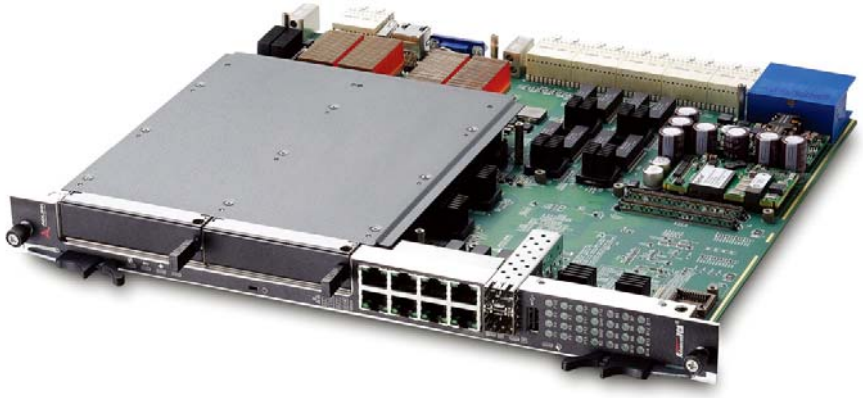
ADLINK TECHNOLOGY INC.

aTCA-3420

10GbE AdvancedTCA Fabric Interface Switch

User's Manual



Manual Revision: 2.00
Revision Date: February 18, 2013
Part Number: 50-1G020-1000

Advance Technologies; Automate the World.

Revision History

Revision	Release Date	Description of Change(s)
2.00	February 18, 2013	Initial release

Copyright 2013 ADLINK Technology, Inc.
All Rights Reserved.

The information in this document is subject to change without prior notice in order to improve reliability, design, and function and does not represent a commitment on the part of the manufacturer.

In no event will the manufacturer be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the product or documentation, even if advised of the possibility of such damages.

This document contains proprietary information protected by copyright. All rights are reserved. No part of this manual may be reproduced by any mechanical, electronic, or other means in any form without prior written permission of the manufacturer.

Trademarks

Product names mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective companies.

Table Of Contents

1. Overview 9
1.1 Introduction 9
1.2 Block Diagram 11
1.3 Package Contents 12
2. Specifications 13
2.1 aTCA-3420 Specifications 13
2.2 Placement 15
2.3 Front Panel Layout 16
2.3.1 LED Definitions 16
2.4 I/O Connectors 18
3. Hardware Platform Management 20
3.1 Platform Management Overview 20
3.2 IPMI Sensors 21
Get Sensor Reading (FRU Hotswap Sensor) 23
Get Sensor Reading (Physical IPMB-0 Sensor) 23
Watchdog Timer Sensor 25
Version Change Sensor 25
Get Sensor Reading Command 27
3.3 IPMI Commands 28
3.4 IPMI Firmware Upgrade Procedure 30
4. Getting Started 32
4.1 Safety Requirements 32
4.2 Blade Installation 33
4.3 Quick Start 35
Connecting to the aTCA-3420 35
Boot into SDK CLI for Base Switch (BCM56312) management 36
Boot into FASTPATH® CLI for Fabric Switch (BCM56800) initial setting 37
Update FASTPATH® Software 39
Login FASTPATH® GUI 42
5. Configure and Manage the Fabric Switch 44
5.1. Configuring System Information 45
Viewing Arp Cache 46
Viewing Inventory Information 47
Viewing The Dual Image Status 49
Viewing System Resources 50
5.2. Defining General Device Information 51
System Description 52
Switch Configuration 54
Service Port 55
Service Port NDP Summary 57
Network Connectivity 58
DHCP Client Options 60
HTTP Configuration 61

Telnet Session 63
Serial Port 65
User Accounts 66
Authentication List Configuration 69
Login Session 73
Authentication List Summary 74
Select Authentication List 76
Line Password 79
Enable Password 80
Password Management 81
Denial of Service 82
Configuring and Searching the Forwarding Database 86
Configuration 86
Search 87
5.3. Managing Logs 89
Buffered Log Configuration 90
Buffered Log 91
Command Logger Configuration 93
Console Log Configuration 94
Event Log 96
Hosts Configuration 97
Persistent Log Configuration 99
Persistent Log 102
Syslog Configuration 103
Configuring And Viewing Device Slot Information 105
Configuration 105
Slot Summary 107
Supported Cards 108
5.4. Configuring And Viewing Device Port Information 109
Configuration 110
Summary 113
Port Description 117
Cable Test 118
Multiple Port Mirroring 120
Adding a Port Mirroring Session 121
Configuring sFlow 122
sFlow Agent Summary 122
sFlow Receiver Configuration 124
sFlow Poller Configuration 125
Counter Sampling 125
sFlow Sampler Configuration 127
Packet Flow Sampling 127
Defining SNMP Parameters 129
SNMP V1 And V2 129
SNMP V3 129
SNMP Community Configuration 130
Trap Receiver Configuration 132
Supported MIBS 133
Viewing System Statistics 134
Switch Detailed 134

Switch Summary 136
Port Detailed 138
Port Summary 144
5.5. Using System Utilities 146
Save All Applied Changes 146
System Reset 148
Reset Configuration To Defaults 149
Erase Startup Config File 150
Reset Passwords To Defaults 151
Download File To Switch (TFTP) 152
Downloading a File to the Switch 154
Upload File From Switch (TFTP) 155
Dual Image Configuration 157
HTTP File Download 158
TraceRoute 161
AutoInstall 162
Managing SNMP Traps 164
Trap Flags 164
Trap Log 166
Managing The DHCP Server 167
Global Configuration 167
Pool Configuration 169
Pool Options 173
Reset Configuration 174
Bindings Information 175
Server Statistics 176
Conflicts Information 178
Configuring DNS 179
Global Configuration 179
Server Configuration 180
DNS Host Name IP Mapping Configuration 182
DNS Host Name IP Mapping Summary 183
Configuring SNTP Settings 185
SNTP Global Configuration 186
SNTP Global Status 188
SNTP Server Configuration 189
SNTP Server Status 191
Configuring And Viewing ISDP Information 193
Global Configuration 193
Cache Table 195
Interface Configuration 196
Statistics 197
5.6. Configuring Switching Information 199
Configuring DHCP Snooping 200
Global DHCP Snooping Configuration 201
DHCP Snooping VLAN Configuration 202
DHCP Snooping Interface Configuration 203
DHCP Snooping Binding Configuration 205
DHCP Snooping Persistent Configuration 208
DHCP Snooping Statistics 209

Configuring DHCP L2 Relay 210
DHCP L2 Relay Global Configuration 211
DHCP L2 Relay Interface Configuration 212
DHCP L2 Relay VLAN Configuration 213
DHCP L2 Relay Interface Statistics 214
5.7 Managing VLANS 216
VLAN Configuration 217
VLAN Status 219
VLAN Port Configuration 220
VLAN Port Summary 221
Reset VLAN Configuration 223
5.8 Double VLAN (DVLAN) Tunneling 224
DVLAN Config 225
DVLAN Summary 226
DVLAN Interface Config 227
DVLAN Interface Summary 228
Configuring Protected Ports 229
Protected Port Configuration 230
Protected Ports Summary 231
5.9 Managing Protocol-Based VLANS 232
Configuration 233
Protocol-Based VLAN Summary 234
5.10 Managing IP Subnet-Based VLANS 236
Configuration 237
Summary 238
MAC-Based VLAN Configuration 239
MAC-Based VLAN Summary 240
Voice VLAN Configuration 241
Creating MAC Filters 243
MAC Filter Configuration 243
Adding MAC Filters 244
Modifying MAC Filters 244
Deleting MAC Filters 244
MAC Filter Summary 245
5.11 Configuring GARP 246
GARP Status 247
GARP Switch Configuration 249
GARP Port Configuration 250
5.12 Configuring Dynamic ARP Inspection 252
DAI Configuration 253
DAI VLAN Configuration 254
DAI Interface Configuration 256
DAI ARP ACL CONFIGURATION 258
DAI ARP ACL Rule Configuration 259
DAI Statistics 260
5.13 Configuring IGMP Snooping 262
Global Configuration And Status 263
Interface Configuration 264
VLAN Status 266
VLAN Configuration 268

Multicast Router Status 270
Multicast Router Configuration 271
Multicast Router VLAN Status 272
Multicast Router VLAN Configuration 273
5.14 Configuring IGMP Snooping Queriers 274
IGMP Snooping Querier Configuration 275
IGMP Snooping Querier VLAN Configuration 276
IGMP Snooping Querier VLAN Configuration Summary 277
IGMP Snooping Querier VLAN Status 278
5.15 Configuring MLD Snooping 280
Configuration And Status 281
Interface Configuration 282
VLAN Status 284
VLAN Configuration 285
Multicast Router Status 287
Multicast Router Configuration 288
Multicast Router VLAN Status 289
Multicast Router VLAN Configuration 290
5.16 Configuring MLD Snooping Queriers 291
MLD Snooping Querier Configuration 292
MLD Snooping Querier VLAN Configuration 293
MLD Snooping Querier VLAN Configuration Summary 294
MLD Snooping Querier VLAN Status 295
5.17 Creating Port Channels 297
Port Channel Configuration 298
Port Channel Status 301
5.18 Viewing Multicast Forwarding Database Information 303
MFDB Table 304
MFDB GMRP Table 306
MFDB IGMP Snooping Table 307
MFDB MLD Snooping Table 308
MFDB Statistics 309
5.19 Configuring Spanning Tree Protocol 310
Switch Configuration/Status 311
CST Configuration/Status 313
MST Configuration/Status 315
CST Port Configuration/Status 317
MST Port Configuration/Status 320
Statistics 322
Mapping 802.1p Priority 323
5.20 Configuring Port Security 324
Port Security Administration 325
Port Security Interface Configuration 326
Port Security Static 328
Port Security Dynamic 329
Port Security Violation Status 330
5.21 Managing LLDP 331
Global Configuration 332
Interface Configuration 333
Interface Summary 335

Statistics 336
Local Device Information 338
Local Device Summary 339
Remote Device Information 340
Remote Device Summary 342
5.22 LLDP-MED 343
LLDP-MED Global Configuration 344
LLDP-MED Interface Configuration 345
LLDP-MED Interface Summary 347
LLDP Local Device Information 348
LLDP-MED Remote Device Information 350
5.23 Managing Device Security 352
Port Access Control 353
Global Port Access Control Configuration 354
Port Configuration 355
Port Status 358
Port Summary 362
Port Access Control Statistics 364
Client Summary 366
Client Detail 367
Port Access Privileges 368
Port Access Summary 369
5.24 RADIUS Settings 370
RADIUS Configuration 371
Server Configuration 373
Named Server Status Information 375
Server Statistics 377
Accounting Server Configuration 379
Named Accounting Server Status 381
Accounting Server Statistics 382
Clear Statistics 383
5.25 TACACS+ Settings 384
TACACS+ Configuration 385
TACACS+ Server Configuration 386
5.26 Secure HTTP 388
Secure HTTP Configuration 388
Generating Certificates 389
Downloading SSL Certificates 389
Secure Shell 391
Secure Shell Configuration 391
Safety Instructions **393**
Getting Service **394**

1. Overview

1.1 Introduction

The aTCA-3420 is a 20-port 10GbE Fabric Interface and 24-port GbE Base Interface AdvancedTCA® (ATCA) multilayer Switch Blade based on Broadcom BCM56800 and BCM56312 switch silicon. It supports up to thirteen 10GbE ports for a 14-slot PICMG 3.0 ATCA system, with six egress GbE ports and two 10GbE SFP+ uplink ports via front panel access. With optional AMC-3420 mezzanine card, users can have 4 additional SFP+ uplink ports for maximum connectivity. The ADLINK aTCA-3420 incorporates Broadcom's FASTPATH® networking software and is designed for ATCA adopters (NEPs & TEMs) who require AMC modularity, 10GbE layer 3 switching, a scalable control-plane engine and high-availability Fabric Interface.

The aTCA-3420 is ideal for ATCA platform adopters who require high speed and high bandwidth data transport interconnects for packet switching and highly flexible external I/O access. It meets the bandwidth-intensive switching requirements of applications such as IP Multimedia Subsystems (IMS) servers, media gateways, 3G wireless, network monitoring, Unified Threat Management servers, packet inspection servers and enterprise media servers.

ADLINK's aTCA-3420 is equipped with Broadcom's FASTPATH® networking software. The extensive feature set and integration capabilities of FASTPATH® enables powerful networking capabilities for the Fabric Interface. It also assists hardware in switching frames and provides comprehensive device management to the network administrator.

