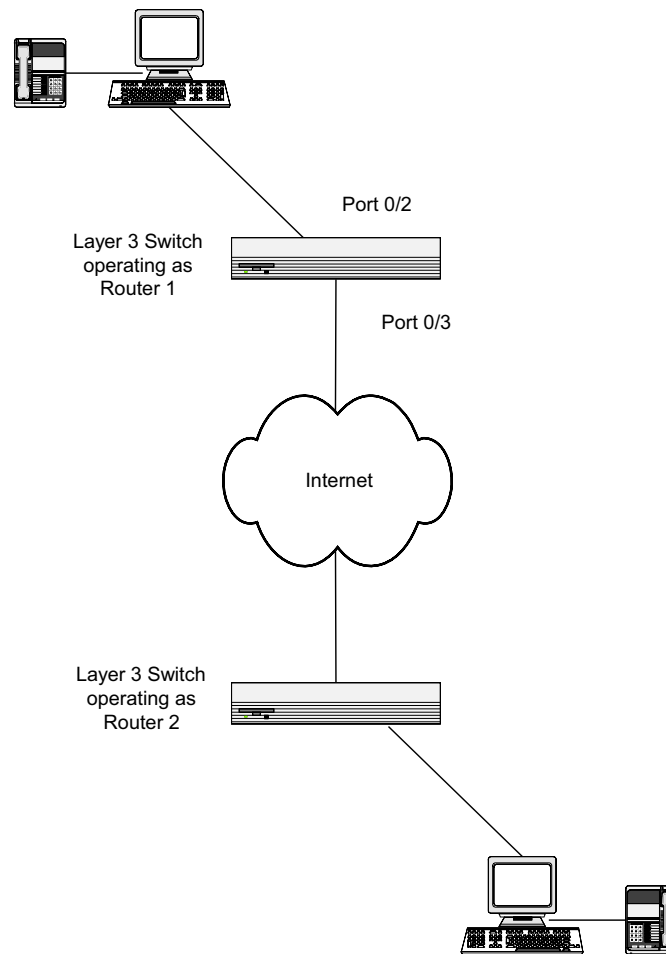
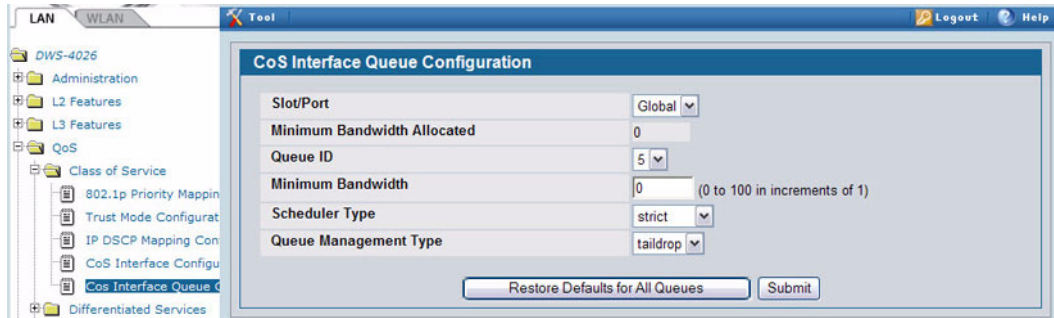
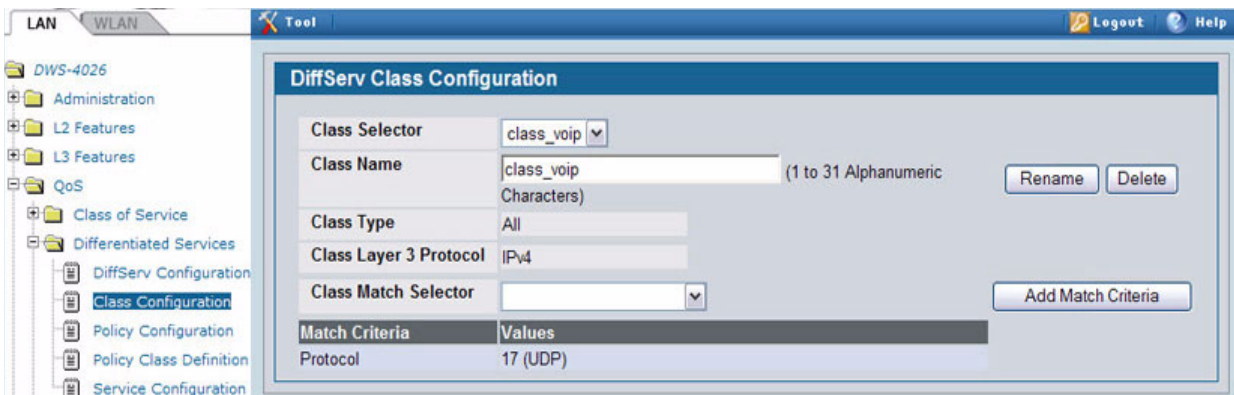


Figure 436: DiffServ VoIP Example Network Diagram

1. To set queue 5 on all ports to use strict priority mode, go to the **LAN > QoS > Class of Service > CoS Interface Queue Configuration** page and configure the following settings:
 - Slot/Port: Global
 - Queue ID: 5
 - Scheduler Type: Strict
2. Click **Submit**.
Queue 5 will be used for all VoIP packets.

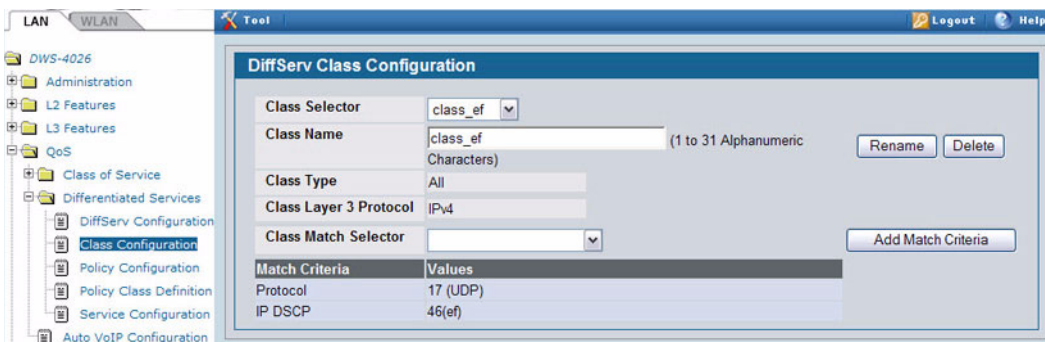


3. Go to the **LAN > QoS > Differentiated Services > DiffServ Configuration** page and enable DiffServ for the switch.
4. Go to the **LAN > QoS > Differentiated Services > Class Configuration** page, select Create from the Class Selector field, enter class_voip in the Class Name field, select All as the Class Type, and then click **Submit**.
5. Select IPv4 as the Class Layer 3 Protocol, and then click **Submit**.
6. Select Protocol from the Class Match Selector menu, and then click **Add Match Criteria**.
7. Select UDP from the Protocol Keyword menu, and then click **Submit**.



8. Create a second DiffServ classifier named class_ef and define a single match criterion to detect a DiffServ code point (DSCP) of ef (expedited forwarding).

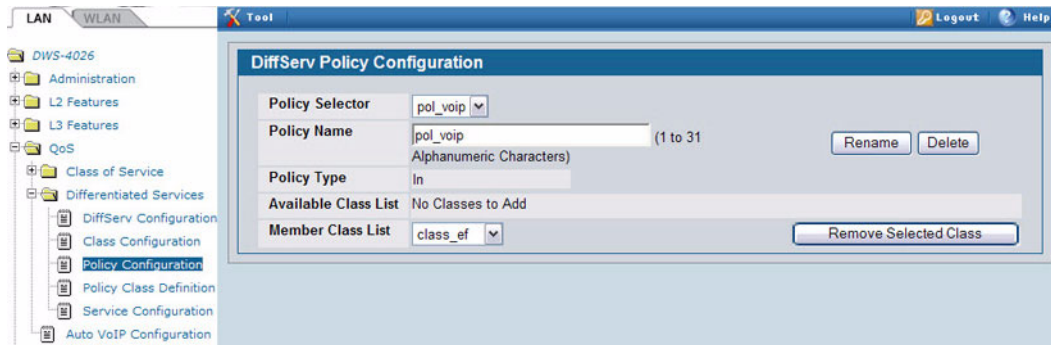
This handles incoming traffic that was previously marked as expedited elsewhere in the network.



9. Go to the **Policy Configuration** page, select Create from the Policy Selector menu, enter pol_voip in the Policy Name field, and then click **Submit**.

10. From the Available Class List menu, select class_voip, and then click **Add Selected Class**.

11. From the Available Class List menu, select class_ef, and then click **Add Selected Class**.



12. Go to the **Policy Class Definition** page and configure how classes that match the policy are handled.

The following steps configure this policy so that incoming packets already marked with a DSCP value of "EF" (per the class_ef definition), or marks UDP packets (per the class_voip definition) with a DSCP value of "EF." In both cases, the matching packets are assigned internally to use queue 5 of the egress port to which they are forwarded.

- Select pol_voip from the Policy Selector menu, class_ef from the Member Class List menu, and Assign Queue from the Policy Attribute Selector, and then click **Configure Selected Attribute**.
- In the Queue ID Value field, enter 5, and then click **Submit**.
- Select pol_voip from the Policy Selector menu, class_voip from the Member Class List menu, and Assign Queue from the Policy Attribute Selector, and then click **Configure Selected Attribute**.
- Select ef from the DSCP Keyword menu, and then click **Submit**.
- Select pol_voip from the Policy Selector menu, class_voip from the Member Class List menu, and Mark IP DSCP from the Policy Attribute Selector, and then click **Configure Selected Attribute**.
- Select ef from the DSCP Keyword menu, and then click **Submit**.

13. To attach the defined policy to an inbound service interface, go to the **Service Configuration** page.

14. Select interface 0/2 from the Slot/Port menu.

15. Select pol_voip from the Policy In menu.

16. Click **Submit**.

Configuring a Network with WDS-Managed APs

In this example, a company has a main building that houses most of the employees and contains all the network infrastructure. The company has acquired some additional office space in the building next door. The network administrator has determined that the best and most cost-effective solution to allow employees in the new building to connect to the network is to extend the WLAN to the new building by configuring the network with WDS-Managed APs.

This example describes how to configure the WDS-Managed settings on the APs and switch involved in the network shown in [Figure 437](#).

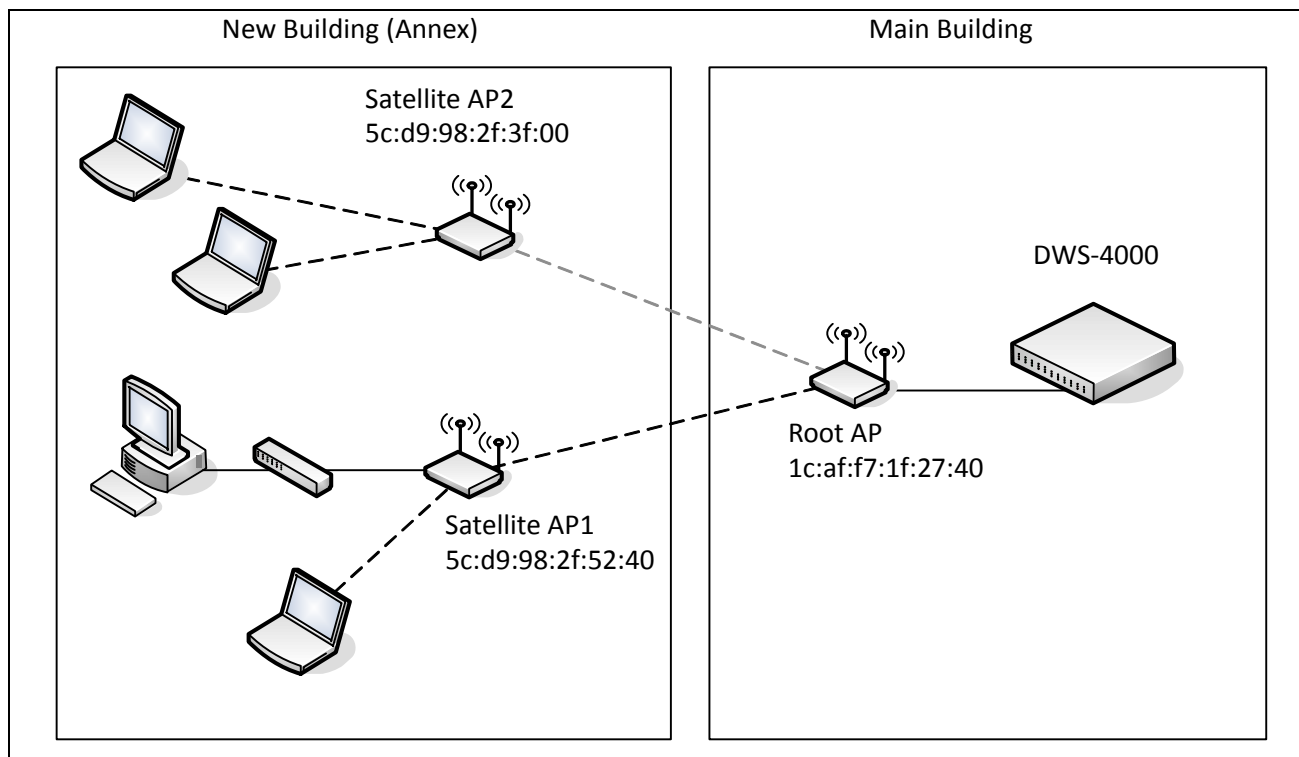


Figure 437: WDS-Managed APs in the Network

The WDS group in [Figure 437](#) has the following characteristics:

- The WDS-Managed AP group name is **annex**, and it includes one root AP and two satellite APs.
- The DWS-4000 switch manages the root AP and the two satellite APs.
- The group has two WDS AP links: one link between the Root AP and Satellite AP1, and one link between the Root AP and Satellite AP2.
- The APs communicate over Radio 1 (IEEE 802.1a/n) on channel 36. The channel is statically configured.
- The Ethernet port on Satellite AP1 is enabled to allow wired LAN access to office PCs in the new building.

To configure the WDS-managed AP group and its links, use the following steps:

1. Configure Satellite AP1 while it is in stand-alone mode.
 - a. Connect to the web-based administration interface for Satellite AP1.
If you know the IP address of the AP, enter it into a browser to access the administration pages for the AP. If you do not know the IP address of the AP, connect to the console port (Baud rate: 115200, Data: 8 bit, Parity: none, Stop: 1 bit, Flow control: none), and enter the `get management` command to view the IP address of the AP.
 - b. Log on to Satellite AP1. The default username is admin, and the default password is admin.
On the home page (Basic Settings), note the MAC address of the AP. When you configure the WDS Managed AP settings on the switch, you must provide the MAC address of the AP.
 - c. Access the **Manage > Managed Access Point** page.
 - d. For the WDS Managed Mode option, select Satellite AP.
 - e. For the WDS Managed Ethernet Port option, select Enabled. This enables the LAN port on the AP to allow wired access to the network.
 - f. In the WDS Group Password field, enter the password for the group, for example **password12345**.

Configure Managed AP Wireless Switch Parameters

Managed AP Administrative Mode: Enabled Disabled

Switch IP Address 1:

Switch IP Address 2:

Switch IP Address 3:

Switch IP Address 4:

Base IP port:

Pass Phrase: Edit

WDS Managed Mode: Root AP Satellite AP

WDS Managed Ethernet Port: Enabled Disabled

WDS Group Password:

Click "Apply" to save the new settings.



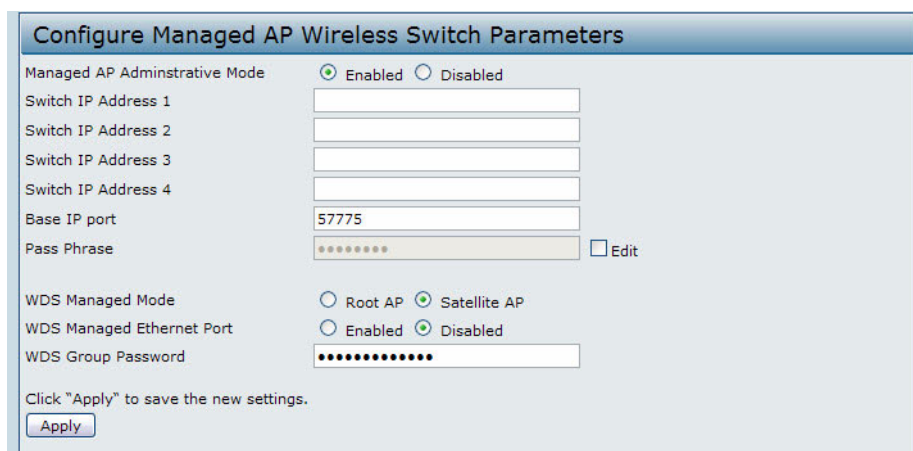
Note: If AP Validation is enabled on the switch on the **WLAN > Administration > Basic Setup > Global** page, the AP must authenticate with a RADIUS server or with the switch before it can be managed. To set the password for AP validation on the AP, select the **Edit** check box and enter the pass phrase in the Pass Phrase field. The pass phrase you enter must match the pass phrase configured on the RADIUS server or in the Authentication Password field on the **WLAN > Administration > Basic Setup > Valid AP** page (see [“Valid Access Point Configuration”](#) on page 557).

- g. Click **Apply**.
- h. Access the **Manage > Radio** page.

- i. Set the radio(s) that will participate in the WDS link to a static channel. In this example, the APs in the WDS group use channel 36 on Radio 1 (IEEE 802.11a/n).



- j. Click **Apply**.
 - k. Click **Logout** to log off of the AP.
2. Configure Satellite AP2 while it is in stand-alone mode.
 - a. Connect to the web-based administration interface for Satellite AP1 while it is in stand-alone mode.
 - b. Log on to Satellite AP2. The default username is admin, and the default password is admin.
On the home page (Basic Settings), note the MAC address of the AP. When you configure the WDS Managed AP settings on the switch, you must provide the MAC address of the AP.
 - c. Access the **Manage > Managed Access Point** page.
 - d. For the WDS Managed Mode option, select Satellite AP.
 - e. In the WDS Group Password field, enter the password for the group, for example **password12345**.



- f. Click **Apply**.
- g. Access the **Manage > Radio** page.
- h. Set the radio(s) that will participate in the WDS link to the same static channel configured on Satellite AP1.
- i. Click **Logout** to log off of the AP.



Note: You do not need to configure any settings on the Root AP. By default, the WDS Managed Mode for an AP is Root AP, and the Root AP obtains the WDS Group Password from the switch when it becomes managed. However, you must know the MAC address of the Root AP so you can add it to the Valid AP database and WDS Managed group. This example assumes the IP address of the AP is assigned by a network DHCP server.

3. Connect to the web-based administration interface for the D-Link DWS-4000 Series switch

If you know the IP address of the switch, enter it into a browser to access the administration pages for the switch. If you do not know the IP address of the switch, connect to the console port (Baud rate: 115200, Data: 8 bit, Parity: none, Stop: 1 bit, Flow control: none), and enter the `show network` command to view the switch IP address.

4. On the **WLAN > Administration > Basic Setup > Valid AP** page, enter the MAC address and (optionally) location of the Root AP in the appropriate fields and click **Add**.

The screenshot shows the 'Valid AP' configuration page. At the top, there are tabs for 'Global', 'Discovery', 'Profile', 'Radio', 'SSID', 'Valid AP', and 'OUI'. The 'Valid AP' tab is selected. Below the tabs is a 'Valid Access Point Summary' section with a table:

AP Database	0/128
Managed AP	0
Rogue AP	0
Standalone AP	0

Below the table is a note: "Note: No entries currently exist in the Local AP Validation Database. If desired, you can add Access Point entries here allowing switch management as Access Points are discovered." Below the note is a form with two input fields: 'MACAddress' containing '1C:AF:F7:1F:27:40' and 'Location' containing 'Root AP'. To the right of the 'Location' field is an 'Add' button. Below the form are buttons for 'Delete', 'Delete All', and 'Refresh'. To the right of these buttons is a 'Change Profile' dropdown menu set to '1 - Default'.

The **Valid Access Point Configuration** page displays.

5. In the Radio 1 field, set the channel to 36 and click **Submit**.



Note: The root AP and satellite APs must use the same radio and channel to communicate over the WDS link.

6. Repeat Step 4 and Step 5 to add Satellite AP1 and Satellite AP2 to the Valid AP database.

7. From the **WLAN > Administration > WDS Configuration > Group Configuration** page, enter the group name and click **Add**.

The WDS Managed AP Group Configuration page displays.

8. Select the **Edit** check box and enter the WDS group password in the appropriate field (**password12345**).

9. Click **Submit**.

10. From the **WLAN > Administration > WDS Configuration > AP Configuration** page, click **Add** to add the root AP to the selected group. If multiple WDS groups are configured, make sure you select the appropriate group ID before you click **Add**.

11. Select the MAC address of the Root AP from the **Valid AP MAC Address** menu to populate the **WDS AP MAC Address** field with the MAC address of the Root AP.

The **Valid AP MAC Address** menu contains the MAC addresses of all APs that have been added to the Valid AP Database on the **WLAN > Administration > Basic Setup > Valid AP** page.

12. Click **Submit**.

13. Repeat [Step 11](#), [Step 12](#), and [Step 12](#) to add the MAC addresses for Satellite AP1 and Satellite AP2 to the group.

14. Click **WLAN > Administration > WDS Configuration > AP Configuration** to return to the main **AP Configuration** page to verify the APs have been added to the group.

AP MAC Address	STP Priority
<input type="checkbox"/> 1C:AF:F7:1F:27:40	36864
<input type="checkbox"/> 5C:D9:98:2F:3F:00	36864
<input type="checkbox"/> 5C:D9:98:2F:52:40	36864

15. From the **WLAN > Administration > WDS Configuration > Link Configuration** page, click **Add** to add the links to the selected group. If multiple WDS groups are configured, make sure you select the appropriate group ID before you click **Add**.
16. On the **WDS Link Create** page, configure the link between the Root AP and Satellite AP1 with the following settings:
- Source AP MAC Address: 1C:AF:F7:1F:27:40 (Root AP)
 - Source AP Radio: 1
 - Destination AP MAC Address: 5C:D9:98:2F:52:40 (Satellite AP1)
 - Destination AP Radio: 1
 - Link Cost: You do not need to provide a value for this field because STP is disabled. By default, the link cost is 40.

WDS Link Create	
Source AP MAC Address	1C:AF:F7:1F:27:40
Source AP Radio	1 (1 to 2)
Destination AP MAC Address	5C:D9:98:2F:52:40
Destination AP Radio	1 (1 to 2)
Link Cost	(0 to 255)

17. Click **Submit**.
18. On the **WDS Link Create** page, configure the link between the Root AP and Satellite AP2 with the following settings:
- Source AP MAC Address: 1C:AF:F7:1F:27:40 (Root AP)
 - Source AP Radio: 1
 - Destination AP MAC Address: 5C:D9:98:2F:3F:00 (Satellite AP2)
 - Destination AP Radio: 1
 - Link Cost: You do not need to provide a value for this field because STP is disabled. By default, the link cost is 40.
19. Click **Submit**.

20. Return to the **WLAN > Administration > WDS Configuration > Link Configuration** page to verify the link settings.

WDS AP Link Configuration

WDS Group Id: 1

	Source AP MAC Address	Source Radio	Dest AP MAC Address	Dest AP Radio	STP Link Cost
<input type="checkbox"/>	1C:AF:F7:1F:27:40	1	5C:D9:98:2F:3F:00	1	40
<input type="checkbox"/>	1C:AF:F7:1F:27:40	1	5C:D9:98:2F:52:40	1	40

Buttons: Add, Submit, Delete, Refresh

21. Deploy the APs, if they have not already been deployed. After the Root AP is discovered and has become managed, it will scan for the Satellite APs. As they are discovered, they will become managed.



Note: It might take several minutes for the APs to establish WDS links and to become managed.

22. To verify that the WDS links and APs are operating as expected, navigate to **WLAN > Monitoring > WDS Managed APs**.

WDS AP Group Status Summary | WDS AP Group Status | WDS AP Status | WDS Link Status Summary | WDS Link Statistics Summary

WDS Group Status Summary

Group Id	Configured AP Count	Connected Root AP Count	Connected Satellite AP Count	Configured WDS Link Count	Detected WDS Links Count
1	3	1	2	2	2

Refresh

WDS AP Group Status Summary | WDS AP Group Status | WDS AP Status | WDS Link Status Summary | WDS Link Statistics Summary

WDS AP Group Status

WDS Group Id: 1

Configured AP Count	3	Connected AP Count	3
Root AP Count	1	Satellite AP Count	2
Root Bridge AP MAC	1C:AF:F7:1F:27:40	Root Device Type	None
Config WDS Link Count	2	Detect WDS Link Count	2
Blocked WDS Link Count	0	WDS Group Password Change Status	Not Started
New WDS Group Password	<input type="text"/>	<input type="checkbox"/> Edit	

Refresh | Apply Password

WDS AP Group Status Summary	WDS AP Group Status	WDS AP Status	WDS Link Status Summary	WDS Link Statistics Summary
-----------------------------	---------------------	---------------	-------------------------	-----------------------------

WDS Group AP Status Summary

1-annex ▾

AP MAC Address	AP Connection Status	Satellite Mode	STP Root Mode	Root Path Cost	Ethernet Port STP State	Ethernet Port Mode	Ethernet Port Link State
1c:af7:1f:27:40	Connected	Wired	Not STP Root	0	Disabled	Disabled	Up
5c:d9:98:2f:3f:00	Connected	Satellite	Not STP Root	0	Disabled	Disabled	Up
5c:d9:98:2f:52:40	Connected	Satellite	Not STP Root	0	Disabled	Enabled	Up

WDS AP Group Status Summary	WDS AP Group Status	WDS AP Status	WDS Link Status Summary	WDS Link Statistics Summary
-----------------------------	---------------------	---------------	-------------------------	-----------------------------

WDS Group Link Status Summary

WDS AP Group Id	Source MAC Address	Source Radio	Destination MAC Address	Destination Radio	Source End-Point Detected	Destination End-Point Detected	Aggregation Mode	Source STP State	Destination STP State
1	1c:af7:1f:27:40	1	5c:d9:98:2f:3f:00	1	Yes	Yes	No	Forwarding	Forwarding
1	1c:af7:1f:27:40	1	5c:d9:98:2f:52:40	1	Yes	Yes	No	Forwarding	Forwarding

WDS AP Group Status Summary	WDS AP Group Status	WDS AP Status	WDS Link Status Summary	WDS Link Statistics Summary
-----------------------------	---------------------	---------------	-------------------------	-----------------------------

WDS Group Link Statistics Summary

WDS AP Group Id	Source MAC Address	Source Radio	Destination MAC Address	Destination Radio	Source AP Packets Sent	Source AP Bytes Sent	Source AP Packets Received	Source AP Bytes Received	Destination AP Packets Sent	Destination AP Bytes Sent	Destination AP Packets Received	Destination AP Bytes Received
1	1c:af7:1f:27:40	1	5c:d9:98:2f:3f:00	1	1755	599347	5463	486194	7173	854112	2563	731203
1	1c:af7:1f:27:40	1	5c:d9:98:2f:52:40	1	16461	1728291	1901	1059726	1639	1021799	15561	1507996

Configuring a Network to Use WPA2-Enterprise and Dynamic VLANs

This configuration example shows a company deploying a wireless network that uses WPA2-Enterprise encryption and dynamic VLANs. To keep financial information separate from other corporate data, the network administrator has configured a separate VLAN for Accounting Department employees. Because some individuals may be granted access to the Accounting VLAN for a short period, the administrator decides to use user-based granular control over VLAN assignments. The administrator controls access to the accounting VLAN by using a RADIUS server and Dynamic VLAN assignment.

This example includes two wireless networks (VAPs):

- The Visitor network provides Internet access to guests. Guests who connect to the the Visitor network are assigned to VLAN 10, which provides limited access to network resources.
- The Corporate network is for employees. An employee who connects to this network must be authenticated by a network RADIUS server. By default, users on this network are assigned to VLAN 20. However, when an Accounting Department user authenticates to the Corporate network, the user is assigned to VLAN 30. The VLAN assignment in the RADIUS profile for an Accounting Department employee takes precedence over the default VLAN of the VAP.

Table 385 shows a summary of the VAP configuration in this example.

Table 385: VAP Summary

Network (SSID)	VLAN	Security	Redirect
Visitor	10	None	http://www.dlink.com/tw
Corporate	20	WPA Enterprise	None

In Figure 438, when Client_1 initiates a connection to the Corporate network, the authentication information is passed from the client to the AP, and from the AP to the switch. Then, the switch forwards the information to the RADIUS server. If the authentication is successful, the RADIUS server response includes the VLAN assignment information. This example includes only one AP, but the configuration is easily scalable to multiple APs.

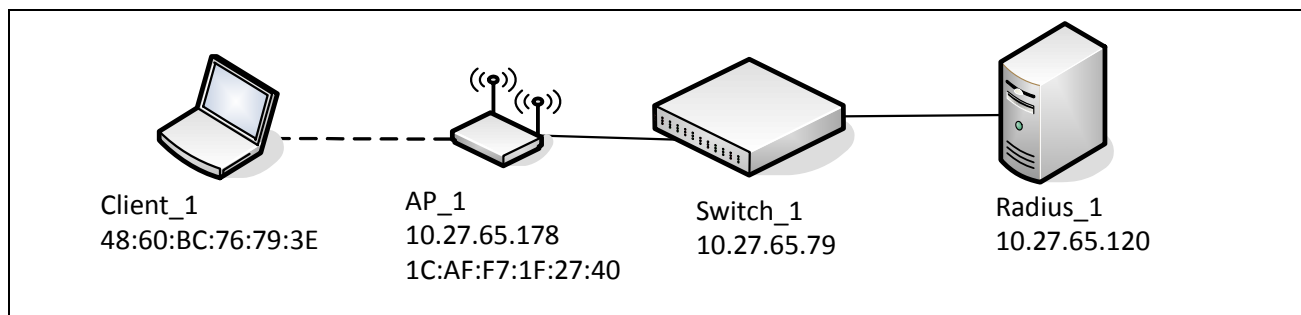


Figure 438: WPA2-Enterprise and Dynamic VLAN Assignment

This example requires configuring settings on the RADIUS server and on the switch.