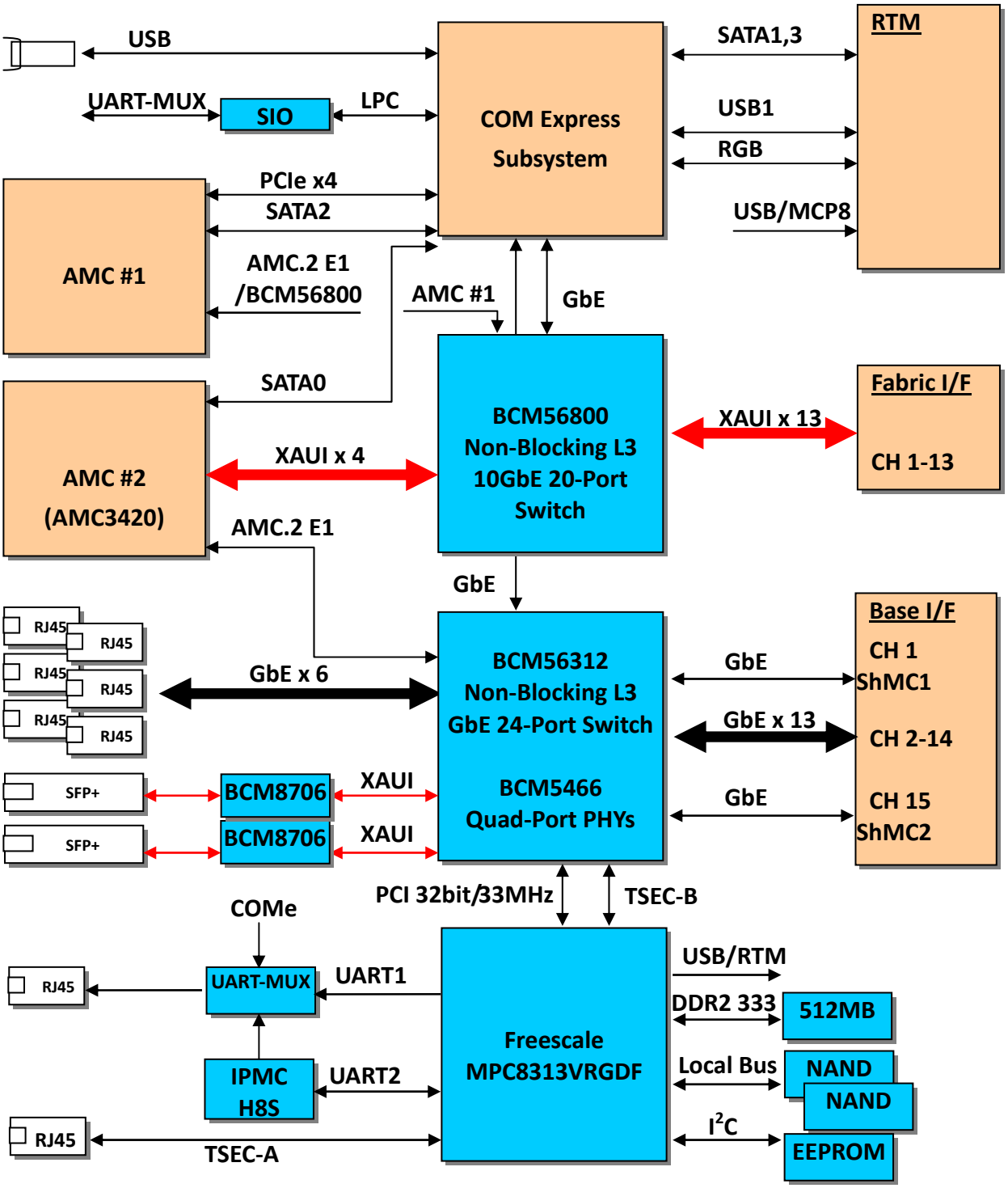
- Base Interface
  - 1000BASE-TX Gigabit Ethernet
  - Layer 3 switching
  - IPV4/IPV6 support
  - Base Interface support for 14 slot chassis
  - Base Interface support for Redundant Switch Card
  - Full speed non-blocking switching (port to port)
  - 6 Front Panel GbE ports (Base Interface access)
  - 2 10Gigabit Base uplink ports (Base Access)
  - Support for dual Ethernet Shelf Management Controllers (ShMC Port)

- Fabric Interface
  - 10GBASE-TX Gigabit Ethernet
  - Layer 3 switching
  - IPV4 support
  - Fabric Interface support for 14-slot chassis

- Fabric Interface support for Redundant Switch Card
- Full speed non-blocking switching (port to port)
- 4 Front Panel 10GbE SFP+ ports (optional with exclusive AMC-3420 card)

- Control Plane Processor
  - Configuration port (serial)
  - Freescale MPC8318E PowerQUICC II Pro 333MHz processor
  - 10/100/1000 Ethernet maintenance ports
  - 32-bit 33MHz PCI bus
  - Dual flash boot capabilities
  - IPM controller

1.2 Block Diagram



1.3 Package Contents

The aTCA-3420 is packaged with the components listed below. If any of the items in the contents list are missing or damaged, retain the shipping carton and packing material and contact the dealer for inspection. Please obtain authorization before returning any product to ADLINK. The packing contents of non-standard configurations may vary depending on customer requests.

- aTCA-3420 AdvancedTCA switch blade
- RJ-45 to DB9 adapter for UART

2. Specifications

2.1 aTCA-3420 Specifications

Core Logic

Data Plane **Switch ASIC/PHY**	Broadcom BCM56800 20-port 10Gigabit Ethernet switch Broadcom BCM56312 24-port Gigabit Ethernet switch Broadcom BCM5466 quad-port 10/100/1000BASE-T PHY Broadcom BCM54616S Single-port 10/100/1000BASE-T PHY Broadcom BCM8706 single-port 10GBASE-LRM PHY
Control Plane **Processor**	Freescale MPC8313E PoweQUICC-II Pro 333MHz DDR2 512MB SDRAM Dual 64MB boot flash

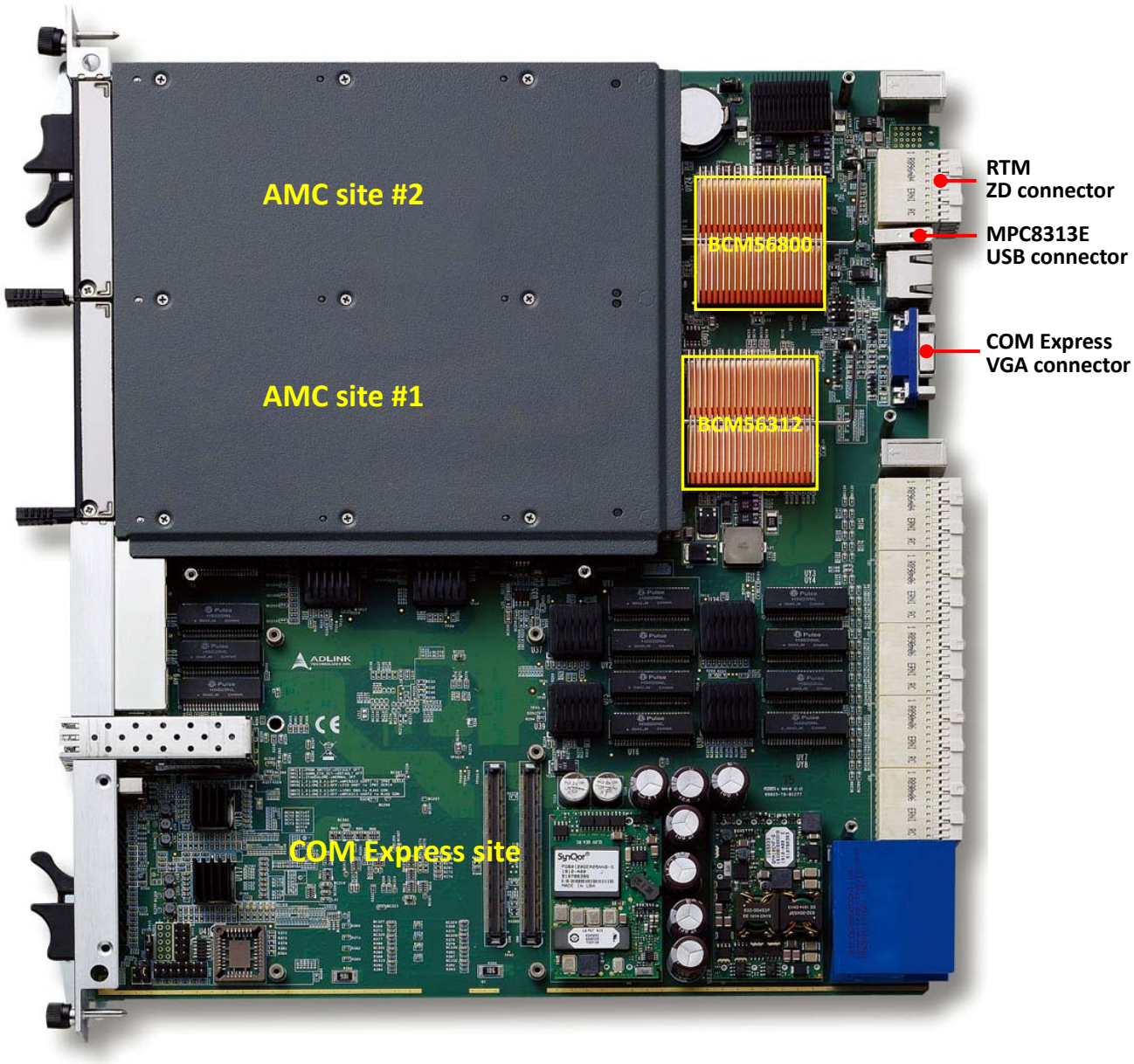
Standard and Interface

Standards	PICMG 3.0 R3.0 AdvancedTCA PICMG AMC.0 AdvancedMC
Networking	Fabric Interface switch: Thirteen 10GbE XAUI ports to backplane Zone 2 Four 10GbE XAUI ports to AMC#2 One 10/100/1000BASE-T port to COM Express GbE One 1000BASE-KX port to AMC site #1, AMC.2 E1
	Base Interface switch: Fifteen 10/100/1000BASE-T ports to backplane Zone2 2 for shelf managers, 13 for Base Interface channel 2-14 Six 10/100/1000BASE-T ports to front panel One 1000BASE-KX port to AMC site #2, AMC.2 E1 One 10/100/1000BASE-T port to COM Express GbE One 1000BASE-KX port to MPC8313E TSEC-B Dual 10GBASE-LRM SFP+ uplink ports to front panel
AMC Sites	Two Single width midsize AMC sites: AMC site #1, for COM Express IO expansion AMC.1 Type4 PCIe x4, driven by COM Express module AMC.3 S1 SATA, driven by COM Express module AMC site #2, for Base/Fabric Interface switch expansion AMC.2 E1 to Base Interface switch AMC.3 S1 SATA, driven by COM Express module AMC-3420 with Quad 10GBASE SFP+ port to Fabric Interfaceswitch (opt.)
COM Express Site	PICMG COM.0 Type 2 Validated with selected ADLINK COM Express modules
Front Panel IO	Six 10/100/1000BASE-T RJ45 jacks to Base Interface switch One 10/100/1000BASE-T RJ45 to MPC8313E TSEC-A service port One mux RS-232 RJ45 jack to MPC8313E/COM Express/IPMC Two 10GBASE-LRM SFP+ uplink ports to Base Interface switch
USB	One type A USB 2.0 port to COM Express module
Rear IO	DB-15 Analog RGB to COM Express module Type A USB 2.0 to MPC8313E ZD connector: Two SATA ports driven by COM Express module One USB port driven by COM Express module
Software	FASTPATH® Software for Fabric Switch (BCM56800) control Broadcom SDK for Base Switch (BCM56312) control

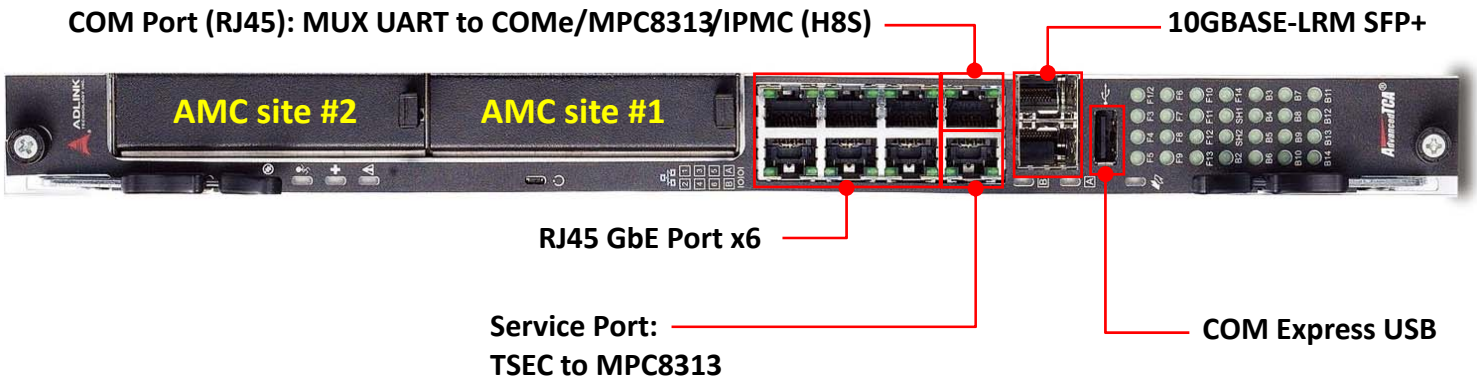
Mechanical & Environmental

Dimensions	322.25mm x 280mm x 30.48mm (H x D x W) - 6HP slot
Operating temperature	Standard: 0°C to 40°C NEBS short-term: 0°C to 55°C
Storage temperature	-40°C to 85°C
Humidity	5% to 90% non-condensing
Shock	15G peak-to-peak, 11ms duration, non-operation
Vibration	Non-operating: 1.88Grms, 5 to 500 Hz, each axis Operating: 0.5G rms. 5 to 500Hz, each axis
Compliance	CE, FCC Class A, CUL, NEBS Level 3 (design)
Power Consumption	DC40-70v, 48v nominal 75w typical, COM Express module not included

2.2 Placement



2.3 Front Panel Layout



2.3.1 LED Definitions

The following section explains the behavior of the LEDs on the front panel, including the Hot-Swap LED, OOS LED, Active LED, Healthy LED and Fault LED.