Configuring Client Information on the RADIUS Server

To use WPA-Enterprise and RADIUS-assigned VLANs, you must configure information about the clients on the network RADIUS server. The configuration of your RADIUS server will vary depending on the manufacturer of the RADIUS server, but the parameters for dynamic VLAN tagging are the same, regardless of the RADIUS server you use.

The following parameters should be set to allow for Dynamic VLAN Tagging where <vlan-ID> is the VLAN to assign to each user.

- Tunnel-Type = 13,
- Tunnel-Medium-Type = 6,
- Tunnel-Private-Group-ID = <vlan-ID>

This example describes how to configure the FreeRADIUS server (available from FreeRADIUS.org) with the users in [Table 386](#).

Table 386: Wireless LAN Users

Username	Password	Group	VLAN
accountant	accountant	Accounting	VLAN 30
engineer	engineer	Corporate	None assigned

To configure the FreeRADIUS server:

1. Edit the `etc/raddb/users.conf` file, which contains the user account information, and add the new users.

The following code shows an example of the entry for the *accountant* and *engineer* users:

```
accountant User-Password == "accountant"
           Tunnel-Type = 13,
           Tunnel-Medium-Type = 6,
           Tunnel-Private-Group-ID = 30
```

```
engineer User-Password == "engineer"
```

2. Edit the `etc/raddb/clients.conf` file to allow the switch to act as a client for the RADIUS server.

The following code shows an example of the entry in the clients file that allows the switch to authenticate with the RADIUS server:

```
client 10.27.65.0/24 {
    secret      = secret12345
    shortname   = private-network-1
}
```

The client network in the entry includes the IP address of the switch. The secret matches the secret to be configured on the switch. The secret must match on both systems

Configuring RADIUS Information and AP Profiles on the Switch

The procedures in this section describe how to configure the RADIUS information on the switch, how to enable RADIUS-assigned VLANs, and how to configure the AP profile to be applied to the APs that the switch manages.

1. Connect to the web-based administration interface on the D-Link DWS-4000 Series switch. If you know the IP address of the switch, enter it into a browser to access the administration pages for the switch. If you do not know the IP address of the switch, connect to the console port (Baud rate: 115200, Data: 8 bit, Parity: none, Stop: 1 bit, Flow control: none), and enter the `show network` command to view the switch IP address.
2. Configure the RADIUS server information.
 - a. Go to the **LAN > Security > RADIUS > RADIUS Authentication** page.
 - b. Configure the RADIUS server host address, for example 10.27.64.120.
 - c. Configure the RADIUS server name, for example RADIUS.

The screenshot shows the 'RADIUS Authentication Server Configuration' page. It contains the following fields:

RADIUS Server Host Address	Add	
RADIUS Server Host Address	10.27.65.120	(Max 255 characters/X.X.X.X)
RADIUS Server Name	RADIUS	(Max 31 characters)

There is a 'Submit' button at the bottom of the form.

- d. Click **Submit**. Additional fields appear on the screen.
- e. To configure the password (shared secret) that the switch uses to authenticate with the RADIUS server, select the **Apply** option and type the password (for example *secret12345*) in the **Secret** field. The secret you configure must match the secret configured in the client entry for the switch on the RADIUS server.
- f. From the Primary Server field, select Yes.

The screenshot shows the 'RADIUS Authentication Server Configuration' page after clicking 'Submit'. The fields are now populated and include additional options:

RADIUS Server Host Address	10.27.65.120	
Port	1812	(1 to 65535)
Secret	Apply <input checked="" type="checkbox"/>
Primary Server	Yes	
Message Authenticator	Enable	
Secret Configured	No	
Current	Yes	
RADIUS Server Name	RADIUS	(Max 31 characters)

At the bottom of the form, there are three buttons: 'Submit', 'Remove', and 'Refresh'.

- g. Click **Submit**.
3. Enable Dynamic VLAN creation mode to allow RADIUS-assigned VLANs to be automatically created on the switch if they do not already exist.
 - a. Access the **LAN > Security > Port Access Control** page
 - b. From the Dynamic VLAN Creation Mode menu, select Enable.

Port Access Control Configuration

Administrative Mode: Disable

VLAN Assignment Mode: Disable

Dynamic VLAN Creation Mode: Enable

Monitor Mode: Disable

Submit

- c. Click **Submit**.
4. Configure the Wireless Network Information for the Visitor network.
 - a. Go to the **WLAN > Administration > Basic Setup > SSID** page.
 - b. Select the radio to configure. This example configures Radio 2 - 802.11b/g/n.
 - c. For Network 1 - dlink1, click **Edit**.

Global | Discovery | Profile | Radio | **SSID** | Valid AP | OUI

Wireless Default VAP Configuration

AP Profile 1-Default

1-802.11a/n 2-802.11b/g/n

Network	VLAN	L3 Tunnel	Hide SSID	Security	Redirect
<input checked="" type="checkbox"/> 1 - dlink1 <input type="button" value="Edit"/>	1-default	Disabled	Disabled	None	None
<input type="checkbox"/> 2 - dlink2 <input type="button" value="Edit"/>	1-default	Disabled	Disabled	None	None
<input type="checkbox"/> 3 - dlink3 <input type="button" value="Edit"/>	1-default	Disabled	Disabled	None	None
<input type="checkbox"/> 4 - dlink4 <input type="button" value="Edit"/>	1-default	Disabled	Disabled	None	None
<input type="checkbox"/> 5 - dlink5 <input type="button" value="Edit"/>	1-default	Disabled	Disabled	None	None
<input type="checkbox"/> 6 - dlink6 <input type="button" value="Edit"/>	1-default	Disabled	Disabled	None	None

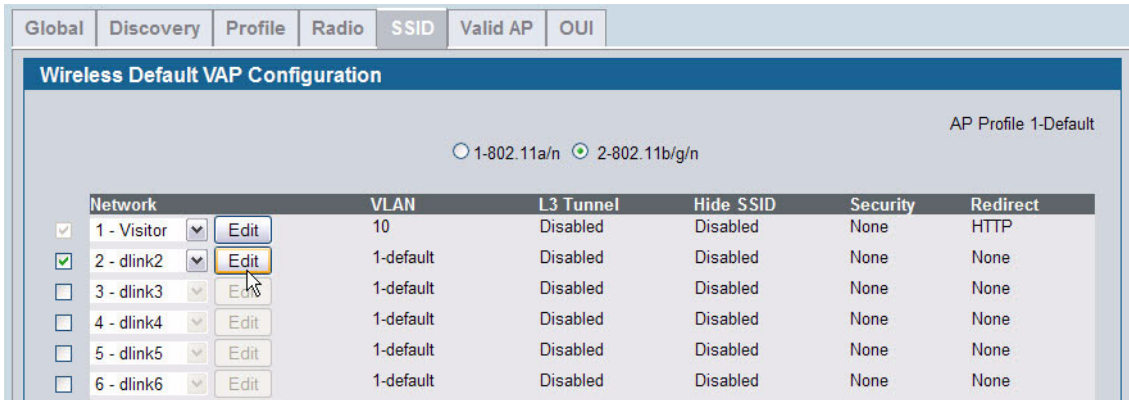
- d. Configure the following information in the appropriate fields:
 - SSID = Visitor
 - VLAN = 10
 - Redirect = HTTP
 - Redirect URL = <http://www.dlink.com/tw>

Global	Discovery	Profile	Radio	SSID	Valid AP	OUI
Wireless Network Configuration						
SSID	<input type="text" value="Visitor"/>					
Hide SSID	<input type="checkbox"/>					
Ignore Broadcast	<input type="checkbox"/>					
VLAN	<input type="text" value="10"/> (1 to 4094)					
L3 Tunnel	<input type="checkbox"/>					
L3 Tunnel Status	None					
L3 Tunnel Subnet	<input type="text" value="0.0.0.0"/>					
L3 Tunnel Mask	<input type="text" value="255.255.255.0"/>					
MAC Authentication	<input type="radio"/> Local <input type="radio"/> RADIUS <input checked="" type="radio"/> Disable					
Redirect	<input type="radio"/> None <input checked="" type="radio"/> HTTP					
Redirect URL	<input type="text" value="http://www.dlink.c"/>					
Wireless ARP Suppression Mode	Disable <input type="text"/>					
L2 Distributed Tunneling Mode	Disable <input type="text"/>					
RADIUS Authentication Server Name	<input type="text" value="Default-RADIUS-Server"/>					
RADIUS Authentication Server Status	Not Configured					
RADIUS Accounting Server Name	<input type="text" value="Default-RADIUS-Server"/>					
RADIUS Accounting Server Status	Not Configured					
RADIUS Use Network Configuration	Enable <input type="text"/>					
RADIUS Accounting	<input type="checkbox"/>					
Security	<input checked="" type="radio"/> None <input type="radio"/> WEP <input type="radio"/> WPA/WPA2					
Client QoS	<input type="checkbox"/>					
Client QoS Bandwidth Limit Down (bits-per-second)	<input type="text" value="0"/> (0 to 4294967295, 0 - Disable)					
Client QoS Bandwidth Limit Up (bits-per-second)	<input type="text" value="0"/> (0 to 4294967295, 0 - Disable)					
Client QoS Access Control Down	<none> <input type="text"/>					
Client QoS Access Control Up	<none> <input type="text"/>					
Client QoS Diffserv Policy Down	<none> <input type="text"/>					
Client QoS Diffserv Policy Up	<none> <input type="text"/>					
<input type="button" value="Submit"/> <input type="button" value="Refresh"/> <input type="button" value="Clear"/>						

e. Click **Submit**.

5. Configure the Wireless Network Information for the Corporate network.

- Click the **SSID** tab (or click **WLAN > Administration > Basic Setup > SSID**) to return to the **Wireless Default VAP Configuration** page.
- Select the radio to configure. This example configures Radio 2 - 802.11b/g/n.
- Select the option next to Network 2- dlink2, and click **Edit**.



d. Configure the following information in the appropriate fields:

SSID = Corporate

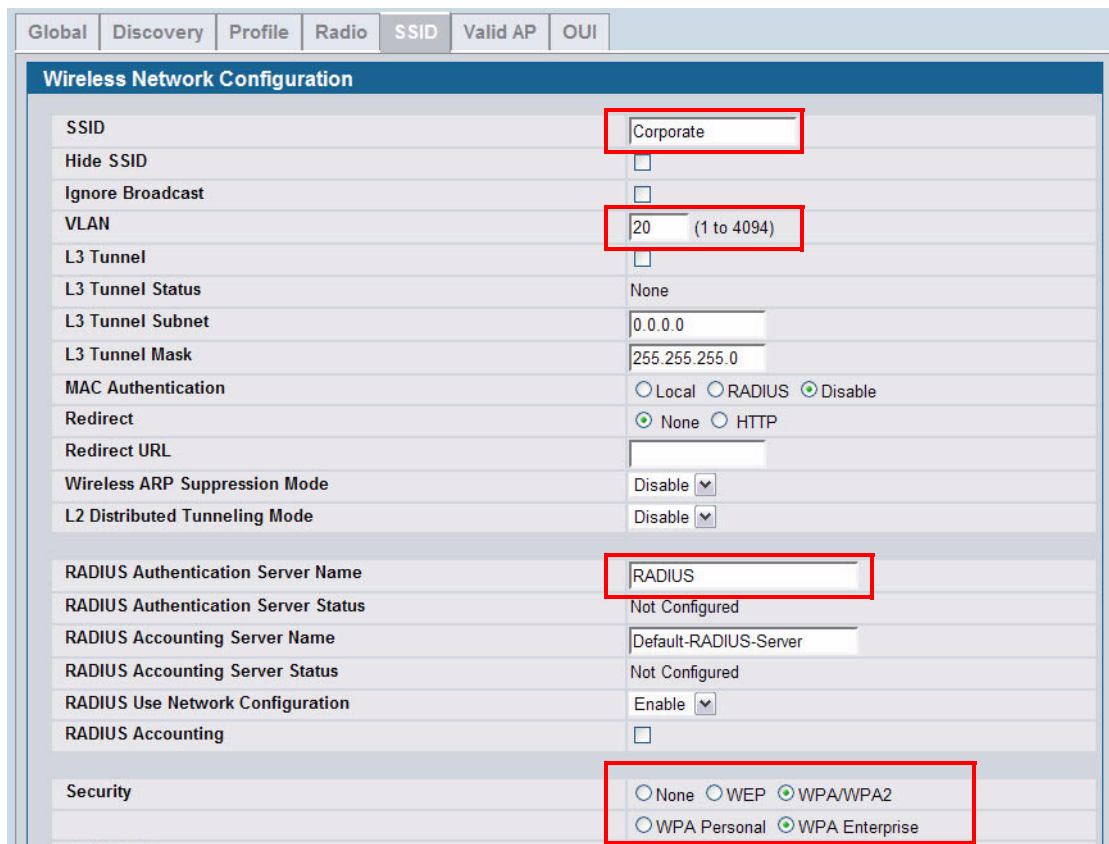
VLAN = 20

Radius Authentication Server Name = RADIUS

Security = WPA/WPA2, WPA Enterprise



Note: The WPA Enterprise option is available only after you select the WPA/WPA2 option.



6. Add the AP to the Valid AP database so that it can become managed when the switch discovers it.
 - a. Go to the **WLAN > Administration > Basic Setup > Valid AP** page.
 - b. Specify the MAC address of the AP in the appropriate field.
 - c. Optionally, specify the location or a name that identifies the AP, for example AP_1.

The screenshot shows a web-based configuration interface for a network switch. At the top, there is a navigation menu with tabs: Global, Discovery, Profile, Radio, SSID, Valid AP (selected), and OUI. Below the menu is a section titled "Valid Access Point Summary" with a table showing the status of the AP database:

AP Database	0/128
Managed AP	0
Rogue AP	0
Standalone AP	0

Below the table is a note: "Note: No entries currently exist in the Local AP Validation Database. If desired, you can add Access Point entries here allowing switch management as Access Points are discovered." Below the note is a form with two input fields: "MACAddress" containing "1C:AF:F7:1F:27:40" and "Location" containing "AP_1". To the right of the "Location" field is an "Add" button. Below the form is a "Change Profile" dropdown menu set to "1 - Default". At the bottom of the form are three buttons: "Delete", "Delete All", and "Refresh".

- d. Click **Add**.

When the AP becomes managed, the default profile is applied. If you make changes to the default profile after the AP is managed, you must reapply the profile to push the changes to the AP from the **WLAN > Administration > Advanced Configuration > AP Profiles** page.

Verifying the Configuration

This section describes the pages available for monitoring information the managed AP and its associated clients.

1. Verify that the AP is now managed by the switch.

Click **WLAN > Monitoring > Access Point > Managed AP Status** and verify that the AP_1 status is Managed and the Configuration status is Success.