Hot-Swap, HS LED

Hot-Swap LED (Blue)	FRU State	Remark
Off	M0	FRU not installed
On	M1	FRU inactive
Long blink	M2	FRU activation request
Off	M3	FRU activation in process
Off	M4	FRU active
Short blink	M5	FRU deactivation request
Short blink	M6	FRU deactivation in process

Out-of-Service, OOS LED

Out–of-Service LED (Red)	State	Remark
Blink	Loading uBoot/OS POST	FRU State M4, active
Off	SDK/SW loaded OK	FRU State M4, active
On	uBoot not loaded or power down	FRU State M1, inactive

Active LED

User LED (Green)	State	Remark
Blink	SDK/SW loaded OK	
On	OS loaded OK	
Off	OS not loaded or power down	

Healthy LED

Healthy LED (Green)	State	Remark
On	uBoot loaded OK	
Off	uBoot not loaded or power down	

Fault LED

Fault LED (Amber)	State	Remark
On	Power failure	
Off	All power OK or power down	

Backplane GbE Status LEDs

SH1, SH2: Shelf manager 1 and 2
B[2:14]: Base Interface Channel 2 to 14
F[1/2:14]: Fabric Interface Channel 1/2 to 14

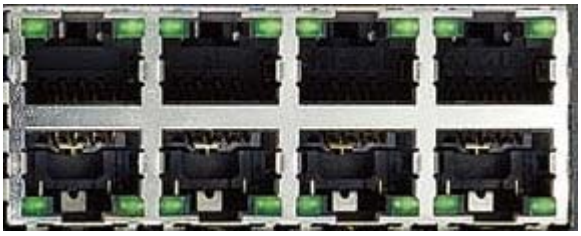
On: Link Up
Blink: Packet Activity
Off: Link Down



Front Panel GbE Status LEDs

Left LED:
On: Link Up
Off: Link Down

Right LED:
Blink: Packet Activity



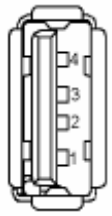
2.4 I/O Connectors

USB

The aTCA-3420 supports two USB 2.0 ports, one on the front panel driven by the COM Express module and the second in RTM Zone 3 space driven by the MPC8313E.

USB Connector

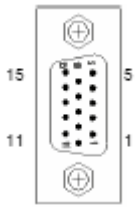
Pin	USB 2.0 Signal Names
1	VCC
2	Data-
3	Data+
4	GND



Analog RGB

The DB-15 female connector in Zone 3 space is for the COM Express site analog display output.

Pin	Name	Pin	Name
1	RED	9	+5v
2	GREEN	10	GND
3	BLUE	11	NC
4	NC	12	DDC_DATA
5	GND	13	HSYNC
6	GND	14	VSYNC
7	GND	15	DDC_CLK
8	GND		



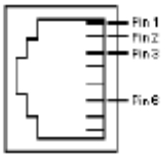
Serial Port

One PC-compatible serial RS-232 RJ45 port is provided on the front panel with DIP switches SW1 and SW2 (solder side near front panel) that are used to set the COM port function. A complete set of handshaking and modem control signals are supported, with data transfer rates up to 115.2 kB/sec.

The Front Panel RJ45 COM connector CN8 pin-assignment and DIP switch settings are described below.

COM Connector Pin Assignment

PIN	Signal Name	Function
1	DCD#	Data Carrier Detect
2	RTS#	Request to Send
3	DSR#	Data Set Ready
4	TXD	Transmit Data
5	RXD	Receive Data
6	GND	Ground
7	CTS#	Clear to Send
8	DTR#	Data Terminal Ready



COM Mode Switch Settings (SWX1 and SWX2)

(solder side near front panel)

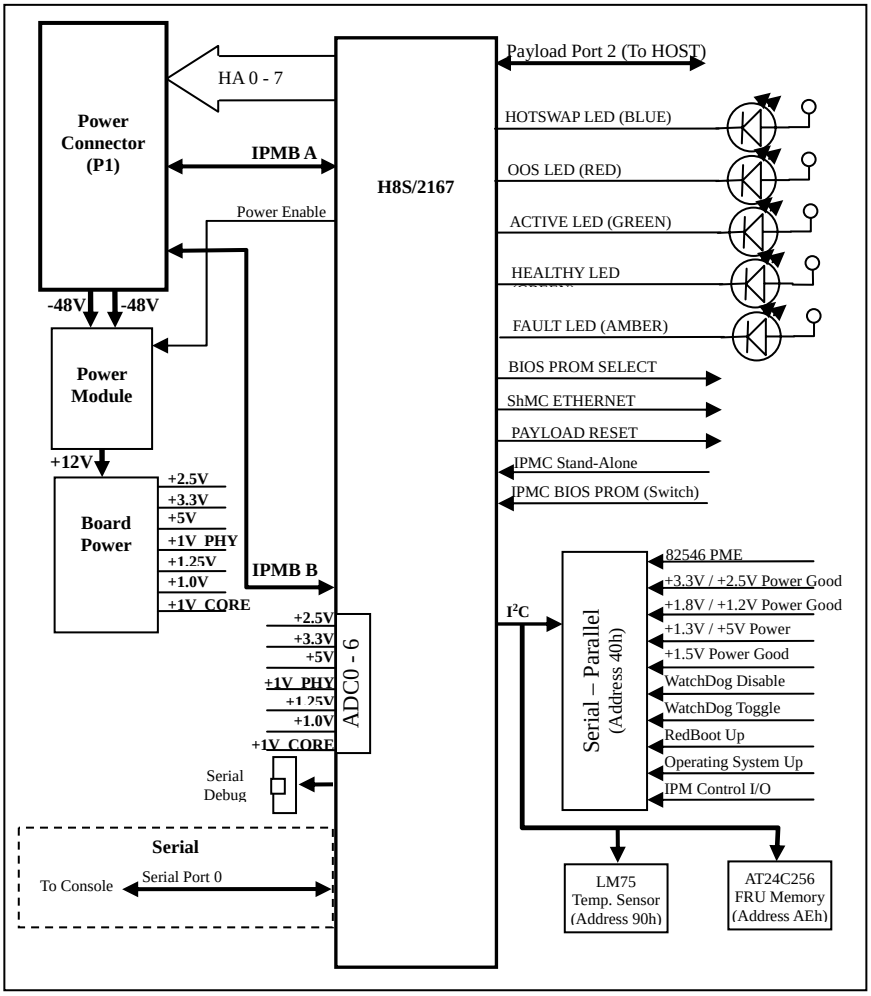
Configuration	**Switch**	**1**	**2**	**3**	**4**
RS-232 port (default)	**SWX1**	ON	ON	OFF	OFF
	SWX2	OFF	ON	N/A	
IPMC debug port	**SWX1**	OFF	OFF	ON	ON
	SWX2	ON	OFF	N/A	

3. Hardware Platform Management

3.1 Platform Management Overview

The purpose of the hardware platform management system is to monitor, control, and assure proper operation of AdvancedTCA® Boards and other shelf components. The hardware platform management system watches over the basic health of the system, reports anomalies, and takes corrective action when needed. The hardware platform management system can retrieve inventory information and sensor readings as well as receive event reports and failure notifications from boards and other intelligent FRUs. The hardware platform management system can also perform basic recovery operations such as power cycle or reset of managed entities.

The IPMC controller on the aTCA-3420 supports an “intelligent” hardware management system, based on the Intelligent Platform Management Interface Specification. The hardware management system provides the ability to manage the power, cooling, and interconnect needs of intelligent devices; to monitor events; and to log events to a central repository.



3.2 IPMI Sensors

Following table lists all the sensors supported by the aTCA-3420.

Sensor Name	Sensor Address	Description
Hot Swap	(0x0)	FRU Hotswap Sensor. Please refer to section 4.2.1
ShelfFRU HotSwap	(0x1)	FRU Hotswap Sensor. Please refer to section 4.2.1
Hot Swap AMC 1	(0x2)	AMC#1 Hotswap Sensor. Please refer to section 4.2.1
Hot Swap AMC 2	(0x3)	AMC#2 Hotswap Sensor. Please refer to section 4.2.1
Hot Swap AMC 2	(0x4)	RTM Hotswap Sensor. Please refer to section 4.2.1
Version change	(0x5)	Version Change Sensor. Please refer to section 4.2.4
IPMB Physical	(0x6)	Physical IPMB Sensor. Please refer to section 4.2.2
BMC Watchdog	(0x7)	Watchdog Timer Sensor. Please refer to section 4.2.3
+1.0V Core	(0x8)	Voltage Sensor. Please refer to section 4.2.5 Upper Non-Recoverable Threshold = 1.20 Volts Upper Critical Threshold = 1.15 Volts Upper Non-Critical Threshold = 1.10 Volts Lower Non-Critical Threshold = 0.90 Volts Lower Critical Threshold = 0.85 Volts Lower Non-Recoverable Threshold = 0.80 Volts
+1.0V	(0x9)	Voltage Sensor. Upper Non-Recoverable Threshold = 1.20 Volts Upper Critical Threshold = 1.15 Volts Upper Non-Critical Threshold = 1.10 Volts Lower Non-Critical Threshold = 0.90 Volts Lower Critical Threshold = 0.85 Volts Lower Non-Recoverable Threshold = 0.80 Volts
+1.25V	(0xA)	Voltage Sensor. Upper Non-Recoverable Threshold = 1.45 Volts Upper Critical Threshold = 1.4 Volts Upper Non-Critical Threshold = 1.35 Volts Lower Non-Critical Threshold = 1.15 Volts Lower Critical Threshold = 1.10 Volts Lower Non-Recoverable Threshold = 1.05 Volts
+1.0V PHY	(0xB)	Voltage Sensor. Upper Non-Recoverable Threshold = 1.20 Volts Upper Critical Threshold = 1.15 Volts Upper Non-Critical Threshold = 1.10 Volts Lower Non-Critical Threshold = 0.90 Volts Lower Critical Threshold = 0.85 Volts Lower Non-Recoverable Threshold = 0.80 Volts
+5V	(0xC)	Voltage Sensor. Upper Non-Recoverable Threshold = 5.5 Volts Upper Critical Threshold = 5.4 Volts

		Upper Non-Critical Threshold = 5.3 Volts Lower Non-Critical Threshold = 4.7 Volts Lower Critical Threshold = 4.6 Volts Lower Non-Recoverable Threshold = 4.5 Volts
+3.3V	(0xD)	Voltage Sensor. Upper Non-Recoverable Threshold = 3.63 Volts Upper Critical Threshold = 3.564 Volts Upper Non-Critical Threshold = 3.498 Volts Lower Non-Critical Threshold = 3.102 Volts Lower Critical Threshold = 3.036 Volts Lower Non-Recoverable Threshold = 2.97 Volts
LM75 SYS Temp	(0xE)	System Temperature. Please refer to section 4.2.5 Upper Non-Recoverable Threshold = 80 degrees C Upper Critical Threshold = 60 degrees C Upper Non-Critical Threshold = 50 degrees C
Flash Num	(0xF)	Discrete Sensor. Read boot flash number 0x01: Primary flash. 0x02: Secondary flash
Flash POST error	(0x10)	Discrete Sensor. Read flash POST status 0x80: Boot from primary flash OK. 0x40: Boot from secondary flash OK. 0x82: Boot from primary flash, but uBoot timeout. 0x42: Boot from secondary flash, but uBoot timeout 0x83: Boot from primary flash, but OS timeout 0x43: Boot from secondary flash, but OS timeout 0x84: Boot from primary flash, but SDK/SW timeout 0x44: Boot from secondary flash, but SDK/SW timeout
LM73 SYS Temp	(0x11)	System Temperature. Please refer to section 4.2.5 Upper Non-Recoverable Threshold = 80 degrees C Upper Critical Threshold = 60 degrees C Upper Non-Critical Threshold = 50 degrees C

Get Sensor Reading (FRU Hotswap Sensor)

	Byte	Data field
Request data	1	Sensor Number (FFh = reserved)
Response data	1	Completion Code
	2	Sensor Reading. [7:0] - Not used. Write as 00h.
	3	Standard IPMI byte (See “Get Sensor Reading” in IPMI specification): [7] - 0b = All Event Messages disabled from this sensor [6] - 0b = sensor scanning disabled [5] - 1b = initial update in progress. This bit is set to indicate that a “Re-arm Sensor Events” or “Set Event Receiver” command has been used to request an update of the sensor status, and that update has not occurred yet. Software should use this bit to avoid getting an incorrect status while the first sensor update is in progress. This bit is only required if it is possible for the IPM Controller to receive and process a “Get Sensor Reading or Get Sensor Event Status” command for the sensor before the update has completed. This is most likely to be the case for sensors, such as fan RPM sensors, that may require seconds to accumulate the first reading after a re-arm. [4:0] – reserved. Ignore on read.
	4	Current State Mask [7] – 1b = FRU Operational State M7 - Communication Lost [6] – 1b = FRU Operational State M6 - FRU Deactivation In Progress [5] – 1b = FRU Operational State M5 - FRU Deactivation Request [4] – 1b = FRU Operational State M4 - FRU Active [3] – 1b = FRU Operational State M3 - FRU Activation in Progress [2] – 1b = FRU Operational State M2 - FRU Activation Request [1] – 1b = FRU Operational State M1 - FRU Inactive [0] – 1b = FRU Operational State M0 - FRU Not Installed
	(5)	[7:0] – Optional/Reserved. If provided, write as 80h (IPMI restriction). Ignore on read.