MAC address	Location	Switch Port	IP Address	Software Version	Age	Status	Configuration Status	Profile	Radio	Channel	Authenticated Clients
1c:af:f7:1f:27:40	AP_1	0/11	10.27.65.178	D.7.11.2	0d:00:00:01	Managed	Success	1-Default	1-802.11a/n 2-802.11b/g/n	149 6	0 0

Buttons: Delete, Delete All, Refresh, Auto Refresh

2. Verify that the *engineer* user can connect to the Corporate network and is assigned to VLAN 20.
 - a. Use a wireless client to access the wireless network with the *Corporate* SSID.
 - b. When prompted for the username and password, enter *engineer* for both fields.
 - c. To verify the VLAN assigned to the *engineer* user, go to the **WLAN > Monitoring > Client > Associated Clients** page and select the MAC address of the client. Note the VLAN of the *engineer* user is VLAN 20, the default VLAN for the VAP.

SSID	Corporate	Associating Switch	Local Switch
BSSID	1C:AF:F7:1F:27:51	Switch MAC Address	00:17:9A:95:4E:C4
AP MAC Address	1C:AF:F7:1F:27:40	Switch IP Address	10.27.65.79
Status	Authenticated	Location	AP_1
Channel	6	Radio	2
User Name	engineer	VLAN	20
Inactive Period	0d:00:00:00	Transmit Data Rate	270 Mbps
Age	0d:00:00:04	Network Time	0d:00:02:14
Dot11n Capable	Yes	STBC Capable	No
NetBIOS Name		Detected IP Address	10.27.65.107
Tunnel IP Address			

Buttons: Disassociate, Refresh, Back

3. Verify that the *accountant* user can connect to the Corporate network and is assigned to VLAN 30.
 - a. Use a wireless client to access the wireless network with the *Corporate* SSID.
 - b. When prompted for the username and password, enter *accountant* for both fields.
 - c. To verify the VLAN assigned to the engineer user, go to the WLAN > Monitoring > Client > Associated Clients page and select the MAC address of the client. Note the VLAN of the *accountant* user is VLAN 30, which has been dynamically assigned by the RADIUS server.

The screenshot shows the 'Associated Client Status' page in the D-Link UWS web interface. The page has a navigation bar with tabs for 'Status', 'SSID Status', 'VAP Status', 'Switch Status', and 'Statistics'. Below this is a sub-navigation bar with tabs for 'Summary', 'Detail', 'Client QoS', 'Neighbor APs', 'Distributed Tunneling', 'TSPEC', and 'RRM'. The main content area is titled 'Associated Client Status' and features a dropdown menu with the MAC address 'f0:7b:cb:35:a0:33'. Below the dropdown is a table of client information. The 'User Name' and 'VLAN' fields are highlighted with red boxes. At the bottom of the page are three buttons: 'Disassociate', 'Refresh', and 'Back'.

SSID	Corporate	Associating Switch	Local Switch
BSSID	1C:AF:F7:1F:27:51	Switch MAC Address	00:17:9A:95:4E:C4
AP MAC Address	1C:AF:F7:1F:27:40	Switch IP Address	10.27.65.79
Status	Authenticated	Location	AP_1
Channel	6	Radio	2
User Name	accountant	VLAN	30
Inactive Period	0d:00:00:04	Transmit Data Rate	270 Mbps
Age	0d:00:00:04	Network Time	0d:00:02:14
Dot11n Capable	Yes	STBC Capable	No
NetBIOS Name		Detected IP Address	10.27.65.107
Tunnel IP Address			

Optimizing WLAN Traffic

The Unified Wired and Wireless Access System includes features that automatically help to optimize wireless traffic on the network. This section describes the following features:

- Automatic channel selection and adjustment on access point radios
- Automatic power adjustment for access point RF transmission power levels
- Per-radio load balancing to set the maximum utilization threshold

By default, the automatic channel selection, automatic channel adjustment, and automatic power adjustment features are enabled but require manual triggers to run. Load balancing is disabled by default. This section describes ways to monitor the channel and power of the AP and to make manual adjustments, if necessary. It also describes how to enable the load balancing feature and monitor WLAN utilization. This section assumes that the switch has been configured and is currently managing multiple APs.

Monitoring and Managing Channel Information

Interference can occur when multiple access points within range of each other are broadcasting on the same or overlapping channels. The impact of this interference on network performance can intensify during busy times when a large amount of data and media traffic is competing for bandwidth. When APs are within broadcast range of each other, the radios must use different channels to avoid causing RF interference. For the 802.11b/g radio, neighboring APs must operate on channels that are at least five channels apart. For example, if AP1 and AP2 are neighbors, AP1 can operate on channel 6 while AP2 operates on channel 11. Channels in the 5 GHz band (802.11a/n) do not overlap, so these channels interfere only if neighboring APs operate on the same channel.

To avoid interference with neighbor APs, the Unified Wired and Wireless Access System uses an Initial Channel Selection (ICS) algorithm. When the AP is powered up the ISI algorithm scans all the available channels and counts the number of packets received on each channel. The best operating channel is considered to be the one with the lowest packet count, and this channel is assigned to the AP radio.

To view the channels that are assigned to managed APs, click **WLAN > Monitoring > Access Point > Managed AP Status**. As [Figure 439 on page 699](#) shows, Radio 1 (802.11a/n) on AP_1 is operating on channel 157, Radio 1 on AP_2 is operating on channel 44, and Radio 1 on AP_3 is operating on channel 36. Radio 2 (802.11b/g/n) on AP_1 is operating on channel 1, Radio 2 on AP_2 is operating on channel 6, and Radio 2 on AP_3 is operating on channel 11. For both radios, the operating channels for AP_1 do not interfere with the operating channels for AP_2.

MAC Address (*) Peer Managed	Location	Switch Port	IP Address	Software Version	Age	Status	Configuration Status	Profile	Radio	Channel	Authenticated Clients
00:11:22:33:44:20	AP_2	0/1	10.27.65.196	4.0.0.1	0d:00:00:02	Managed	Success	1-Default	1-802.11a/n 2-802.11b/g/n	44 6	0 0
00:11:22:33:44:40	AP_3	0/1	10.27.65.199	4.0.0.1	0d:00:00:04	Managed	Success	1-Default	1-802.11a/n 2-802.11b/g/n	36 11	0 0
5c:d9:98:2f:4a:40	AP_1	0/1	10.27.65.76	D.5.16.1	0d:00:01:01	Managed	Success	1-Default	1-802.11a/n 2-802.11b/g/n	157 1	0 0

Figure 439: Monitoring Managed AP Channels

A second algorithm, the Auto Channel Adjustment (ACA) can periodically evaluate the operating channel and can automatically change the channel if the current operating channel is noisy. The cluster controller runs the ACA algorithm for the whole cluster. Non-cluster controller switches do not run the ACA algorithm. The setting to enable or disable the ACA algorithm is on the **WLAN > Administration > Basic Settings > Radio** page.

Global | Discovery | Profile | Radio | SSID | Valid AP | OUI

Wireless Default Radio Configuration

AP Profile 1-Default

1-802.11a/n 2-802.11b/g/n

State	<input checked="" type="radio"/> On <input type="radio"/> Off	Mode	IEEE 802.11a/n
RTS Threshold (bytes)	2347 (0 to 2347)	DTIM Period (# beacons)	10 (1 to 255)
Load Balancing	<input type="checkbox"/>	Beacon Interval (msecs)	100 (20 to 2000)
Load Utilization (%)	60 (1 to 100)	Automatic Channel	<input checked="" type="checkbox"/>
Maximum Clients	200 (0 to 200)	Automatic Power	<input checked="" type="checkbox"/>
RF Scan Other Channels	<input checked="" type="checkbox"/>	Initial Power (%)	100 (1 to 100)
RF Scan Sentry	<input type="checkbox"/>		
Supported Channels	36 44 149 157		
Auto Eligible	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		
Available MCS Indices	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15		
	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		
Rate Sets (Mbps)	6 9 12 18 24 36 48 54		
Basic	<input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		
Supported	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		

Refresh Clear Submit Next

Figure 440: Automatic Channel Adjustment

The ACA algorithm is enabled by default on each radio, but the default channel plan mode is manual. This means by default, the administrator must manually trigger the ACA algorithm. To configure the switch to run the ACA algorithm automatically, go to the **WLAN > Administration > AP Management > RF Management** page and configure the channel plan mode as Fixed Time (once per day) or Interval (once every 6–24 hours).



Note: D-Link recommends that you run the ACA algorithm (either manually or periodically) when WLAN traffic is low because wireless clients must briefly disassociate from any radio that changes its channel.

Figure 441 shows a channel plan that is configured to run at 3:15 AM every day.

The screenshot shows the 'RF Configuration' page with the following settings:

- Channel Plan: 5 GHz (802.11 a/n) selected
- Channel Plan Mode: Fixed Time selected (highlighted with a red box)
- Channel Plan History Depth: 5 (0 to 10)
- Channel Plan Interval (hours): 6 (6 to 24)
- Channel Plan Fixed Time (hh:mm): 3 : 15 (highlighted with a red box)
- Power Adjustment Mode: Manual selected
- Power Adjustment Interval (minutes): 15 (15 to 1440)

A 'Submit' button is located at the bottom of the configuration area.

Figure 441: Fixed Channel Plan

Running and Applying a Manual Channel Plan

The following procedures describe how to run and apply the channel plan manually.

1. Go to the **WLAN > Administration > AP Management > RF Management** page and note the Channel Plan Mode setting.

The default mode is Manual. If the mode is Fixed Time or Interval, you cannot run the ACA algorithm manually.

The screenshot shows the 'RF Configuration' page with the following settings:

- Channel Plan: 5 GHz (802.11 a/n) selected
- Channel Plan Mode: Manual selected (highlighted with a red box)
- Channel Plan History Depth: 5 (0 to 10)
- Channel Plan Interval (hours): 6 (6 to 24)
- Channel Plan Fixed Time (hh:mm): 0 : 0
- Power Adjustment Mode: Manual selected
- Power Adjustment Interval (minutes): 15 (15 to 1440)

A 'Submit' button is located at the bottom of the configuration area.

2. Click the **Manual Channel Plan** tab.
3. Select the radio to run the channel plan on, and then click **Start**.
4. To view the channel plan that the ACA algorithm recommends, click **Refresh**.

The following figure shows that the ACA algorithm determined that the best operating channel for Radio 1 on AP_3 is channel 149, and not its current operating channel.

Configuration | Channel Plan History | **Manual Channel Plan** | Manual Power Adjustments

Manual Channel Plan

5 GHz (802.11 a/n) 2.4 GHz (802.11 b/g/n)

Current Status: Algorithm Complete

AP MAC Address	Location	Radio	Current Channel	New Channel
00:11:22:33:44:40	AP_3	1-802.11a/n	36	149

Apply Clear Refresh Start



Note: If the ACA algorithm determines that the APs are currently operating on the best channel, the Current Status field reports “Algorithm Complete: No Change Required.”

5. To apply the suggested channel plan, click **Apply**.



Note: D-Link recommends that you apply the channel plan when WLAN traffic is low. When a radio changes to a different channel, any associated clients are forced to disassociate and reassociate.

6. To view information about the channel plans that have been applied, click the **Channel Plan History** tab.

Configuration | **Channel Plan History** | Manual Channel Plan | Manual Power Adjustments

Channel Plan History

5 GHz (802.11 a/n) 2.4 GHz (802.11 b/g/n)

Operational Status: Active

Last Iteration: 1

Last Algorithm Time: JAN 14 23:25:12 1970

AP MAC Address	Location	Radio	Iteration	Channel
00:11:22:33:44:40	AP_3	1	1	149

Refresh

7. To view the operating channel for AP_3 and all managed APs, go to the **WLAN > Monitoring > Access Point > Managed AP Status** page.

MAC Address (*)-Peer Managed	Location	Switch Port	IP Address	Software Version	Age	Status	Configuration Status	Profile	Radio	Channel	Authenticated Clients
00:11:22:33:44:20	AP_2	0/1	10.27.65.196	4.0.0.1	0d:00:00:02	Managed	Success	1-Default	1-802.11a/n 2-802.11b/g/n	44 6	0 0
00:11:22:33:44:40	AP_3	0/1	10.27.65.199	4.0.0.1	0d:00:00:04	Managed	Success	1-Default	1-802.11a/n 2-802.11b/g/n	149 11	0 0
5c:d9:98:2f:4a:40	AP_1	0/1	10.27.65.76	D.5.16.1	0d:00:01:01	Managed	Success	1-Default	1-802.11a/n 2-802.11b/g/n	157 1	0 0

Buttons: Delete, Delete All, Refresh, Auto Refresh

Monitoring the RF Transmission Power Level

The RF signal transmission power level directly affects the broadcast range of the AP signal. If the power level is too low, wireless clients will not detect the signal or experience poor WLAN performance. If the power level is too high, the RF signal might interfere with other APs within range. If the RF signal broadcasts beyond the physical confines of your building or network, it increases the security threat to the network.

The Automatic Power Adjustment algorithm works by setting the initial power of the AP to the value specified in the AP profile. The power is then periodically adjusted to a level based on the presence or absence of packet transmission errors. The power is changed in increments of 10%. The Automatic Power Adjustment feature is enabled by default. However, by default the algorithm is triggered manually, and not at a fixed interval.



Note: The algorithm never reduces the AP power below the initial power setting as specified in the profile, and since the default power level in the default profile is 100%, the power would never be reduced unless this value is first changed.

Configuring the Automatic Power Adjustment

This example describes how to run and apply the Automatic Power Adjustment (APA) algorithm.

1. To adjust the initial power level setting on the AP profile, go to the **WLAN > Administration > Basic Settings > Radio** page and set the Initial Power field to a percentage lower than 100, for example 60%.

Global | Discovery | Profile | **Radio** | SSID | Valid AP | OUI

Wireless Default Radio Configuration AP Profile 1-Default

1-802.11a/n 2-802.11b/g/n

State	<input checked="" type="radio"/> On <input type="radio"/> Off	Mode	IEEE 802.11a/n
RTS Threshold (bytes)	2347 (0 to 2347)	DTIM Period (# beacons)	10 (1 to 255)
Load Balancing	<input type="checkbox"/>	Beacon Interval (msecs)	100 (20 to 2000)
Load Utilization (%)	60 (1 to 100)	Automatic Channel	<input checked="" type="checkbox"/>
Maximum Clients	200 (0 to 200)	Automatic Power	<input checked="" type="checkbox"/>
RF Scan Other Channels	<input checked="" type="checkbox"/>	Initial Power (%)	60 (1 to 100)
RF Scan Sentry	<input type="checkbox"/>		
Supported Channels	36 44 149 157		
Auto Eligible	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		
Available MCS Indices	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15		
	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		
Rate Sets (Mbps)	6 9 12 18 24 36 48 54		
Basic	<input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		
Supported	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		

Refresh Clear Submit Next

2. Click **Submit**.
3. Optionally, select Radio 2 and configure the Initial Power setting, and then click **Submit**.
4. If the APs are already managed, use the following steps to reapply the profile so the new settings take effect:
 - a. Go to the **WLAN > Administration > Advanced Configuration > AP Profiles** page.
 - b. Select the check box next to the profile you modified.
 - c. Click **Apply**.

Summary | Default | **2-DWL8600**

Access Point Profile List

Profile	Profile Status
<input checked="" type="checkbox"/> 1-Default	Associated - Modified
<input type="checkbox"/> 2-DWL8600	Configured

Add Copy

Delete **Apply** Refresh

A message appears and indicates that the AP radios will be reset, which will disassociate any associated wireless clients. Click **OK** to continue.

- View the transmit power for the associated APs by clicking **WLAN > Monitoring > Access Points > Managed AP Status > Radio Summary**.

MAC Address	Location	Radio	Channel	Transmit Power	Authenticated Clients
(*)-Peer Managed					
00:11:22:33:44:20	AP_2	1-802.11a/n	36	60	4
		2-802.11b/g/n	11	60	0
00:11:22:33:44:40	AP_3	1-802.11a/n	149	60	9
		2-802.11b/g/n	6	60	0
1c:af:f7:1f:27:40	AP_1	1-802.11a/n	157	60	6
		2-802.11b/g/n	1	60	0

- Go to the **WLAN > Administration > AP Management > RF Management** page and note the Power Adjustment Mode setting.

The default mode is Manual. If the mode is Interval, you cannot run the APA algorithm manually.

RF Configuration	
Channel Plan	<input checked="" type="radio"/> 5 GHz (802.11 a/n) <input type="radio"/> 2.4 GHz (802.11 b/g/n)
Channel Plan Mode	<input type="radio"/> Fixed Time <input checked="" type="radio"/> Manual <input type="radio"/> Interval
Channel Plan History Depth	5 (0 to 10)
Channel Plan Interval (hours)	6 (6 to 24)
Channel Plan Fixed Time (hh:mm)	0 : 0
Power Adjustment Mode	<input checked="" type="radio"/> Manual <input type="radio"/> Interval
Power Adjustment Interval (minutes)	15 (15 to 1440)

- Click the **Manual Power Adjustment** tab.
- Click **Start** to allow the algorithm to run and determine whether any power adjustments are appropriate.
- To view the adjustments that the APA algorithm recommends, click **Refresh**.



Note: The APA recommends power adjustments based on the presence or absence of packet transmission errors. A high number of packet transmission errors indicates that the signal strength might be too low and that wireless clients are unable to successfully transmit traffic. If no wireless clients are connected to the AP, no power adjustments will be recommended.

The following figure shows that the APA algorithm detected a high number of transmission errors on AP_2, and that the power level should be increased by 10% to increase the transmission area.

Manual Power Adjustments

Current Status: Algorithm Complete

AP MAC Address	Location	Radio	Current Power	New Power
00-11-22-33-44-40	AP_2	1-802.11a/n	60	70

Buttons: Apply, Clear, Refresh, Start

10. To apply the recommendation and allow the AP to adjust its transmission power level, click **Apply**.

11. Verify that the power level has been adjusted by viewing the **WLAN > Monitoring > Access Points > Managed AP Status > Radio Summary** page.

Managed Access Point Radio Status

MAC Address	Location	Radio	Channel	Transmit Power	Authenticated Clients
(*) Peer Managed 00-11-22-33-44-20	AP_2	1-802.11a/n	36	70	4
		2-802.11b/g/n	11	70	0
00-11-22-33-44-40	AP_3	1-802.11a/n	149	60	9
		2-802.11b/g/n	6	60	0
1c:af:f7:1f:27:40	AP_1	1-802.11a/n	157	60	6
		2-802.11b/g/n	1	60	0

Buttons: Refresh, Back

Load Balancing and WLAN Utilization

When the power level on an access point is high and the RF broadcast area is large, more wireless clients can detect the signal and associate with the AP than when the power is low and the broadcast area is small. However, an increase in the number of wireless clients that associate with the AP generally means that the amount of traffic the AP receives and transmits increases as well, which can impact wireless network speed and performance.

You can limit the network utilization level allowed on an AP to prevent wireless clients from experiencing slower network speeds. Once the network utilization is reached, new clients are unable to associate with the AP. However, the wireless client might be able to associate with a neighboring AP if it is within range. If an AP frequently reaches the network utilization limit, it might indicate that you should add another AP nearby. For each AP profile, you can enable and configure load balancing on a per radio basis. You can also monitor WLAN utilization for each AP and switch within the Unified Wired and Wireless Access System.

By monitoring the WLAN utilization information for the FASTPATH Unified Wireless System and for specific switches and APs within the system, you can make informed decisions about where to place additional APs or make adjustments in AP placement and power transmission levels.

To configure load balancing and monitor WLAN utilization:

1. Go to the **WLAN > Administration > Basic Setup > Radio** page and select the radio to configure.
2. Select the Load Balancing check box to enable load balancing.
3. Specify the threshold for the percentage of network bandwidth utilization allowed on the radio. Once the level you specify is reached, the AP stops accepting new client associations.

Global | Discovery | Profile | **Radio** | SSID | Valid AP | OUI

Wireless Default Radio Configuration AP Profile 1-Default

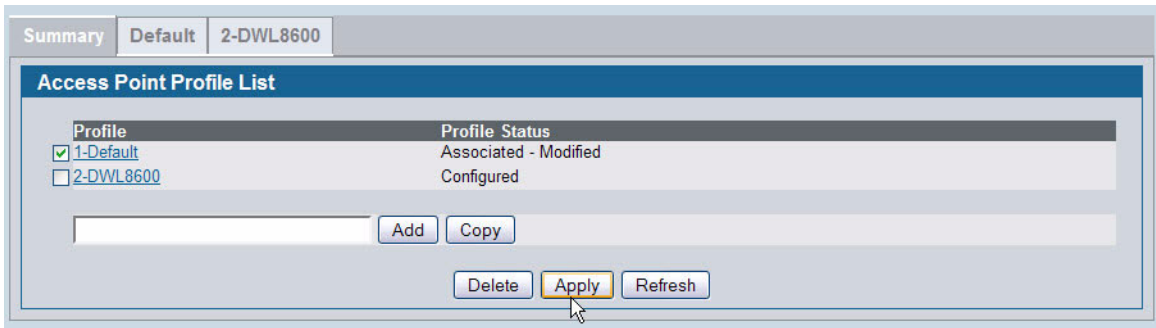
1-802.11a/n 2-802.11b/g/n

State	<input checked="" type="radio"/> On <input type="radio"/> Off	Mode	IEEE 802.11a/n
RTS Threshold (bytes)	2347 (0 to 2347)	DTIM Period (# beacons)	10 (1 to 255)
Load Balancing	<input checked="" type="checkbox"/>	Beacon Interval (msecs)	100 (20 to 2000)
Load Utilization (%)	60 (1 to 100)	Automatic Channel	<input checked="" type="checkbox"/>
Maximum Clients	200 (0 to 200)	Automatic Power	<input checked="" type="checkbox"/>
RF Scan Other Channels	<input checked="" type="checkbox"/>	Initial Power (%)	70 (1 to 100)
RF Scan Sentry	<input type="checkbox"/>		
Supported Channels	36 44 149 157		
Auto Eligible	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		
Available MCS Indices	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15		
Rate Sets (Mbps)	6 9 12 18 24 36 48 54		
Basic	<input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		
Supported	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		

Refresh Clear Submit Next

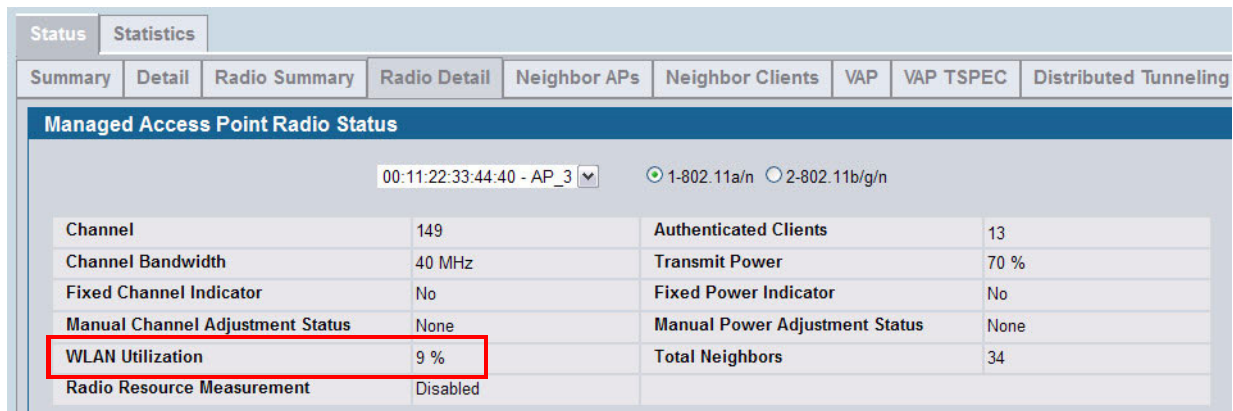
4. Click **Submit** to apply the changes to the selected radio.

5. If the APs are already managed, use the following steps to reapply the profile so the new settings take effect:
 - a. Go to the **WLAN > Administration > Advanced Configuration > AP Profiles** page.
 - b. Select the check box next to the profile you modified.
 - c. Click **Apply**.



A message appears and indicates that the AP radios will be reset, which will disassociate any associated wireless clients. Click **OK** to continue.

6. To monitor the current WLAN utilization rate for a radio, go to the **WLAN > Monitoring > Access Point > Managed AP Status > Radio Detail** page and select the AP (listed by MAC address) and its radio. The WLAN Utilization field displays the current traffic load that the radio is bearing based on the total possible percentage of traffic that the radio can handle.



7. To monitor the current WLAN utilization rate for the FASTPATH Unified Wireless System, go to the **WLAN > Monitoring > Global** page and view the WLAN Utilization field.

Global Switch Status IP Discovery Configuration Received AP Hardware Capability			
Wireless Global Status/Statistics			
WLAN Switch Operational Status	Enabled	IP Address	10.27.65.167
Peer Switches	0		
Cluster Controller	Yes	Cluster Controller IP Address	10.27.65.167
Total Access Points	2	Managed Access Points	2
Standalone Access Points	0	Rogue Access Points	31
Discovered Access Points	0	Connection Failed Access Points	0
Authentication Failed Access Points	2	Unknown Access Points	415
Rogue AP Mitigation Limit	16	Rogue AP Mitigation Count	0
Maximum Managed APs in Peer Group	256	WLAN Utilization	46 %

8. If the FASTPATH Unified Wireless System includes multiple switches in a cluster, click the **Switch Status** tab to view WLAN Utilization information for an individual switch within the cluster.

Global Switch Status IP Discovery Configuration Received AP Hardware Capability			
Switch Status/Statistics			
10.27.65.167 - Local Switch ▼			
Total Access Points	2	Total Clients	13
Managed Access Points	2	Authenticated Clients	0
Discovered Access Points	0	IP Address	10.27.65.167
Connection Failed Access Points	0	Cluster Priority	1
Maximum Managed Access Points	64	Distributed Tunnel Clients	0
WLAN Utilization	46 %		

Detecting and Preventing Wireless Intrusion

This section describes how to use of some of the Wireless Intrusion Detection System (WIDS) and Wireless Intrusion Prevention System (WIPS) functions on the D-Link Unified Wireless Switch.

In this example, a company has configured a wireless network with the VAPs shown in [Table 387](#).

Table 387: WIDS/WIPS VAP Summary

Network (SSID)	VLAN	Security	Redirect
Visitor	10	None	http://www.dlink.com/tw
Corporate	20	WPA Enterprise	None

For information about configuring the VAPs see [“Configuring a Network to Use WPA2-Enterprise and Dynamic VLANs” on page 689](#).

As an additional security measure, the network administrator has decided to employ the use of the WIDS/WIPS functionality to further protect the corporate network. The examples in this section show how to configure the Unified Switch and how to monitor the system as it mitigates potential security risks in the wireless domain.

Configuring a Radio in Sentry Mode

To implement the security policies of the company in this example, the second radio on the Access Point DWL-8600 is configured in sentry mode to scan for violations of the WIDS tests. Alternately, separate APs can be configured as dedicated sentry APs. When a radio operates in sentry mode, the radio performs a continuous radio scan. In sentry mode, no beacons are sent, and no clients are allowed to associate with the AP through the sentry radio.

If a dedicated sentry radio or AP is *not* configured, the active radios still scan other channels but will do so at a slower rate than a radio in sentry mode. The rate at which a radio scans the RF traffic is important to WLAN security because slower scanning allows Rogue APs to remain undetected for a longer period of time.

To enable sentry mode in the default profile on radio 1:

1. Click **WLAN > Administration > Basic Setup > Radio** to access the Wireless Default Radio Configuration page.
2. Select Radio 1.
3. Select the **RF Scan Sentry** option.



Note: By default, the sentry radio scans 802.11a and 802.11 g/b channels. To configure the sentry radio to scan only 802.11a or 802.11b/g channels, but not both, click **WLAN > Administration > Advanced Configuration > AP Profiles > Profile Name > Radio** to access the Access Point Profile Radio Configuration page for the selected profile.

4. Click **Submit** to apply the changes to the running configuration on the switch. Note that the label for radio 1 changes to *Sentry*.

Global | Discovery | Profile | **Radio** | SSID | Valid AP | OUI

Wireless Default Radio Configuration AP Profile 1-Default

1-Sentry 2-802.11b/g/n

State	<input checked="" type="radio"/> On <input type="radio"/> Off	Mode	IEEE 802.11a/n
RTS Threshold (bytes)	2347 (0 to 2347)	DTIM Period (# beacons)	10 (1 to 255)
Load Balancing	<input type="checkbox"/>	Beacon Interval (msecs)	100 (20 to 2000)
Load Utilization (%)	60 (1 to 100)	Automatic Channel	<input checked="" type="checkbox"/>
Maximum Clients	200 (0 to 200)	Automatic Power	<input checked="" type="checkbox"/>
RF Scan Other Channels	<input checked="" type="checkbox"/>	Initial Power (%)	100 (1 to 100)
RF Scan Sentry	<input checked="" type="checkbox"/>		
Supported Channels	36 44 149 157		
Auto Eligible	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		
Available MCS Indices	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15		
Rate Sets (Mbps)	6 9 12 18 24 36 48 54		
Basic	<input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		
Supported	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>		

Refresh Clear Submit Next

5. If an AP is already managed, use the following steps to reapply the profile so the new settings take effect:
- Go to the **WLAN > Administration > Advanced Configuration > AP Profiles** page.
 - Select the check box next to the profile you modified.
 - Click **Apply**.

Configuring and Monitoring WIDS/WIPS to Detect Rogue APs

All passive WIDS detection algorithms for APs are enabled by default on the Unified Switch. The tests are passive because they can detect and report rogue APs and clients but do not attempt to prevent these devices from interfering with the network. It is the responsibility of the administrator to monitor the WIDS test results and take action against potential rogue devices.

To view and configure the WIDS and WIPS parameters click **WLAN > Administration > Advanced Configuration > WIDS Security**.

Figure 442 shows the default values on the WIDS configuration page for the AP.