Get Sensor Reading (Physical IPMB-0 Sensor)

	Byte	Data field
Request data	1	Sensor Number (FFh = reserved)
Response data	1	Completion Code
	2	[7] – IPMB B Override State 0b = Override state, bus isolated 1b = Local Control state - IPM Controller determines state of bus. [6:4] = IPMB B Local Status 0h = No Failure. Bus enabled if no override in effect. 1h = Unable to drive clock HI 2h = Unable to drive data HI

		3h = Unable to drive clock LO 4h = Unable to drive data LO 5h = Clock low timeout 6h = Under test (the IPM Controller is attempting to determine if it is causing a bus hang). 7h = Undiagnosed Communications Failure [3] – IPMB A Override State 0b = Override state, bus isolated 1b = Local Control state - IPM Controller determines state of bus. [2:0] = IPMB A Local Status 0h = No failure. Bus enabled if no override in effect. 1h = Unable to drive clock HI 2h = Unable to drive data HI 3h = Unable to drive clock LO 4h = Unable to drive data LO 5h = Clock low timeout 6h = Under test (the IPM Controller is attempting to determine if it is causing a bus hang). 7h = Undiagnosed Communications Failure
	3	Standard IPMI byte (see “Get Sensor Reading” in IPMI specification) [7] – 0b = All Event Messages disabled from this sensor [6] – 0b = Sensor scanning disabled [5] – 1b = Initial update in progress. This bit is set to indicate that a “Re-arm Sensor Events” or “Set Event Receiver” command has been used to request an update of the sensor status, and that update has not occurred yet. Software should use this bit to avoid getting an incorrect status while the first sensor update is in progress. This bit is only required if it is possible for the controller to receive and process a “Get Sensor Reading” or “Get Sensor Event Status” command for the sensor before the update has completed. This is most likely to be the case for sensors, such as fan RPM sensors, that may require seconds to accumulate the first reading after a re-arm. [4:0] – Reserved. Ignore on read.
	4	[7:4] – Reserved. Write as 0h, ignore on read [3] 1b = IPMB A enabled, IPMB-B enabled [2] 1b = IPMB A disabled, IPMB-B enabled [1] 1b = IPMB-A enabled, IPMB-B disabled [0] 1b = IPMB A disabled, IPMB-B disabled
	(5)	[7:0] – Optional/Reserved. If provided, write as 80h (IPMI restriction). Ignore on read.

Watchdog Timer Sensor

Sensor Type	Sensor Type Code	Sensor Specific Offset	Event
Watchdog 2	23h		This sensor is recommended for new IPMI v1.0 and later implementations.
		00h	Timer expired, status only (no action, no interrupt)
		01h	Hard Reset
		02h	Power Down
		03h	Power Cycle
		04h-07h	reserved
		08h	Timer interrupt
			The Event Data 2 field for this command can be used to provide an event extension code, with the following definition: 7:4 interrupt type 0h = none 1h = SMI 2h = NMI 3h = Messaging Interrupt Fh = unspecified all other = reserved 3:0 timer use at expiration: 0h = reserved 1h = BIOS FRB2 2h = BIOS/POST 3h = OS Load 4h = SMS/OS 5h = OEM Fh = unspecified all other = reserved

Version Change Sensor

Sensor Type	Sensor Type Code	Sensor Specific Offset	Event
Version Change	2Bh	00h	00h Hardware change detected with associated Entity. Informational. This offset does not imply whether the hardware change was successful or not. Only that a change occurred.
		01h	01h Firmware or software change detected with associated Entity.Informational. Success or failure not implied.
		02h	02h Hardware incompatibility detected with associated Entity.

		03h 04h 05h 06h 07h	03h Firmware or software incompatibility detected with associated Entity. 04h Entity is of an invalid or unsupported hardware version. 05h Entity contains an invalid or unsupported firmware or software version. 06h Hardware Change detected with associated Entity was successful. (deassertion event means unsuccessful'). 07h Software or F/W Change detected with associated Entity was successful. (deassertion event means 'unsuccessful') *Event data 2 can be used for additional event information on the type of version change, with the following definition:* Event Data 2 7:0 Version change type 00h unspecified 01h management controller device ID (change in one or more fields from 'Get Device ID') 02h management controller firmware revision 03h management controller device revision 04h management controller manufacturer ID 05h management controller IPMI version 06h management controller auxiliary firmware ID 07h management controller firmware boot block 08h other management controller firmware 09h system firmware (EFI / BIOS) change 0Ah SMBIOS change 0Bh operating system change 0Ch operating system loader change 0Dh service or diagnostic partition change 0Eh management software agent change 0Fh management software application change 10h management software middleware change 11h programmable hardware change (e.g. FPGA) 12h board/FRU module change (change of a module plugged into associated entity) 13h board/FRU component change (addition or removal of a replaceable component on the board/FRU that is not tracked as a FRU) 14h board/FRU replaced with equivalent version 15h board/FRU replaced with newer version 16h board/FRU replaced with older version 17h board/FRU hardware configuration change (e.g. strap, jumper, cable change, etc.)

Get Sensor Reading Command

	Byte	Data field
Request data	1	Sensor Number (FFh = reserved)
Response data	1	Completion Code
	2	Sensor reading Byte 1: byte of reading. Ignore on read if sensor does not return an numeric (analog) reading.
	3	[7] - 0b = All Event Messages disabled from this sensor [6] - 0b = sensor scanning disabled [5] - 1b = reading/state unavailable (formerly “initial update in progress”). This bit is set to indicate that a ‘re-arm’ or ‘Set Event Receiver’ command has been used to request an update of the sensor status, and that update has not occurred yet. Software should use this bit to avoid getting an incorrect status while the first sensor update is in progress. This bit is only required if it is possible for the controller to receive and process a ‘Get Sensor Reading’ or ‘Get Sensor Event Status’ command for the sensor before the update has completed. This is most likely to be the case for sensors, such as fan RPM sensors, that may require seconds to accumulate the first reading after a re-arm. The bit is also used to indicate when a reading/state is unavailable because the management controller cannot obtain a valid reading or state for the monitored entity, typically because the entity is not present. For more in formation, please see *Section 16.4, Event Status, Even Conditions, and Present State* and *Section 16.6, Re-arming* on the PICMG specification 3.0. [4:0] - reserved. Ignore on read.
	4	For threshold-based sensors Present threshold comparison status [7:6] - reserved. Returned as 1b. Ignore on read. [5] - 1b = at or above (≥) upper non-recoverable threshold [4] - 1b = at or above (≥) upper critical threshold [3] - 1b = at or above (≥) upper non-critical threshold [2] - 1b = at or below (≤) lower non-recoverable threshold [1] - 1b = at or below (≤) lower critical threshold [0] - 1b = at or below (≤) lower non-critical threshold For discrete reading sensors [7] - 1b = state 7 asserted [6] - 1b = state 6 asserted [5] - 1b = state 5 asserted [4] - 1b = state 4 asserted [3] - 1b = state 3 asserted [2] - 1b = state 2 asserted [1] - 1b = state 1 asserted [0] - 1b = state 0 asserted
	(5)	For discrete reading sensors only. (Optional) (00h Otherwise) [7] - reserved. Returned as 1b. Ignore on read. [6] - 1b = state 14 asserted

		[5] - 1b = state 13 asserted [4] - 1b = state 12 asserted [3] - 1b = state 11 asserted [2] - 1b = state 10 asserted [1] - 1b = state 9 asserted [0] - 1b = state 8 asserted

3.3 IPMI Commands

The following table presents all the commands which are supported by the aTCA-3420's different interfaces and are compatible with IPMI v1.5 and PICMG 3.0 R2.0 ECN001.

There are two interfaces implemented with IPMI command support.
(1) UART: OpenIPMI; (2) IPMB0: IPMBa & IPMBb

	UART	IPMB0
IPMI command		
IPM Device "Global" Commands		
Get Device ID	●	●
Cold Reset	●	●
Warm Reset	●	●
Get Self Test Results	●	●
Get Device GUID	●	●
IPMI Messaging Support Commands		
Set BMC Global Enables	●	●
Get BMC Global Enables	●	●
Clear Message Flags	●	●
Get Message Flags	●	●
Get Message	●	●
Send Message	●	●
Master Write-Read	●	●
BMC Watchdog Timer		
Reset Watchdog Timer	●	●
Set Watchdog Timer	●	●
Get Watchdog Timer	●	●
Event Commands		
Set Event Receiver	●	●
Get Event Receiver	●	●
Platform Event	●	●
Sensor Device Commands		
Get Device SDR Info	●	●
Get Device SDR	●	●
Reserve Device SDR Repository	●	●
Get Sensor Reading Factors	●	●
Set Sensor Hysteresis	●	●
Get Sensor Hysteresis	●	●
Set Sensor Threshold	●	●

Get Sensor Threshold	●	●
Set Sensor Event Enable	●	●
Get Sensor Event Enable	●	●
Rearm Sensor Events	●	●
Get Sensor Event Status	●	●
Get Sensor Reading	●	●
FRU Device Commands		
Get FRU Inventory Area Info	●	●
Read FRU Data	●	●
Write FRU Data	●	●
PICMG Command		
HPM.1 Upgrade Commands (HPM.1)		
Get target upgrade capabilities	●	●
Get component properties	●	●
Abort Firmware Upgrade	●	●
Initiate upgrade action	●	●
Upload firmware block	●	●
Finish firmware upload	●	●
Get upgrade status	●	●
Activate firmware	●	●
Query Self-test Results	●	●
Query Rollback status	●	●
Initiate Manual Rollback	●	●
AdvancedTCA		
Get PICMG Properties	●	●
Get Address Info	●	●
FRU Control	●	●
FRU Control Capabilities	●	●
Get FRU LED Properties	●	●
Get LED Color Capabilities	●	●
Set FRU LED State	●	●
Get FRU LED State	●	●
Set IPMB State		●
Set FRU Activation Policy	●	●
Get FRU Activation Policy	●	●
Set FRU Activation	●	●
Get Device Locator Record ID	●	●
Get Port State	●	●
Set Port State		●
Compute Power Properties		●
Set Power Level		●
Get Power Level	●	●
Bused Resource Control		●
Get IPMB Link Info	●	●
SET_CLOCK_STATE	●	●
GET_CLOCK_STATE	●	●
Get AMC-Port State		●
Set AMC-Port State		●

3.4 IPMI Firmware Upgrade Procedure

The processor can communicate with the IPMC via a UART interface. Please follow the procedures below to upgrade the IPMC firmware.

Step 1: Prepare an x86 PC with Windows OS and connect it to the aTCA-3420 via COM port with the RJ-45 to DB9 adapter provided. Download the latest firmware from the ADLINK website: http://www.adlinktech.com/



Step 2: Put the files **h8sprg.exe** and **install2.mot** (IPMC firmware) into a folder on the x86 Windows OS PC (e.g. "D:\3420").