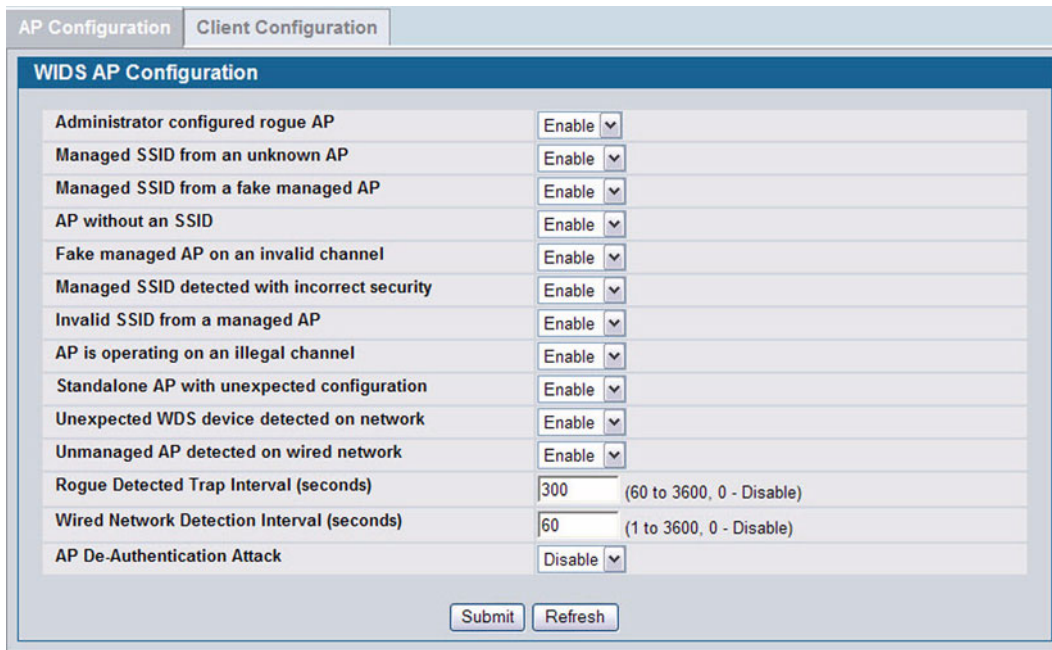


Figure 442: WIDS AP Configuration

To demonstrate the WIDS and WIPS capabilities of the DWS-4000 Series switch, in this scenario a hacker has set up a *HoneyPot AP* in the parking lot of the company's building. This AP is configured with the SSID *Corporate* to try to get valid clients from inside the company to associate to it in an attempt to gather passwords and other confidential information that will allow the hacker to gain further access to the company's resources.

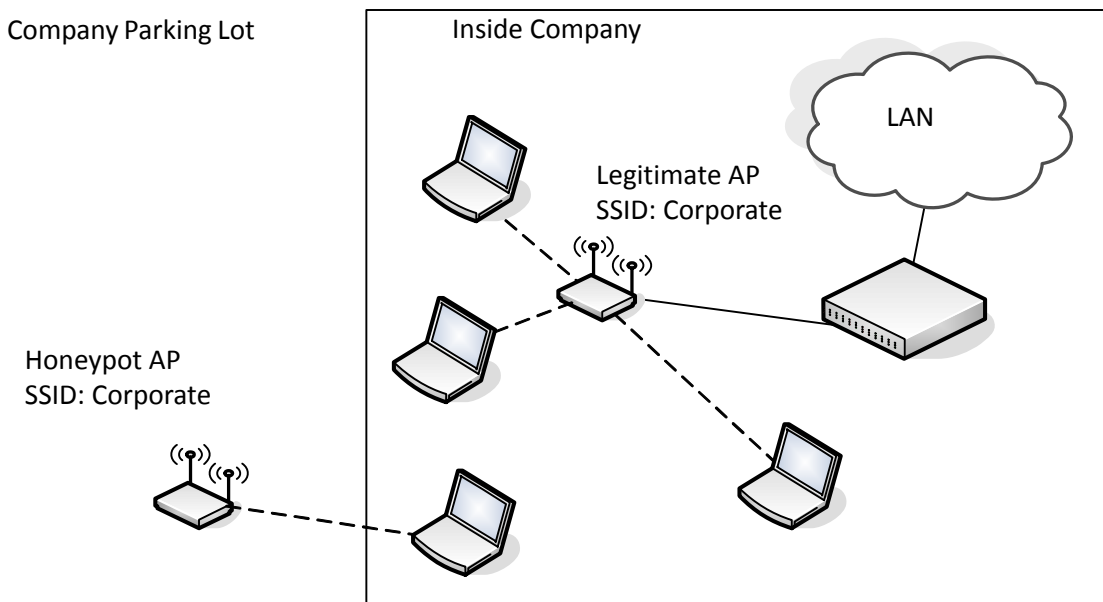


Figure 443: HoneyPot AP

As [Figure 443 on page 711](#) shows, most clients have authenticated with the legitimate AP within the company. However, one client within the company has unknowingly associated with the honeypot AP that is physically located outside the walls of the company.

In this situation, the WIDS system on the AP automatically tags the honeypot AP as a Rogue on the **WLAN > Monitoring > Access Point > All AP Status** page.

MAC address	Location	Switch Port	IP Address	Software Version	Age	Status	Profile	Radio	Channel	Authenticated Clients
5c:d9:98:2f:4a:40		0/1	10.27.65.76	D.5.16.1	0h:1m:27s	Managed	1-Default	1-Sentry 2-802.11b/g/n	0 0	0 0
00:11:22:33:44:e0		N/A	N/A	N/A	4h:5m:27s	Rogue	N/A	802.11a	149	N/A

Figure 444: All AP Status with Rogue

Click the MAC address of the rogue AP to view additional information about the AP.

AP RF Scan Status			
MAC address	00:11:22:33:44:e0	BSSID	00:11:22:33:44:e0
SSID	Corporate	Physical Mode	802.11a
Channel	149	Security Mode	Open
Status	Rogue	802.11n Mode	Supported
Initial Status	Rogue	Beacon Interval	100 msec
Transmit Rate	6 Mbps	Highest Supported Rate	300 Mbps
WIDS Rogue AP Mitigation	AP Attack is Disabled	Peer Managed AP	
Age	0d:00:02:53	Ad hoc Network	Not Ad hoc
Discovered Age	0d:04:09:30	OUI Description	CIMSYS Inc

Refresh

Figure 445: Honeypot AP Rogue Status

Click the **WIDS AP Rogue Classification** tab to learn which WIDS test triggered the rogue status.

Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Administrator configured rogue AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Managed SSID from an unknown AP	True	5c:d9:98:2f:4a:40	1	Enabled	Rogue	0d:04:10:48	0d:00:04:11
Managed SSID from a fake managed AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
AP without an SSID	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Fake managed AP on an invalid channel	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Managed SSID detected with incorrect security	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Invalid SSID from a managed AP	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
AP is operating on an illegal channel	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Standalone AP with unexpected configuration	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Unexpected WIDS device detected on network	False	None	0	Enabled		0d:00:00:00	0d:00:00:00
Unmanaged AP detected on wired network	False	None	0	Enabled		0d:00:00:00	0d:00:00:00

Figure 446: WIDS Test Discovers Rogue

As Figure 446 shows, the honeypot AP is identified as a rogue because it triggered the Managed SSID from an unknown AP test. In other words, the honeypot AP, which is an unknown AP to the company, is using the same SSID as the legitimate AP inside the building.

At this point, no further action is taken by the DWS-4000 Series switch because the AP deauthentication attack feature is disabled. To enable the AP to take further action, enable the AP De-Authentication Attack option on the **WLAN > Administration > Advanced Configuration > WIDS Security** tab.

Administrator configured rogue AP	Enable
Managed SSID from an unknown AP	Enable
Managed SSID from a fake managed AP	Enable
AP without an SSID	Enable
Fake managed AP on an invalid channel	Enable
Managed SSID detected with incorrect security	Enable
Invalid SSID from a managed AP	Enable
AP is operating on an illegal channel	Enable
Standalone AP with unexpected configuration	Enable
Unexpected WIDS device detected on network	Enable
Unmanaged AP detected on wired network	Enable
Rogue Detected Trap Interval (seconds)	300 (60 to 3600, 0 - Disable)
Wired Network Detection Interval (seconds)	60 (1 to 3600, 0 - Disable)
AP De-Authentication Attack	Enable

Figure 447: De-Authentication Attack Enabled

When the AP De-Authentication Attack is configured, the WIDS AP Rogue AP Mitigation field on the **AP RF Scan Status** page shows that the mitigation is in progress.

AP RF Scan Status			
MAC address	00:11:22:33:44:e0	BSSID	00:11:22:33:44:e0
SSID	Corporate	Physical Mode	802.11a
Channel	149	Security Mode	Open
Status	Rogue	802.11n Mode	Supported
Initial Status	Rogue	Beacon Interval	100 msec
Transmit Rate	6 Mbps	Highest Supported Rate	300 Mbps
WIDS Rogue AP Mitigation	In Progress	Peer Managed AP	
Age	0d:00:02:53	Ad hoc Network	Not Ad hoc
Discovered Age	0d:04:09:30	OUI Description	CMSYS Inc

Figure 448: Rogue AP Mitigation

You can also track the progress of the deauthentication attack on the **WLAN > Monitoring > Access Point > AP De-Authentication Attack Status** page.

AP De-Authentication Attack Status			
BSSID	Channel	Time Since Attack Started	RF Scan Report Age
00:11:22:33:44:E0	149	0d 00:00:25	0d 00:00:25

Figure 449: De-Authentication Attack Status

The AP deauthentication attack causes deauthentication frames to be sent to the rogue AP and to clients communicating with the rogue AP. All clients connected to the rogue AP will experience poor connectivity. The intent of the attack is to serve as a temporary measure until the rogue AP is located and disabled.



Note: Radios in non-sentry mode transmit deauthentication frames only on their active channel. Therefore, D-Link recommends that you deploy radios in sentry mode to effectively implement rogue AP deauthentication attacks.



Caution! The deauthentication attack interrupts communication between all APs designated as *rogue* and their stations. Therefore, it is important to make sure all rogue APs are truly rogue before initiating this attack.

Using WIDS/WIPS to Detect Rogue Clients

In addition to targeting Rogue APs, the DWS-4000 Series switch supports client-based security detection algorithms to help monitor and control wireless clients on the network.

To view and configure the WIDS and WIPS parameters for wireless clients, click **WLAN > Administration > Advanced Configuration > WIDS Security > Client Configuration**.

Figure 450 shows the default values on the WIDS configuration page for the client.

WIDS Client Configuration	
Not Present in OUI Database Test	Disable ▾
Known Client Database Test	Disable ▾
Configured Authentication Rate Test	Enable ▾
Configured Probe Requests Rate Test	Enable ▾
Configured De-Authentication Requests Rate Test	Enable ▾
Maximum Authentication Failures Test	Enable ▾
Authentication with Unknown AP Test	Disable ▾
Client Threat Mitigation	Disable ▾
Known Client Database Lookup Method	Local ▾
Known Client Database Radius Server Name	Default-RADIUS-Server
Rogue Detected Trap Interval (seconds)	300 (60 to 3600, 0 - Disable)
De-Authentication Requests Threshold Interval (seconds)	60 (1 to 3600)
De-Authentication Requests Threshold Value	10 (1 to 99999)
Authentication Requests Threshold Interval (seconds)	60 (1 to 3600)
Authentication Requests Threshold Value	10 (1 to 99999)
Probe Requests Threshold Interval (seconds)	60 (1 to 3600)
Probe Requests Threshold Value	120 (1 to 99999)
Authentication Failure Threshold Value	5 (1 to 99999)

Figure 450: WIDS Client Configuration

If a client exhibits suspicious behavior by triggering a test or exceeding the acceptable threshold values configured on the page, it is marked as Rogue. To view information about all detected clients, click **WLAN > Monitoring > Client > Detected Clients**. Click the MAC address of the client to access additional information, including the client's rogue classification.

Figure 451 shows a client that is identified as a rogue because the Authentication Failure Threshold Value configured on the **WIDS Client Configuration** page shown in Figure 451 on page 716 is five, and the client has failed the authentication 12 times.

Detected Client Status			
MAC address	48:60:bc:76:79:3e	Auth Msgs Recorded	0
Client Status	Rogue	Auth Collection Interval	0d:00:00:34
Authentication Status	Not Authenticated	Highest Auth Msgs	6
Threat Detection	Detected	De-Auth Msgs Recorded	0
Threat Mitigation Status	Not Done	De-Auth Collection Interval	0d:00:00:34
Time Since Entry Last Updated	0d:00:00:03	Highest De-Auth Msgs	6
Time Since Entry Create	0d:02:35:26	Authentication Failures	12
Client Name	UsersSmartphone	Probes Detected	34
RSSI	87	Broadcast BSSID Probes	17
Signal	-29	Broadcast SSID Probes	17
Noise	-78	Specific BSSID Probes	0
Probe Req Recorded	0	Specific SSID Probes	0
Probe Collection Interval	0d:00:00:34	Last Directed Probe BSSID	00:00:00:00:00:00
Highest Probes Detected	40	Last Directed Probe SSID	
Channel	6	Threat Mitigation Sent	0d:00:00:00
OUI Description	Unknown		

Figure 451: Excessive Authentication Failures

Click the **Rogue Classification** tab to view information about why the client is classified as a rogue.

WIDS Client Rogue Classification							
MAC Address : 48:60:bc:76:79:3e							
Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Known Client Database Test	False	1c:af:f7:1f:27:40	2	Disabled		3d:07:36:15	0d:00:00:17
Client exceeds configured rate for auth msgs	False	1c:af:f7:1f:27:40	2	Enabled		3d:07:36:15	0d:00:00:17
Client exceeds configured rate for probe msgs	False	1c:af:f7:1f:27:40	2	Enabled		3d:07:36:15	0d:00:00:17
Client exceeds configured rate for de-auth msgs	False	1c:af:f7:1f:27:40	2	Enabled		3d:07:36:15	0d:00:00:17
Client exceeds max failing authentications	True	1c:af:f7:1f:27:40	2	Enabled	Rogue	0d:00:00:17	0d:00:00:17
Known Client authenticated with unknown AP	False	1c:af:f7:1f:27:40	2	Disabled		3d:07:36:15	0d:00:00:17
Client OUI not in the OUI Database	True	1c:af:f7:1f:27:40	2	Disabled		0d:02:31:55	0d:00:00:17

Figure 452: Client Rogue Classification

The WIDS client rogue classification information indicates that either the user has forgotten his password, or perhaps someone is trying to guess a password to gain access to the network. The network administrator should investigate further. Implementing features such as WLAN Visualization and the Device Locator can help locate the rogue client.

Mitigating a Rogue Client Threat

In this scenario, the network administrator for a retail store is implementing Rogue Client Threat Mitigation to provide additional security in her store located in a shopping mall. Several tablet PCs are used to track inventory within the establishment. The network administrator decides to use Client Threat Mitigation to make sure that these tablets are associated only with company-controlled APs.

This scenario uses Client Threat Mitigation rather than the AP De-Authentication Attack for the following reasons:

- Using AP Mitigation would be difficult because the administrator has no control over APs in adjoining stores, and keeping up with changes in APs located in other stores might create too much overhead.
- If the administrator were to accidentally classify a neighboring store's AP as Rogue and jam the other store's traffic, she could potentially be liable for interrupting the business of the adjacent store.
- Employees can be prevented from using the tablet PCs to access public networks for non work-related functions or to circumvent corporate firewalls, which could expose company data.



Note: Radios in non-sentry mode will not transmit Client Threat Mitigation frames. Therefore, sentry radios must be deployed for the network administrator to use this feature.