Step 3: Set the DIP switches on the board as follows (solder side near front panel):

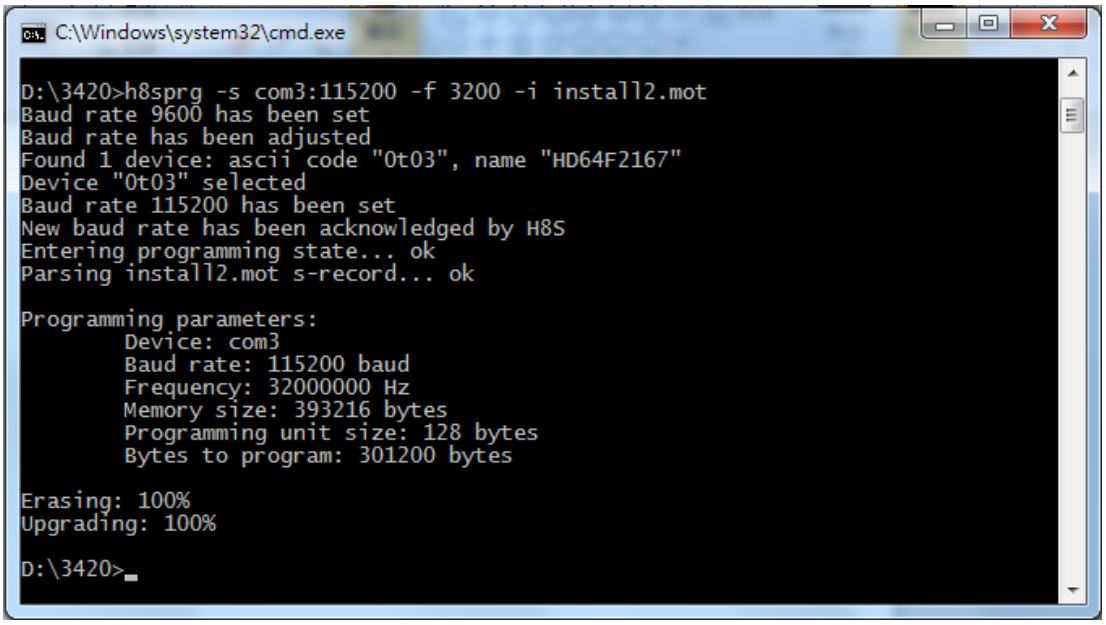
SW2	1	2	3	4
	OFF	OFF	OFF	ON

SW3	1	2	3	4
	ON	OFF	OFF	OFF

SW8	1	2	3	4
	OFF	OFF	ON	ON

Step 4: Open a command window on the x86 PC and go to the directory where **h8sprg.exe** and **install2.mot** are located (e.g. "D:\3420"), then run **h8sprg.exe** using the command below:

D:\3420> h8sprg -s com3:115200 -f 3200 -i install2.mot



Step 5: Power down the aTCA-3420. Set the DIP switches as follows (solder side near front panel):

SW2	1	2	3	4
	OFF	OFF	OFF	OFF

SW3	1	2	3	4
	OFF	OFF	OFF	OFF

SW8	1	2	3	4
	ON	ON	OFF	OFF

4. Getting Started

The aTCA-3420 has been designed for easy installation. However, the following standard precautions, installation procedures, and general information must be observed to ensure proper installation and to prevent damage to the board, other system components, or injury to personnel.

4.1 Safety Requirements

The following safety precautions must be observed when installing or operating the aTCA-3420. ADLINK assumes no responsibility for any damage resulting from failure to comply with these requirements.

Be careful when handling the board as the heatsink can get very hot. Do not touch the heatsink when installing or removing the board. The board should not be placed on any surface or in any form of storage container until the board and heat sink have cooled down to room temperature.

If your board type is not specifically qualified as being hot swap capable, switch off the AMC system power before installing an AMC mezzanine card in a free AMC slot. Failure to do so could endanger your life or health and may damage your board or system.

Certain AMC modules require bus master and/or Rear I/O capability. If you are in doubt whether such features are required for the board you intend to install, please check your specific board and/or system documentation to make sure that your system is provided with an appropriate free slot in which to insert the board.

This ATCA blade contains electrostatic sensitive devices. Please observe the necessary precautions to avoid damage to your board:

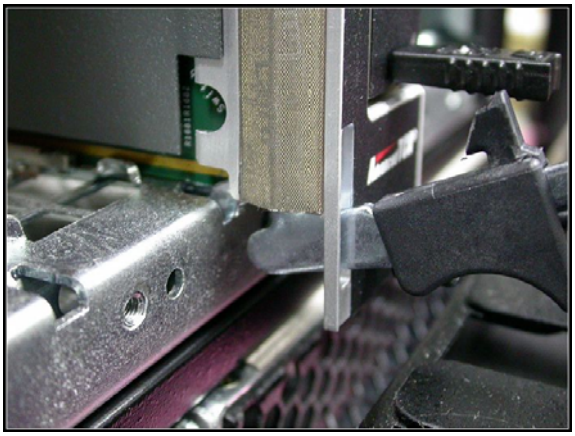
- Discharge your clothing before touching the assembly. Tools must be discharged before use.
- Do not touch components, connector-pins or traces.
- If working at an anti-static workbench with professional discharging equipment, please do not omit to use it.

4.2 Blade Installation

Follow these steps to install or remove the aTCA-3420 into/from the chassis.

Step 1

Carefully align the board edges with the chassis guide rails and insert the module.



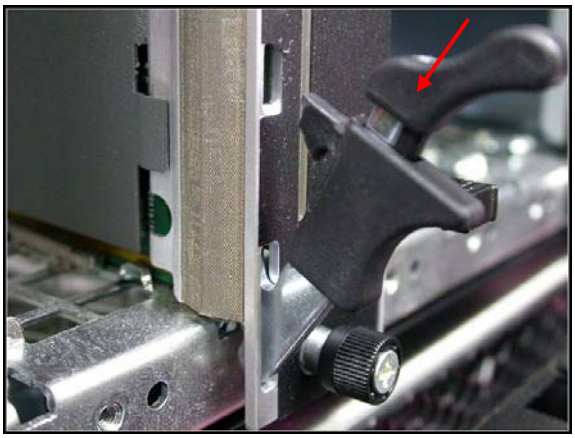
Step 2

Check that the catch hooks and alignment pins at either end of the module are correctly inserted into the proper openings. Push inwards on the handles until the module is firmly seated in the chassis. (Do not force the handles if there is resistance as this may damage the connectors or backplane.)

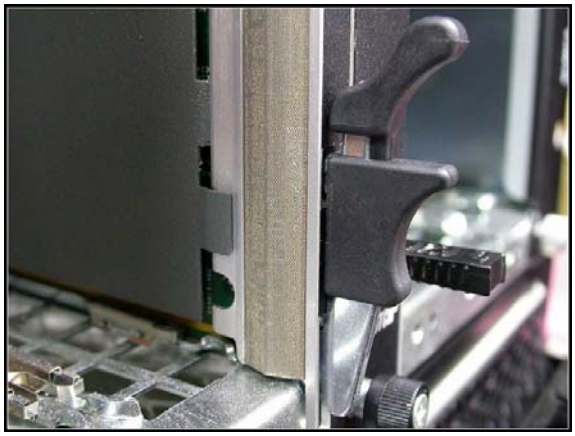


Step 3

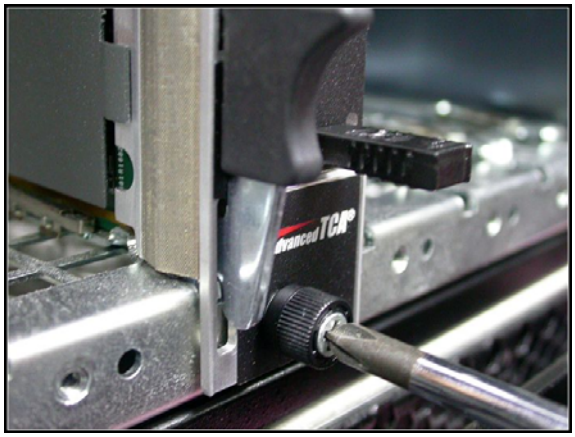
Depress the buttons to unlock the ejector handles and push the handles into the faceplate.



Step 4
Release the buttons to lock the ejector handles in place.



Step 5
Secure the module by tightening the captive screws.



To remove the module from chassis, undo the captive screws, depress the buttons on the ejector handles, and pull outwards on the handles to eject the module from the backplane. Pull the module towards you until it is free of the chassis.

4.3 Quick Start

Connecting to the aTCA-3420

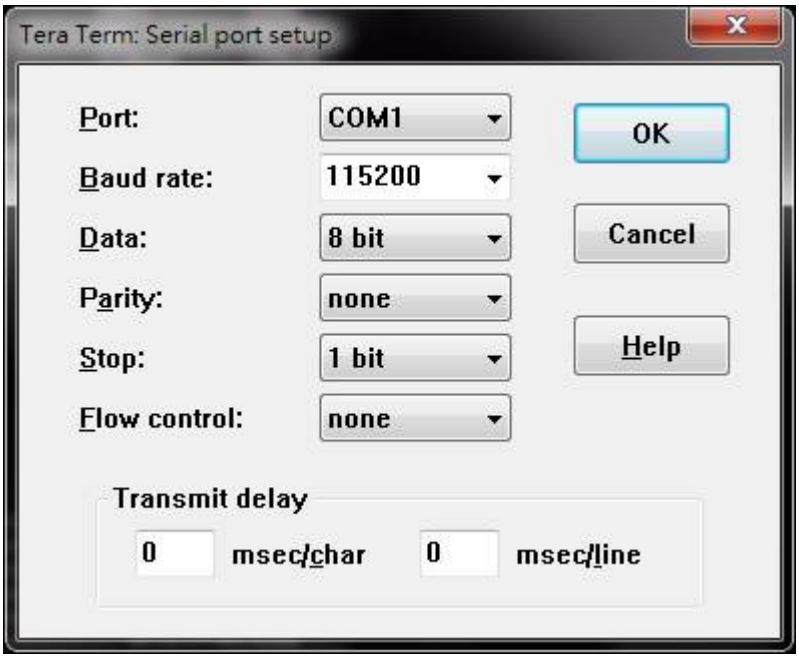
Step 1

Connect the COM port of a laptop/PC to the to MPC8313E via the front panel COM port (RJ45) on the aTCA-3420 (upper right jack) using the RJ45-to-DB9 adapter provided and connect the Ethernet port of the laptop/PC to the front panel service port (lower right Jack) with a CAT5 Ethernet cable.



Step 2

Start a terminal-emulator application (e.g. Tera Term) on the laptop/PC with the settings listed below: corresponding laptop/PC COM port, 115,200 baud, 8 data bits, no parity, one stop bit and no flow control.



Step 3

Set the Broadcom SDK for Base switch or FASTPATH® for Fabric switch management.

The aTCA-3420 is a 20-port 10GbE Fabric Interface and 24-port GbE Base Interface AdvancedTCA® (ATCA) multilayer Switch Blade based on Broadcom BCM56800 and BCM56312 switch silicon. The Fabric Switch (BCM56800) is paired with Broadcom FASTPATH® software for management while the Base Switch (BCM56312) is paired with Broadcom SDK software. In default settings, the system will boot to the FASTPATH® shell. The user can follow the steps below to select SDK or FASTPATH®

Boot into SDK CLI for Base Switch (BCM56312) management

(Note: FASTPATH® CLI/web-GUI will be suspended until user exits the SDK shell.)

1. Turn on the aTCA-3420 unit

2. After system boot up is complete, you will see a login prompt. Login with user name: *admin* and a blank password:

User:admin
Password:

3. Enter privilege level with the “enable” command and blank password:

(aTCA3420) >enable
Password:
(aTCA3420) #

4. Enter the SDK shell with the “dev diag_shell” command:

(aTCA3420) #dev diag_shell
Please note: All other UI sessions will be suspended until you exit the shell.
Devshell output (Session #0): diag_shell
Broadcom Command Monitor: Copyright (c) 1998-2008 Broadcom Corporation
OS: Unix (Posix)
BCM.1>

5. Use the “exit” command to go back to the FASTPATH® privilege level:

BCM.1>exit
(aTCA3420) #

Boot into FASTPATH® CLI for Fabric Switch (BCM56800) initial setting

1. Turn on the aTCA-3420 unit

2. After system boot up is complete, you will see a login prompt. Login with user name: *admin* and blank password:

User:admin
Password:

3. Enter privilege level with the “enable” command and a blank password

(aTCA3420) >enable
Password:

4. Show current serviceport settings

(aTCA3420) #show serviceport
Interface Status..... Up
IP Address..... 0.0.0.0
Subnet Mask..... 0.0.0.0
Default Gateway..... 0.0.0.0
Configured IPv4 Protocol..... DHCP
Burned In MAC Address..... 00:30:64:0D:43:61

5. Set serviceport protocol

(aTCA3420) #serviceport protocol none
Changing protocol mode will reset ip configuration.

Are you sure you want to continue? (y/n)y

6. Set the serviceport IP and subnet mask

(aTCA3420) #serviceport ip 10.0.0.6 255.255.255.0

(aTCA3420) #show serviceport
Interface Status..... Up
IP Address..... 10.0.0.6
Subnet Mask..... 255.255.255.0
Default Gateway..... 0.0.0.0
Configured IPv4 Protocol..... None
Burned In MAC Address..... 00:30:64:0D:43:61
(aTCA3420) #

7. For more CLI instruction/commands, you can use “help” or “?” to continue

(aTCA3420) #help

HELP:
Special keys:
DEL, BS .... delete previous character
Ctrl-A .... go to beginning of line
Ctrl-E .... go to end of line
Ctrl-F .... go forward one character
Ctrl-B .... go backward one character
Ctrl-D .... delete current character
Ctrl-U, X .. delete to beginning of line
Ctrl-K .... delete to end of line
Ctrl-W .... delete previous word
Ctrl-T .... transpose previous character
Ctrl-P .... go to previous line in history buffer
Ctrl-R .... rewrites or pastes the line
Ctrl-N .... go to next line in history buffer
Ctrl-Y .... print last deleted character
Ctrl-Q .... enables serial flow
Ctrl-S .... disables serial flow
Ctrl-Z .... return to root command prompt
Tab, <SPACE> command-line completion
Exit .... go to next lower command prompt
? .... list choices

(aTCA3420) #?

boot	*Marks the given image as active for subsequent re-boots.*
cablestatus	*Isolate the problem in the cable attached to an interface.*
clear	*Reset configuration to factory defaults.*
configure	*Enter into Global Config Mode.*
copy	*Uploads or Downloads file.*
debug	*Configure debug flags.*
delete	*Deletes given image on the node.*
disconnect	*Close active remote session(s).*
dot1x	*Configure dot1x privileged exec parameters.*
enable	*Set the password for the enable privilege level.*
erase	*Erase configuration file.*
exit	*To exit from the mode.*
filedescr	*Sets text description for a given image.*
help	*Display help for various special keys.*
hostname	*Change the system hostname.*
ip	*Configure IP parameters.*
logout	*Exit this session. Any unsaved changes are lost.*
network	*Configuration for inband connectivity.*
ping	*Send ICMP echo packets to a specified IP address.*
quit	*Exit this session. Any unsaved changes are lost.*
reload	*Reset the switch.*
renew	*To renew IP Address*
script	*Apply/Delete/List/Show/Validate Configuration Scripts.*
serviceport	*Specify the serviceport parameters / protocol.*

set	*Set Router Parameters.*
show	*Display Switch Options and Settings.*
sshcon	*Configure SSH connection parameters.*
telnet	*Telnet to a remote host.*
telnetcon	*Configure telnet connection parameters.*
terminal	*Set terminal line parameters.*
traceroute	*Trace route to destination.*
update	*Updates the bootloader on the node from the activated image.*
vlan	*Type 'vlan database' to enter into VLAN mode.*
write	*Save the current configuration to NVRAM.*

Update FASTPATH® Software

1. Prepare a laptop/PC with TFTP server installed. Create a folder called “tftpboot” under /root and load the target image file in the “tftpboot” folder. You can find the latest image file on the ADLINK website http://www.adlinktech.com/

2. Connect the COM port of a laptop/PC to the to MPC8313E via the front panel COM port (RJ45) on the aTCA-3420 (upper right jack) using the RJ45-to-DB9 adapter provided and connect the Ethernet port of the laptop/PC to the front panel service port (lower right Jack) with a CAT5 Ethernet cable.



3. Verify current image version:

(aTCA3420) #show bootvar

Image Descriptions
active :
backup :
Images currently available on Flash

unit	*active*	*backup*	*current-active*	*next-active*
1	*3.0.0.4*	*3.0.0.4*	*3.0.0.4*	*3.0.0.4*

4. Copy the image file from the TFTP server to update the active image (example: TFTP server IP is 10.0.0.6, default image file name is “image1”):

(aTCA3420) #copy tftp://10.0.0.5/tftpboot/image1 active

Mode..... TFTP
Set Server IP..... 10.0.0.5
Path..... tftpboot/
Filename..... image1
Data Type..... Code
Destination Filename..... active
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
TFTP Code transfer starting...
File transfer operation completed successfully.

5. Verify updated image version:

(aTCA3420) #show bootvar

Image Descriptions
active :
backup :
Images currently available on Flash

unit	*active*	*backup*	*current-active*	*next-active*
1	*3.0.0.6*	*3.0.0.4*	*3.0.0.6*	*3.0.0.6*

6. Copy the image file from TFTP server to update backup image

(aTCA3420) #copy tftp://10.0.0.5/tftpboot/image1 backup

Mode..... TFTP
Set Server IP..... 10.0.0.5
Path..... tftpboot/
Filename..... image1
Data Type..... Code
Destination Filename..... backup
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
TFTP Code transfer starting...
File transfer operation completed successfully.

7. Verify updated image version

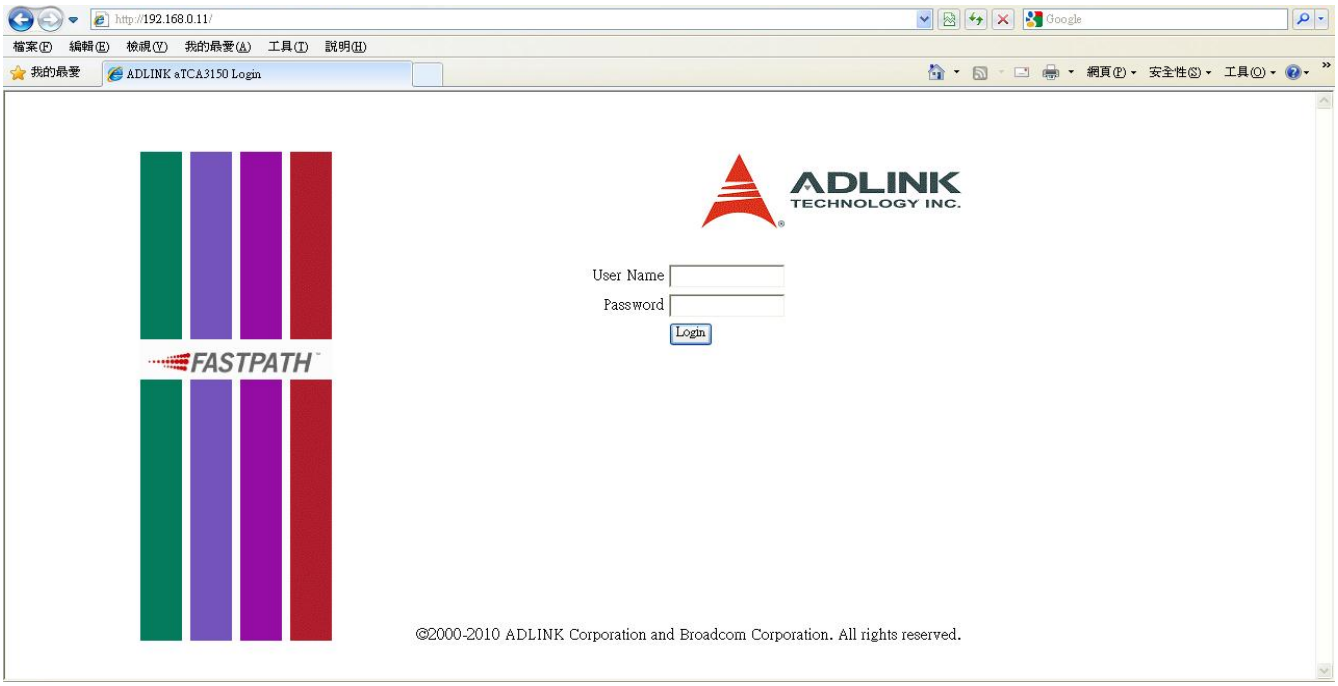
(aTCA3420) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash

unit	*active*	*backup*	*current-active*	*next-active*
1	*3.0.0.6*	*3.0.0.6*	*3.0.0.6*	*3.0.0.6*

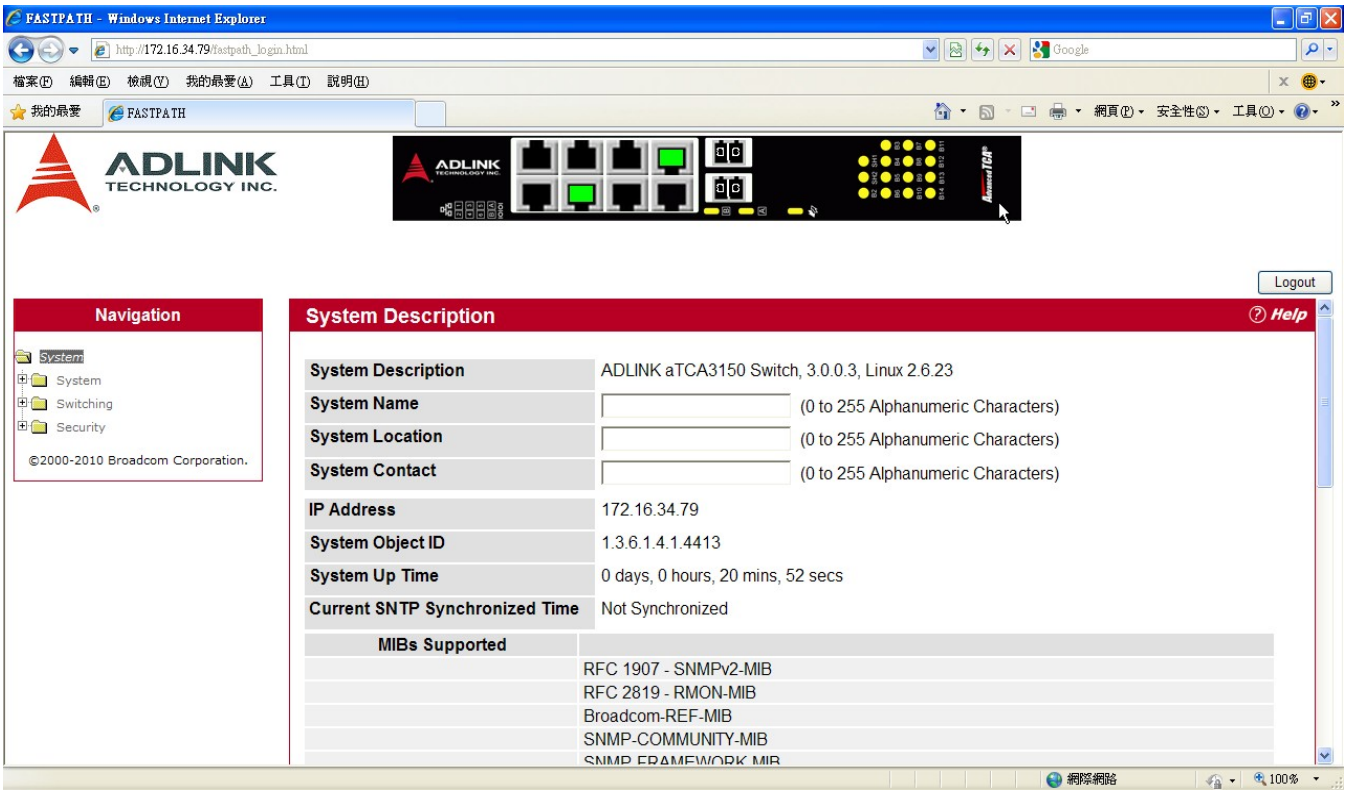
Update successfully

Login FASTPATH® GUI

With the Ethernet cable attached to the service port as described above in **Connecting to the aTCA-3420**, start a browser on the laptop/PC (e.g. IE, Firefox, Chrome, etc.) in the same domain and type in the preset IP address from Boot into FASTPATH® CLI for Fabric Switch, Step 6 (10.0.0.6 in the example). The switch management login page appear as shown. Default User Name is admin with blank password.

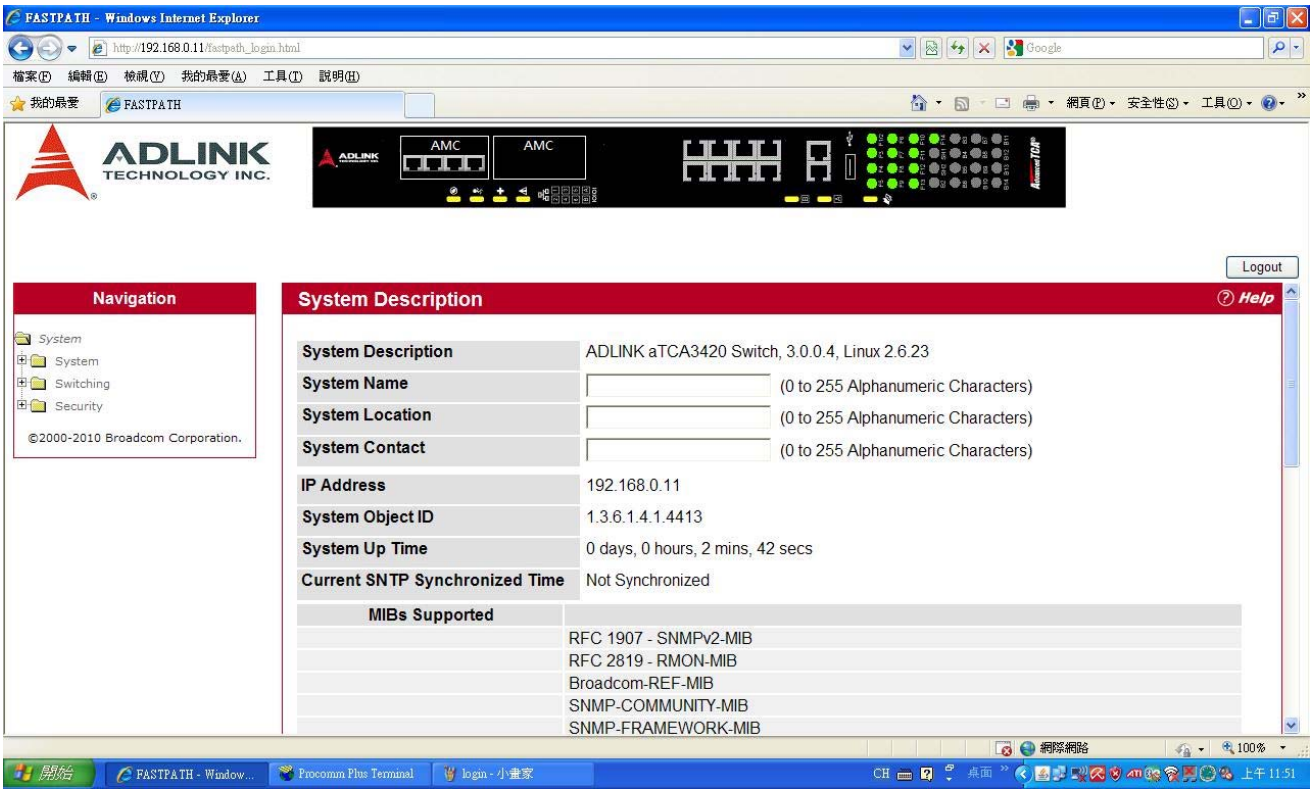


After authentication, the management GUI homepage will appear as shown.