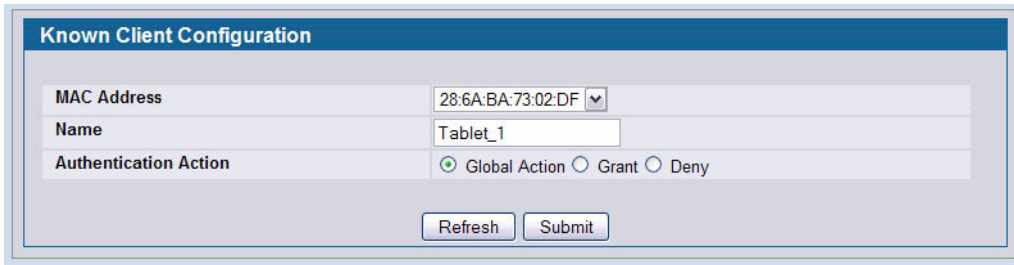
To add the the clients that are allowed to access the network into the Known Client Database and configure the Client Threat Mitigation feature:

1. Verify the MAC Authentication mode is *white-list* on the **WLAN > Administration > Advanced Configuration > Global** page.

The white-list authentication mode means that wireless clients with MAC addresses that are specified in the Known Client database, and are not explicitly denied access, are granted access. If the MAC address is not in the database then the access to the network is denied.

Wireless Global Configuration		
Peer Group ID	17	(1 to 255)
Client Roam Timeout (secs)	30	(1 to 120)
Ad Hoc Client Status Timeout (hours)	24	(0 to 168)
AP Failure Status Timeout (hours)	24	(0 to 168)
MAC Authentication Mode	white-list	▼
RF Scan Status Timeout (hours)	24	(0 to 168)
Detected Clients Status Timeout (hours)	24	(0 to 168)
AP Provisioning Database Age Time(hours)	72	(0 to 240)
Tunnel IP MTU Size	1500	▼
Cluster Priority	1	(0 to 255, 0-Disable)
AP Client QoS	Disable	▼
TSPEC Violation Report Interval (secs)	300	(0 to 900, 0 - Disable)
Base IP Port	57775	(1 to 65000)

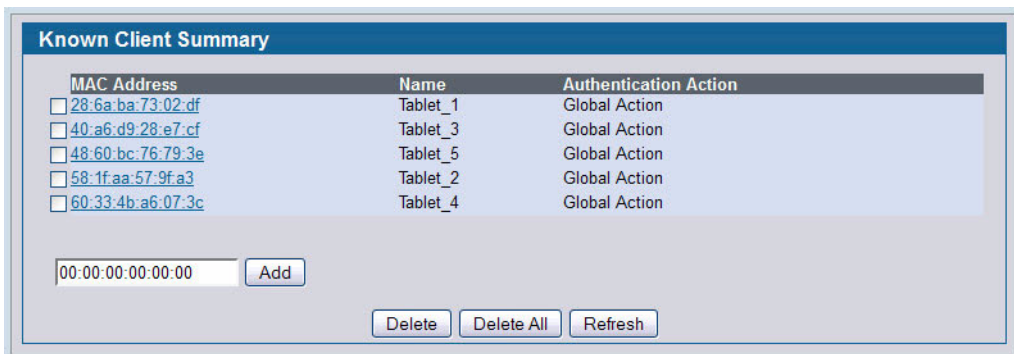
2. On the **WLAN > Administration > Advanced Configuration > Clients > Known Clients** page, type the MAC addresses of a tablet PC into the available field.
3. Click **Add**.
The **Known Client Configuration** page appears.



The image shows the 'Known Client Configuration' form. It has three input fields: 'MAC Address' with a dropdown menu showing '28:6A:BA:73:02:DF', 'Name' with a text box containing 'Tablet_1', and 'Authentication Action' with radio buttons for 'Global Action' (selected), 'Grant', and 'Deny'. At the bottom are 'Refresh' and 'Submit' buttons.

The default authentication action is Global Action, which means the switch uses the white-list authentication mode as specified on the **Wireless Global Configuration** page. Only the MAC addresses in the Known Client database are marked as Known Clients.

4. Specify a name to identify the client in the **Name** field
5. Click **Submit**.
6. Repeat [Step 2–Step 5](#) until all allowed clients are in the Known Clients database.



The image shows the 'Known Client Summary' table. It has three columns: 'MAC Address', 'Name', and 'Authentication Action'. Below the table is an 'Add' button with a text box containing '00:00:00:00:00:00'. At the bottom are 'Delete', 'Delete All', and 'Refresh' buttons.

MAC Address	Name	Authentication Action
<input type="checkbox"/> 28:6a:ba:73:02:df	Tablet_1	Global Action
<input type="checkbox"/> 40:a6:d9:28:e7:cf	Tablet_3	Global Action
<input type="checkbox"/> 48:60:bc:76:79:3e	Tablet_5	Global Action
<input type="checkbox"/> 58:1f:aa:57:9f:a3	Tablet_2	Global Action
<input type="checkbox"/> 60:33:4b:a6:07:3c	Tablet_4	Global Action

7. To configure the client-based WIDS security tests and enable the client threat mitigation feature, go to the **WLAN > Administration > Advanced Configuration > WIDS Security > Client Configuration** page and configure the following settings:
 - a. Set the Known Client Database Test to Enable
 - b. Set Authentication with Unknown AP Test to Enable
 - c. Set Client Threat Mitigation to Enable

AP Configuration Client Configuration

WIDS Client Configuration

Not Present in OUI Database Test	Disable
Known Client Database Test	Enable
Configured Authentication Rate Test	Enable
Configured Probe Requests Rate Test	Enable
Configured De-Authentication Requests Rate Test	Enable
Maximum Authentication Failures Test	Enable
Authentication with Unknown AP Test	Enable
Client Threat Mitigation	Enable
Known Client Database Lookup Method	Local
Known Client Database Radius Server Name	Default-RADIUS-Server
Rogue Detected Trap Interval (seconds)	300 (60 to 3600, 0 - Disable)
De-Authentication Requests Threshold Interval (seconds)	60 (1 to 3600)
De-Authentication Requests Threshold Value	10 (1 to 99999)
Authentication Requests Threshold Interval (seconds)	60 (1 to 3600)
Authentication Requests Threshold Value	10 (1 to 99999)
Probe Requests Threshold Interval (seconds)	60 (1 to 3600)
Probe Requests Threshold Value	120 (1 to 99999)
Authentication Failure Threshold Value	5 (1 to 99999)

Submit Refresh

- View information about all detected clients on the **WLAN > Monitoring > Client > Detected Clients** page. In the following figure, the Known Client is shown as Authenticated while it is associated to the Corporate SSID. Other detected clients have failed the Known Clients Database test and are listed as Rogue.

Detected Client Summary Pre-Authentication History Summary Roam History Summary

Detected Client Status

MAC Address	Client Name	Client Status	Age	Create Time
<input type="checkbox"/> 00:27:10:99:45:d8		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> 0c:60:76:4f:56:a9		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> 18:3d:a2:30:bf:0c		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> 18:3d:a2:35:bb:1c		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> 40:5f:be:90:ef:90		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> 48:60:bc:76:79:3a	Tablet 5	Authenticated	0d:00:00:05	0d:19:49:49
<input type="checkbox"/> 68:94:6b:7c:c0:60		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> 68:94:6b:91:5e:00		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> 5c:d9:98:2f:4c:c0		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> 5c:d9:98:2f:52:40		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> 90:27:e4:55:27:7b		Rogue	0d:00:00:17	0d:00:00:17
<input type="checkbox"/> c0:18:da:3b:32:fc		Rogue	0d:00:00:17	0d:00:00:17

12

Delete Delete All Acknowledge All Rogues Refresh



Note: If the client status for some clients stays as *Detected*, check the age of the connection. Rogue classification is performed only on current clients and only when the Known Clients Database Test is enabled. Clients that existed in the Detected Clients database prior to the activation of the Known Clients Database Test and are no longer present will **not** be tagged as Rogue.

If an employee using Tablet_5 attempts to use an unknown AP with one of the tablets, the DWS-4000 Series switch initiates a Client Threat Mitigation attack. The **WLAN > Monitoring > Client > Detected Clients** page shows that the Tablet_5 client now has a client status of Rogue.

MAC Address	Client Name	Client Status	Age	Create Time
48-60-bc-76-79-3e	Tablet_5	Rogue	0d:00:00:02	1d 00:47:43
48-60-bc-a1-25-7f		Rogue	0d:00:03:04	0d 04:08:31
50-ea-d6-0c-87-d0		Rogue	0d:00:18:35	0d 04:01:02
58-1f-aa-5e-b1-5c		Rogue	0d:00:00:02	0d 04:34:38
58-1f-aa-82-7c-17		Rogue	0d:00:54:09	0d 04:36:40
58-55-ca-cd-53-0d		Rogue	0d:00:07:01	0d 04:49:10
58-94-6b-41-2d-a4		Rogue	0d:00:18:06	0d 04:54:41
58-94-6b-76-c6-08		Rogue	0d:00:05:32	0d 00:38:07
58-94-6b-7c-85-60		Rogue	0d:00:20:33	0d 04:53:11

Click the MAC address of the client to display the client’s Detected Client Status page. As the following figure shows, the client is detected as a threat, and the threat mitigation feature caused the AP to send a deauthentication request to the client. Traffic transmitted by the rogue tablet is interrupted, and it is not able to remain associated with the unknown AP.

Detected Client Status		Rogue Classification		Pre-Auth History		Triangulation		Roam History	
MAC address	48-60-bc-76-79-3e	Auth Msgs Recorded	0	Auth Collection Interval	0d:00:00:01	Highest Auth Msgs	6	De-Auth Msgs Recorded	0
Client Status	Known	De-Auth Collection Interval	0d:00:00:01	Highest De-Auth Msgs	6	Authentication Failures	0	Probes Detected	42
Authentication Status	Not Authenticated	Broadcast BSSID Probes	21	Broadcast SSID Probes	21	Specific BSSID Probes	0	Specific SSID Probes	0
Threat Detection	Detected	Last Directed Probe BSSID	00:00:00:00:00:00	Last Directed Probe SSID		Threat Mitigation Sent	0d:00:06:21		
Threat Mitigation Status	Done								
Time Since Entry Last Updated	0d:00:00:18								
Time Since Entry Create	1d 00:37:59								
Client Name	Tablet_5								
RSSI	77								
Signal	-36								
Noise	-92								
Probe Req Recorded	43								
Probe Collection Interval	0d:00:00:01								
Highest Probes Detected	50								
Channel	6								
OUI Description	Unknown								

Click the **Rogue Classification** tab to confirm the WIDS security test results for the client.

Detected Client Status		Rogue Classification	Pre-Auth History	Triangulation	Roam History		
WIDS Client Rogue Classification							
MAC Address : 48:60:bc:76:79:3e							
Test Description	Condition Detected	Reporting MAC Address	Radio	Test Config	Test Result	Time Since First Report	Time Since Last Report
Known Client Database Test	False	1c:af:f7:1f:27:40	1	Enabled		4d 05:31:08	0d 00:03:08
Client exceeds configured rate for auth msgs	False	1c:af:f7:1f:27:40	1	Enabled		4d 05:31:08	0d 00:03:08
Client exceeds configured rate for probe msgs	False	1c:af:f7:1f:27:40	1	Enabled		4d 05:31:08	0d 00:03:08
Client exceeds configured rate for de-auth msgs	False	1c:af:f7:1f:27:40	1	Enabled		4d 05:31:08	0d 00:03:08
Client exceeds max failing authentications	False	1c:af:f7:1f:27:40	1	Enabled		4d 05:31:08	0d 00:03:08
Known client authenticated with unknown AP	True	1c:af:f7:1f:27:40	1	Enabled	Rogue	0d 00:09:11	0d 00:03:08
Client OUI not in the OUI Database	True	1c:af:f7:1f:27:40	1	Disabled		1d 00:26:48	0d 00:03:08
<input type="button" value="Refresh"/>							

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below ("Hardware") will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below ("Warranty Period"), except as otherwise stated herein.

Limited Lifetime Warranty for the product is defined as follows:

- Hardware: For as long as the original customer/end user owns the product, or five (5) years after product discontinuance, whichever occurs first (excluding power supplies and fans)
- Power supplies and fans: Three (3) Year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.com/>.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

Copyright Statement: No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice. Copyright 2004 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning: This is a Class A product. In a residential environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. Operation of this equipment in a residential environment is likely to cause harmful interference to radio or television reception. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Product Registration

Register your D-Link product online at <http://support.dlink.com/register/>

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Tech Support

Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the service period, and warranty confirmation service, during the warranty period on this product. U.S. and Canadian customers can contact D-Link technical support through our website, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

USA - 877-DLINK-55 (877-354-6555)

D-Link Technical Support over the Internet:

<http://support.dlink.com>

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

877-354-6560

D-Link Technical Support over the Internet:

<http://support.dlink.com>

D-Link[®]
Building Networks for People

Technical Support

United Kingdom (Mon-Fri)

Home Wireless/Broadband 0871 873 3000 (9.00am–06.00pm, Sat 10.00am-02.00pm)
Managed, Smart, & Wireless Switches, or Firewalls 0871 873 0909 (09.00am – 05.30pm)
(BT 10ppm, other carriers may vary.)

Ireland (Mon-Fri)

All Products 1890 886 899 (09.00am-06.00pm, Sat 10.00am-02.00pm)
€ 0.05ppm peak, €0.045ppm off peak Times

Internet

<http://www.dlink.co.uk>

<ftp://ftp.dlink.co.uk>

Technische Unterstützung

Deutschland:	Web:	http://www.dlink.de
	Telefon:	+49(0)1805 2787 0,14 € pro Minute
	Zeiten:	Mo. –Fr. 09:00 – 17:30 Uhr
Österreich:	Web:	http://www.dlink.at
	Telefon:	+43(0)820 480084 0,116 € pro Minute
	Zeiten:	Mo. –Fr. 09:00 – 17:30 Uhr
Schweiz:	Web:	http://www.dlink.ch
	Telefon:	+41(0)848 331100 0,08 CHF pro Minute
	Zeiten:	Mo. –Fr. 09:00 – 17:30 Uhr

* Gebühren aus Mobilnetzen und von anderen Providern können abweichen.

Assistance technique

Assistance technique D-Link sur internet : <http://www.dlink.fr>

Assistance technique D-Link par téléphone : 0820 0803 03

0.12 € TTC/min depuis un poste fixe

Du lundi au vendredi de 9h à 19h (hors jours fériés)

Asistencia Técnica

Asistencia Técnica Telefónica de D-Link: +34 902 30 45 45

0,067 €/min

De Lunes a Viernes de 9:00 a 19:00

<http://www.dlink.es>

Supporto tecnico

Supporto Tecnico dal lunedì al venerdì dalle ore 9.00 alle ore 19.00 con orario continuato

Telefono: 02 87366396

<http://www.dlink.it/support>

TECHNISCHE ONDERSTEUNING

Technische ondersteuning voor klanten in Nederland:

www.dlink.nl / 0900 501 2007 / €0.15per minuut.

Tech Support for customers within Belgium:

www.dlink.be / 070 66 06 40 / €0.175per minuut(spitsuren), €0.0875per minuut(daluren)

Technische ondersteuning voor klanten in Luxemburg:

www.dlink.be / +32 70 66 06 40

Pomoc techniczna

Telefoniczna pomoc techniczna firmy D-Link: 0 801 022 021

Pomoc techniczna firmy D-Link świadczona przez Internet:

<http://www.dlink.eu/support/>

Technická podpora

Web: <http://www.dlink.cz/support/>

E-mail: support@dlink.cz

Telefon ČR: +420 211 151 640 nebo SK: +421 (0)692 147 110

Telefonická podpora je v provozu: PO - PÁ od 09:00 do 17:00

Volání je zpoplatněno dle příslušných tarifů Vašeho operátora.

Technikai Támogatás

Tel. : 06 1 461-3001

Fax : 06 1 461-3004

Land Line 14,99 HUG/min - Mobile 49.99,HUF/min

email : support@dlink.hu

URL : <http://www.dlink.hu>

Teknisk Support

D-Link Teknisk Support over Internett: <http://www.dlink.no>

D-Link Teknisk telefonsupport: 820 00 755

(Hverdager 08:00-20:00)

Teknisk Support

D-Link teknisk support over telefonen: Tlf.: 9013 8899

Normale åbningstider: Hverdage kl. 08:00 - 20:00

D-Link teknisk support på Internettet: <http://www.dlink.dk>

Teknistä tukea asiakkaille Suomessa:

Internetin kautta : <http://www.dlink.fi>

Arkisin klo. 9 - 21

Numerosta : 0600 155 57

Teknisk Support

D-Link Teknisk Support via Internet: <http://www.dlink.se>

D-Link Teknisk Support via telefon: 0900-100 77 00

Vardagar 08:00-20:00

Assistência Técnica

Assistência Técnica da D-Link na Internet:

<http://www.dlink.pt>

e-mail: soporte@dlink.es

Τεχνική Υποστήριξη

D-Link Hellas Support Center

Κεφαλληνίας 64, 11251 Αθήνα,

Τηλ: 210 86 11 114 (Δευτέρα- Παρασκευή 09:00-17:00)

Φαξ: 210 8611114

<http://www.dlink.gr/support>

Tehnička podrška

Hvala vam na odabiru D-Link proizvoda. Za dodatne informacije, podršku i upute za korištenje uređaja, molimo vas da posjetite D-Link internetsku stranicu na www.dlink.eu
www.dlink.biz/hr

Tehnična podpora

Zahvaljujemo se vam, ker ste izbrali D-Link proizvod. Za vse nadaljnje informacije, podporo ter navodila za uporabo prosimo obiščite D-Link - ovo spletno stran www.dlink.eu
www.dlink.biz/sl

Suport tehnic

Vă mulțumim pentru alegerea produselor D-Link. Pentru mai multe informații, suport și manuale ale produselor vă rugăm să vizitați site-ul D-Link www.dlink.eu
www.dlink.ro

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers in

Australia:

Tel: 1300-766-868
24/7 Technical Support
Web: <http://www.dlink.com.au>
E-mail: support@dlink.com.au

India:

Tel: +91-22-27626600
Toll Free 1800-22-8998
Web: www.dlink.co.in
E-Mail: helpdesk@dlink.co.in

Singapore, Thailand, Indonesia, Malaysia, Philippines, Vietnam:

Singapore - www.dlink.com.sg
Thailand - www.dlink.co.th
Indonesia - www.dlink.co.id
Malaysia - www.dlink.com.my
Philippines - www.dlink.com.ph
Vietnam - www.dlink.com.vn

Korea:

Tel : +82-2-2028-1810
Monday to Friday 9:00am to 6:00pm
Web : <http://d-link.co.kr>
E-mail : g2b@d-link.co.kr

New Zealand:

Tel: 0800-900-900
24/7 Technical Support
Web: <http://www.dlink.co.nz>
E-mail: support@dlink.co.nz

South Africa and Sub Sahara Region:

Tel: +27 12 661 2025
08600 DLINK (for South Africa only)
Monday to Friday 8:30am to 9:00pm South Africa Time
Web: <http://www.d-link.co.za>
E-mail: support@d-link.co.za

Saudi Arabia (KSA):

Tel: +966 01 217 0008
Fax: +966 01 217 0009
Saturday to Wednesday 9.30AM to 6.30PM
Thursdays 9.30AM to 2.00 PM
E-mail: Support.sa@dlink-me.com

D-Link Middle East - Dubai, U.A.E.

Plot No. S31102,
Jebel Ali Free Zone South,
P.O.Box 18224, Dubai, U.A.E.
Tel: +971-4-8809022
Fax: +971-4-8809066 / 8809069
Technical Support: +971-4-8809033
General Inquiries: info.me@dlink-me.com
Tech Support: support.me@dlink-me.com

Egypt

1, Makram Ebeid Street - City Lights Building
Nasr City - Cairo, Egypt
Floor 6, office C2
Tel.: +2 02 26718375 - +2 02 26717280
Technical Support: +2 02 26738470
General Inquiries: info.eg@dlink-me.com
Tech Support: support.eg@dlink-me.com

Kingdom of Saudi Arabia

Office # 84 ,
Al Khaleej Building (Mujamathu Al-Khaleej)
Opp. King Fahd Road, Olaya
Riyadh - Saudi Arabia
Tel: +966 1 217 0008
Technical Support:
+966 1 2170009 / +966 2 6522951
General Inquiries: info.sa@dlink-me.com
Tech Support: support.sa@dlink-me.com

Pakistan

Islamabad Office:
61-A, Jinnah Avenue, Blue Area,
Suite # 11, EBC, Saudi Pak Tower,
Islamabad - Pakistan
Tel.: +92-51-2800397, 2800398
Fax: +92-51-2800399

Karachi Office:

D-147/1, KDA Scheme # 1,
Opposite Mudassir Park, Karsaz Road,
Karachi - Pakistan
Phone: +92-21-34548158, 34326649
Fax: +92-21-4375727
Technical Support: +92-21-34548310, 34305069
General Inquiries: info.pk@dlink-me.com
Tech Support: support.pk@dlink-me.com

Technical Support

You can find software updates and user documentation on the D-Link website.

Tech Support for customers in

Iran

Unit 5, 5th Floor, No. 20, 17th Alley , Bokharest
St. , Argentine Sq. ,
Tehran IRAN
Postal Code : 1513833817
Tel: +98-21-88880918,19
+98-21-88706653,54
General Inquiries: info.ir@dlink-me.com
Tech Support: support.ir@dlink-me.com

Morocco

M.I.T.C
Route de Nouaceur angle RS et CT 1029
Bureau N° 312 ET 337
Casablanca , Maroc
Phone : +212 663 72 73 24
Email: support.na@dlink-me.com

Lebanon RMA center

Dbayeh/Lebanon
PO Box:901589
Tel: +961 4 54 49 71 Ext:14
Fax: +961 4 54 49 71 Ext:12
Email: taoun@dlink-me.com

Bahrain

Technical Support: +973 1 3332904

Kuwait:

Technical Support: + 965 22453939 / +965
22453949

Türkiye Merkez İrtibat Ofisi

Ayazağa Maslak yolu
Erdebil Cevahir İş Merkezi No: 5/A Ayazağa /
Maslak İstanbul
Tel: +90 212 2895659
Ücretsiz Müşteri Destek Hattı: 0 800 211 00 65
Web:www.dlink.com.tr
Teknik Destek: support.tr@dlink.com.tr

Israel

רח' המגשימים 20
קרית מטלון, פ"ת 49348
ת.ד. 7060
טלפון: 77-11-277-073
אי-מאייל כללי: info@dlink.co.il
אי-מאייל תמיכה: support@dlink.co.il

Техническая поддержка

Обновления программного обеспечения и документация доступны на Интернет-сайте D-Link. D-Link предоставляет бесплатную поддержку для клиентов в течение гарантийного срока. Клиенты могут обратиться в группу технической поддержки D-Link по телефону или через Интернет.

Техническая поддержка D-Link:

+7(495) 744-00-99

Техническая поддержка через Интернет

<http://www.dlink.ru>

e-mail: support@dlink.ru

Офисы

Украина,

04080 г. Киев , ул. Межигорская, 87-А, офис 18

Тел.: +38 (044) 545-64-40

E-mail: kiev@dlink.ru

Беларусь

220114, г. Минск, проспект Независимости,
169 , БЦ "XXI Век"

Тел.: +375(17) 218-13-65

E-mail: minsk@dlink.ru

Казахстан,

050008, г. Алматы, ул. Курмангазы, дом 143
(уг. Муканова)

Тел./факс: +7 727 378-55-90

E-mail: almaty@dlink.ru

Узбекистан

100015, г.Ташкент, ул. Нукусская, 89

Тел./Факс: +998 (71) 120-3770, 150-2646

E-mail: tashkent@dlink.ru

Армения

0038, г. Ереван, ул. Абеяна, 6/1, 4 этаж

Тел./Факс: + 374 (10) 398-667

E-mail: erevan@dlink.ru

Грузия

0162, г. Тбилиси,

проспект Чавчавадзе 74, 10 этаж

Тел./Факс: + 995 (32) 244-563

Lietuva

09120, Vilnius, Žirmūnų 139-303

Tel./faks. +370 (5) 236-3629

E-mail: info@dlink.lt

Eesti

Peterburi tee 46-205

11415, Tallinn, Eesti , Susi Bürookeskus

tel +372 613 9771

e-mail: info@dlink.ee

Latvija

Mazā nometņu 45/53 (ieeja no Nāras ielas)

LV-1002, Rīga

tel.: +371 6 7618703 +371 6 7618703

e-pasts: info@dlink.lv

SOPORTE TÉCNICO

Usted puede encontrar actualizaciones de softwares o firmwares y documentación para usuarios a través de nuestro sitio www.dlinkla.com

SOPORTE TÉCNICO PARA USUARIOS EN LATINO AMERICA

Soporte técnico a través de los siguientes teléfonos de D-Link

PAIS	NUMERO
Argentina	0800 - 12235465
Chile	800 - 835465 ó (02) 5941520
Colombia	01800 - 9525465
Costa Rica	0800 - 0521478
Ecuador	1800 - 035465
El Salvador	800 - 6335
Guatemala	1800 - 8350255
México	01800 - 1233201
Panamá	011 008000525465
Perú	0800 - 00968
Venezuela	0800 - 1005767

Soporte Técnico de D-Link a través de Internet

Horario de atención Soporte Técnico en www.dlinkla.com

e-mail: soporte@dlinkla.com & consultas@dlinkla.com

D-Link®
Building Networks for People

Suporte Técnico

Caso tenha dúvidas na instalação do produto, entre em contato com o Suporte Técnico D-Link por:

Chat Online

www.dlink.com.br/suporte

E-mail

suporte@dlink.com.br

Back Office

backoffice@dlink.com.br *

*Acionar Garantia para 4 ou mais equipamentos

Telefones

São Paulo: (11) 2755-6950

*GO: 4052-1850 (Ligação local)

*Nordeste: 0800-7024104

*Demais Estados: 4062-1850 (Ligação local)

*Apenas Modems ADSL

Garantia diferenciada vendida pela internet. Agilidade e tranquilidade para suas atividades!

Conheça: <http://garantiapremium.dlink.com.br>

**Atendimento disponível das 9h as 21h de segunda a sexta
feira e aos sábados das 9h as 15h**

D-Link[®]
Building Networks for People

D-Link 友訊科技 台灣分公司 技術支援資訊

如果您還有任何本使用手冊無法協助您解決的產品相關問題，台灣地區用戶可以透過我們的網站、電子郵件或電話等方式與D-Link台灣地區技術支援工程師聯絡。

D-Link 免付費技術諮詢專線

0800-002-615

服務時間：週一至週五，早上9:00到晚上9:00

(不含周六、日及國定假日)

網 站：<http://www.dlink.com.tw>

電子郵件：dssqa_service@dlink.com.tw

如果您是台灣地區以外的用戶，請參考D-Link網站全球各地分公司的聯絡資訊以取得相關支援服務。

產品保固期限、台灣區維修據點查詢，請參考以下網頁說明：

<http://www.dlink.com.tw>

產品維修：

使用者可直接送至全省聯強直營維修站或請洽您的原購買經銷商。

D-Link[®]
Building Networks for People

Dukungan Teknis

Update perangkat lunak dan dokumentasi pengguna dapat diperoleh pada situs web D-Link.

Dukungan Teknis untuk pelanggan:

Dukungan Teknis D-Link melalui telepon:

Tel: +62-21-5731610

Dukungan Teknis D-Link melalui Internet:

Email : support@dlink.co.id

Website : <http://support.dlink.co.id>

D-Link[®]
Building Networks for People

Technical Support

この度は弊社製品をお買い上げいただき、誠にありがとうございます。
ございます。

下記弊社 Web サイトからユーザ登録及び新製品登録を
行っていただき、ダウンロードサービスにて
サポート情報、ファームウェア、ユーザマニュアルを
ダウンロードすることができます。

ディーリンクジャパン Web サイト

URL:<http://www.dlink-jp.com>

D-Link[®]
Building Networks for People

技术支持

办公地址：北京市东城区北三环东路 36 号 环球贸易中心 B 座
26F 02-05 室 邮编: 100013

技术支持中心电话：8008296688/ (028)66052968

技术支持中心传真：(028)85176948

各地维修中心地址请登陆官方网站查询

网址：<http://www.dlink.com.cn>

办公时间：周一到周五，早09:00到晚18:00

D-Link[®]
Building Networks for People

Registration Card

All Countries and Regions Excluding USA

Print, type or use block letters.

Your name: Mr./Ms _____

Organization: _____ Dept. _____

Your title at organization: _____

Telephone: _____ Fax: _____

Organization's full address: _____

Country: _____

Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____

Telephone: _____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?

Home Office Travel Company Business Home Business Personal Use

2. How many employees work at installation site?

1 employee 2-9 10-49 50-99 100-499 500-999 1000 or more

3. What network protocol(s) does your organization use ?

XNS/IPX TCP/IP DECnet Others _____

4. What network operating system(s) does your organization use ?

D-Link LANsmart Novell NetWare NetWare Lite SCO Unix/Xenix PC NFS 3Com 3+Open Cisco Network

Banyan Vines DECnet Pathwork Windows NT Windows 98 Windows 2000/ME Windows XP

Others _____

5. What network management program does your organization use ?

D-View HP OpenView/Windows HP OpenView/Unix SunNet Manager Novell NMS

NetView 6000 Others _____

6. What network medium/media does your organization use ?

Fiber-optics Thick coax Ethernet Thin coax Ethernet 10BASE-T UTP/STP

100BASE-TX 1000BASE-T Wireless 802.11b and 802.11g wireless 802.11a Others _____

7. What applications are used on your network?

Desktop publishing Spreadsheet Word processing CAD/CAM

Database management Accounting Others _____

8. What category best describes your company?

Aerospace Engineering Education Finance Hospital Legal Insurance/Real Estate Manufacturing

Retail/Chain store/Wholesale Government Transportation/Utilities/Communication VAR

System house/company Other _____

9. Would you recommend your D-Link product to a friend?

Yes No Don't know yet

10. Your comments on this product?

PLEASE
PLACE STAMP
HERE

TO:

D-Link[®]