5. Configure and Manage the Fabric Switch

Use the Navigation tab to see all possible settings and functions. There are three main categories: System, Switching and Security. A faceplate layout drawing at the top of the web GUI indicates ports that are actively linked highlighted in green.



5.1. Configuring System Information

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

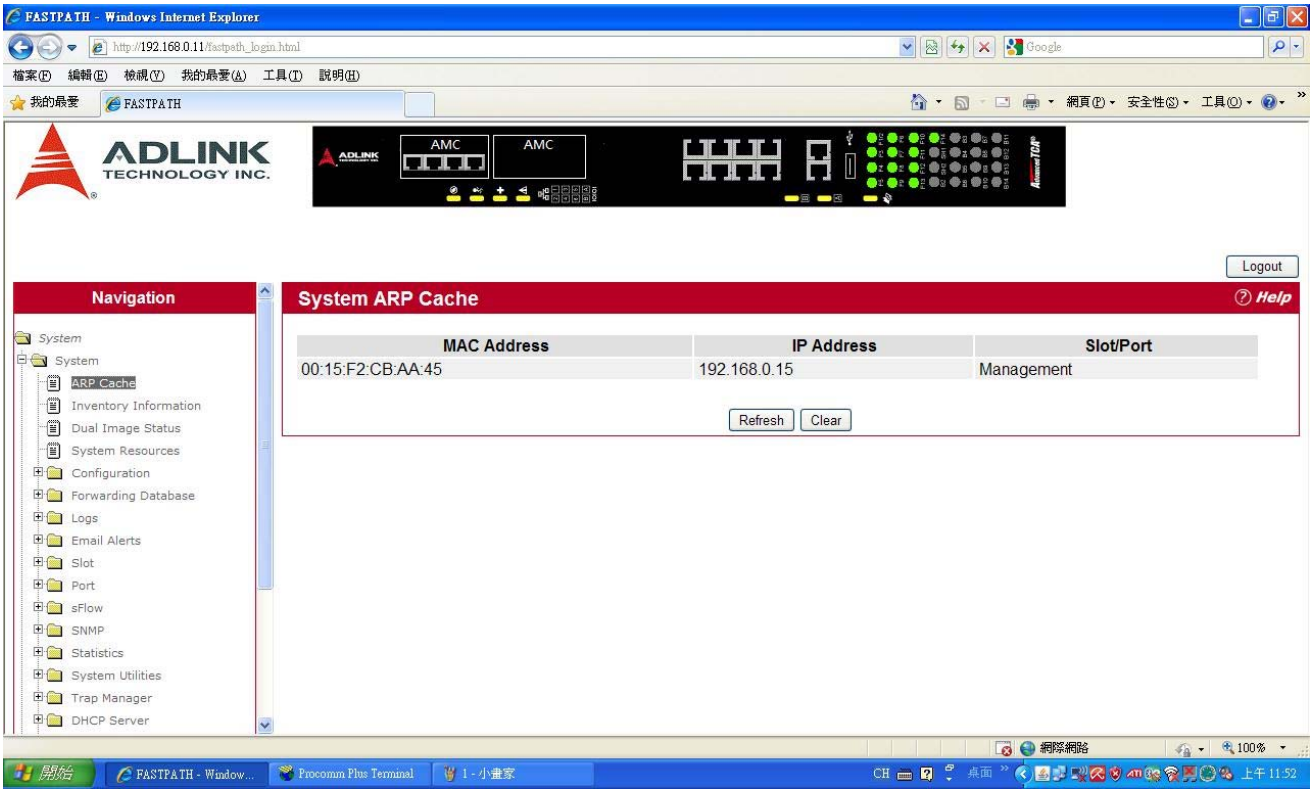
- Viewing ARP Cache
- Viewing Inventory Information
- Viewing the Dual Image Status
- Viewing System Resources
- Defining General Device Information
- Configuring and Searching the Forwarding Database
- Managing Logs
- Configuring and Viewing Device Slot Information
- Configuring and Viewing Device Port Information
- Configuring sFlow
- Defining SNMP Parameters
- Viewing System Statistics
- Using System Utilities
- Managing SNMP Traps
- Managing the DHCP Server
- Configuring DNS
- Configuring SNTP Settings
- Configuring and Viewing ISDP Information

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.

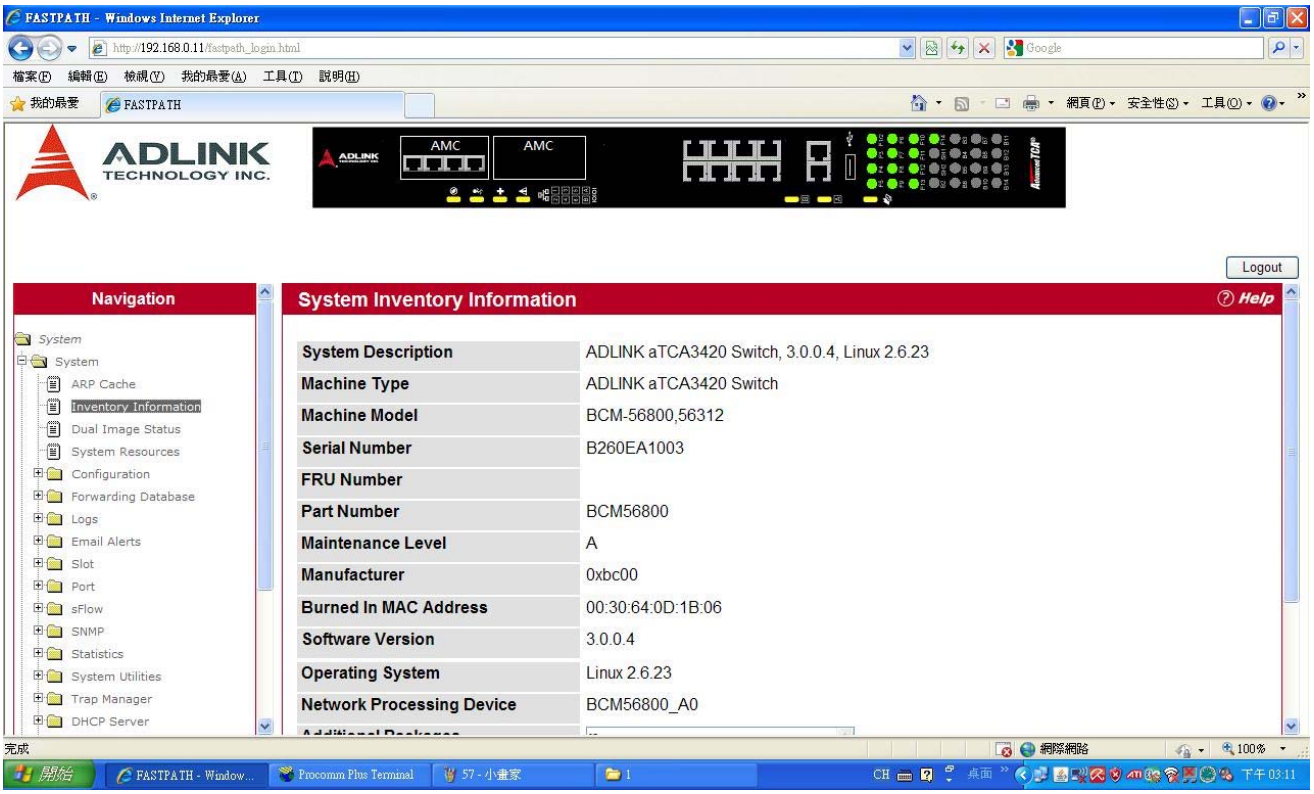
To display the system ARP cache, click **System** > **ARP Cache** page in the navigation tree. Click **Refresh** to reload the page and refresh the ARP cache view.



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 unit, slot, and port number being used for the connection. For non-stacking systems, only the slot and port number is displayed. For units that have a service port, the service port will be listed as "Management" in this field.

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 **System** > **Inventory Information** page in the navigation tree.



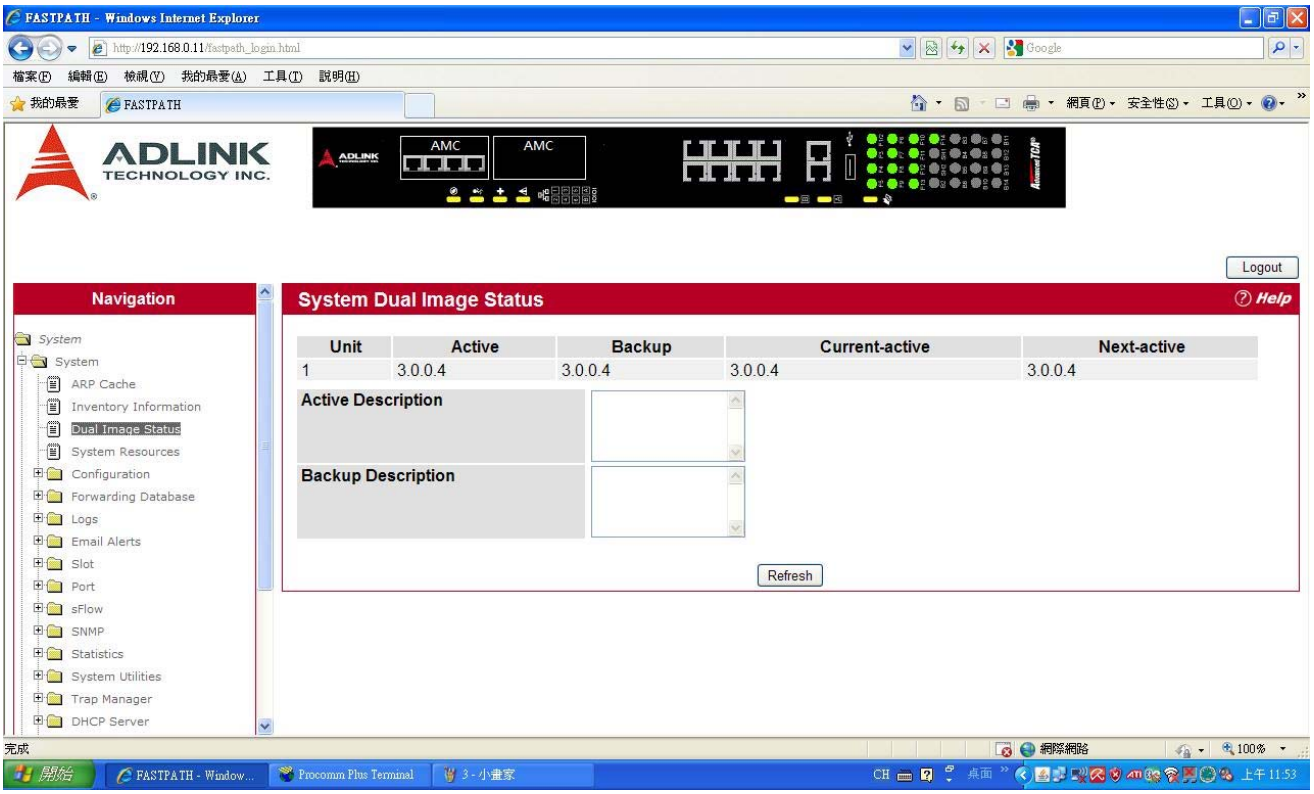
Field	Description
Management Unit Number	Unit number that corresponds to the stack manager.
System Description	The product name of this switch.
Machine Type	The machine type of this switch.
Machine Model	The model within the machine type.
Serial Number	The unique serial number for this switch.
FRU Number	The field replaceable unit number.
Part Number	The manufacturing part number.
Maintenance Level	The identification of the hardware change level.
Manufacturer	The two-octet code that identifies the manufacturer.
Base MAC Address	The burned-in universally administered MAC address of this switch.
Software Version	The release.version.maintenance number of the code currently running on the switch. For example, if the release is 1, the version is 2 and the maintenance number is 4, the format is “1.2.4.”

Field	Description
Operating System	The operating system currently running on the switch.
Network Processing Device	Identifies the network processor hardware.
Additional Packages	A list of the optional software packages installed on the switch, if any. For example, FASTPATH® BGP-4, or FASTPATH® Multicast.

Viewing the Dual Image Status

The Dual Image feature allows the switch to have two FASTPATH® 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 **System** > **Dual Image Status** in the navigation menu.



Field	Description
Unit	Displays the unit ID of the switch.
Active	Displays the version of the Active code file.
Backup	Displays the version of the Backup 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.
Active Description	Displays the description associated with the Active code file.
Backup Description	Displays the description associated with the Backup code file.

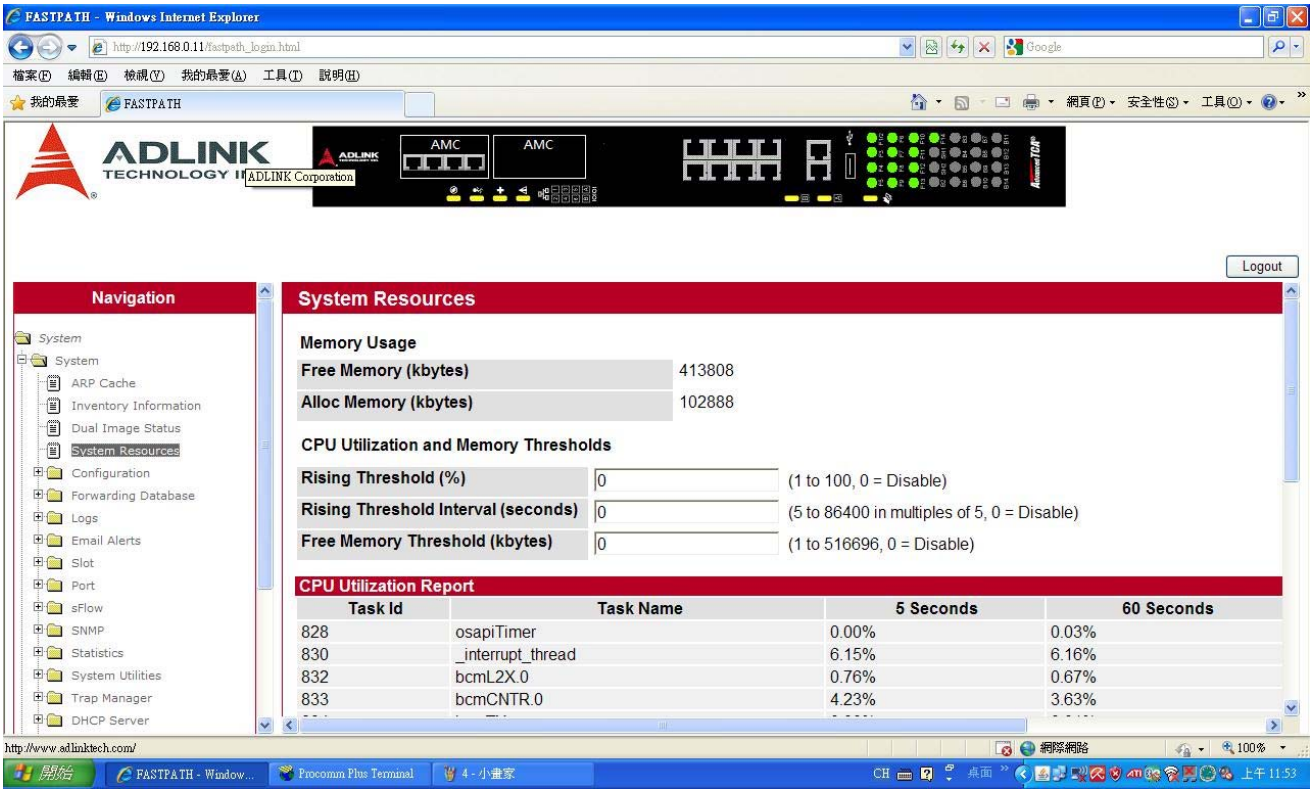
Click **Refresh** to display the latest information from the router. For information about how to update or change the system images, see “Using System Utilities”

Viewing System Resources

Use the System Resources page to display the following memory information for the switch:

- Free memory
- Allocated memory
- CPU utilization by task
- Total CPU utilization at the following intervals: - Five seconds – One minute – Five minutes

To display the System Resources page, click **System** > **System Resources** in the navigation menu.



Field	Description
Free Memory	Displays the available Free Memory on the switch.
Alloc Memory	Displays the allocated Memory for the switch.
Task Id	Displays the Id of running tasks.
Task Name	Displays the name of the running tasks.
CPU Utilization(%)	Displays the CPU Utilization of tasks in terms of percentage of utilization.
Total CPU Utilization	Displays the Total CPU Utilization in terms of percentage. **Total CPU Utilization** is shown in the following intervals: • Five seconds • One minute • Five minutes

5.2. Defining General Device Information

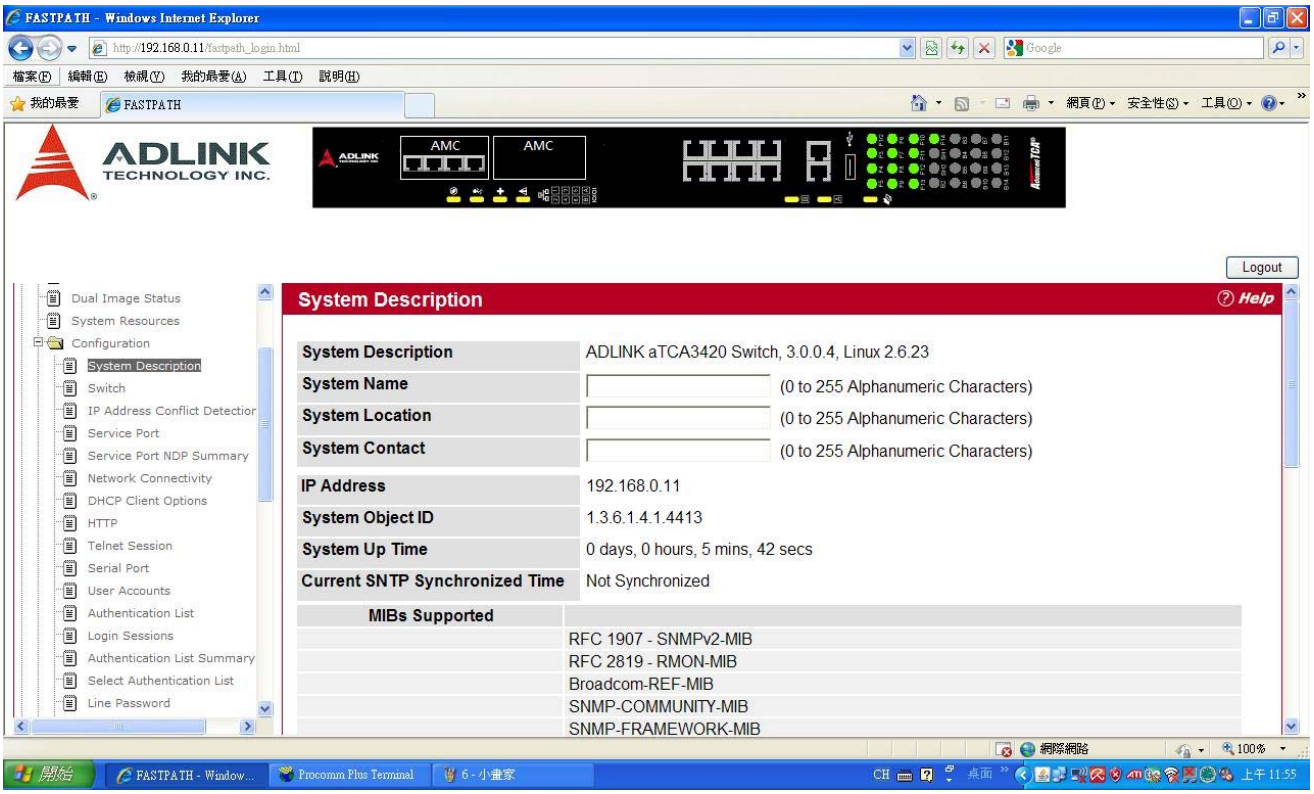
The Configuration folder in the System menu contains links to pages that allow you to configure device parameters. The Configuration folder contains links to the following features:

- System Description
- Switch Configuration
- Service Port
- Service Port NDP Summary
- Service Port DHCPv6 Client Statistics
- Network Connectivity
- Network Connection NDP Summary
- Network Port DHCPv6 Client Statistics
- DHCP Client Options
- HTTP Configuration
- Telnet Session
- Serial Port
- User Accounts
- Authentication List Configuration
- Login Session
- Authentication List Summary
- Select Authentication List
- Line Password
- Enable Password
- Password Management
- Denial of Service

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 **System > Configuration > System Description** in the navigation tree.



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 255 alpha-numeric characters. The factory default is blank.
System Location	Enter the location of this switch. You may use up to 255 alpha-numeric characters. The factory default is blank.
System Contact	Enter the contact person for this switch. You may use up to 255 alpha-numeric characters. The factory default is blank.
IP Address	The IP Address assigned to the network interface. To change the IP address, see “Network Connectivity”.
System Object ID	The base object ID for the switch's enterprise MIB.
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

Field	Description
	displays “Not Synchronized.” To specify an SNTP server, see “Configuring SNTP Settings”.
MIBs Supported	Displays the list of MIBs supported by the management agent running on this switch.

Defining System Information

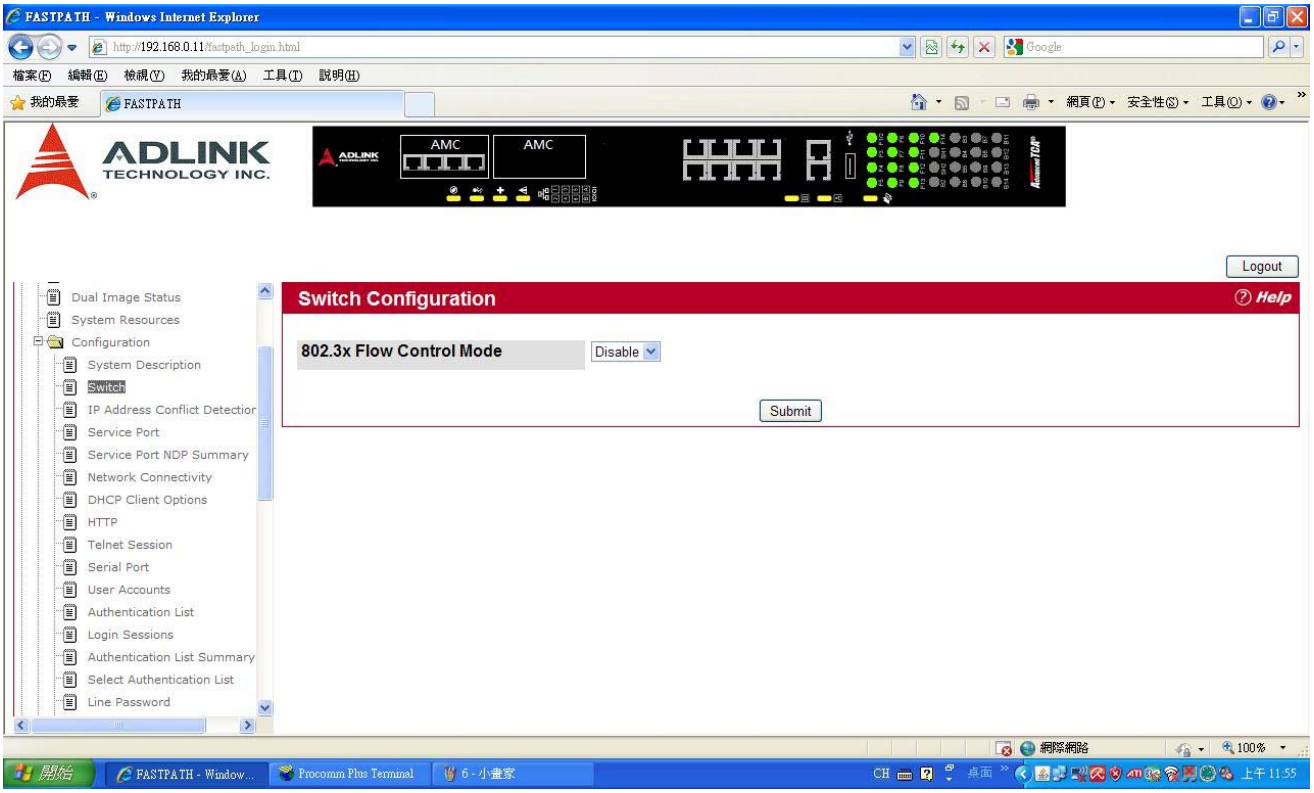
1. Open the System Description page.
2. Define the following fields: System Name, System Contact, and System Location.
3. Click Submit. The system parameters are applied, and the device is updated.

Note: If you want the switch to retain the new values across a power cycle, you must perform a save.

Switch Configuration

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 **System > Configuration > Switch** in the navigation tree.



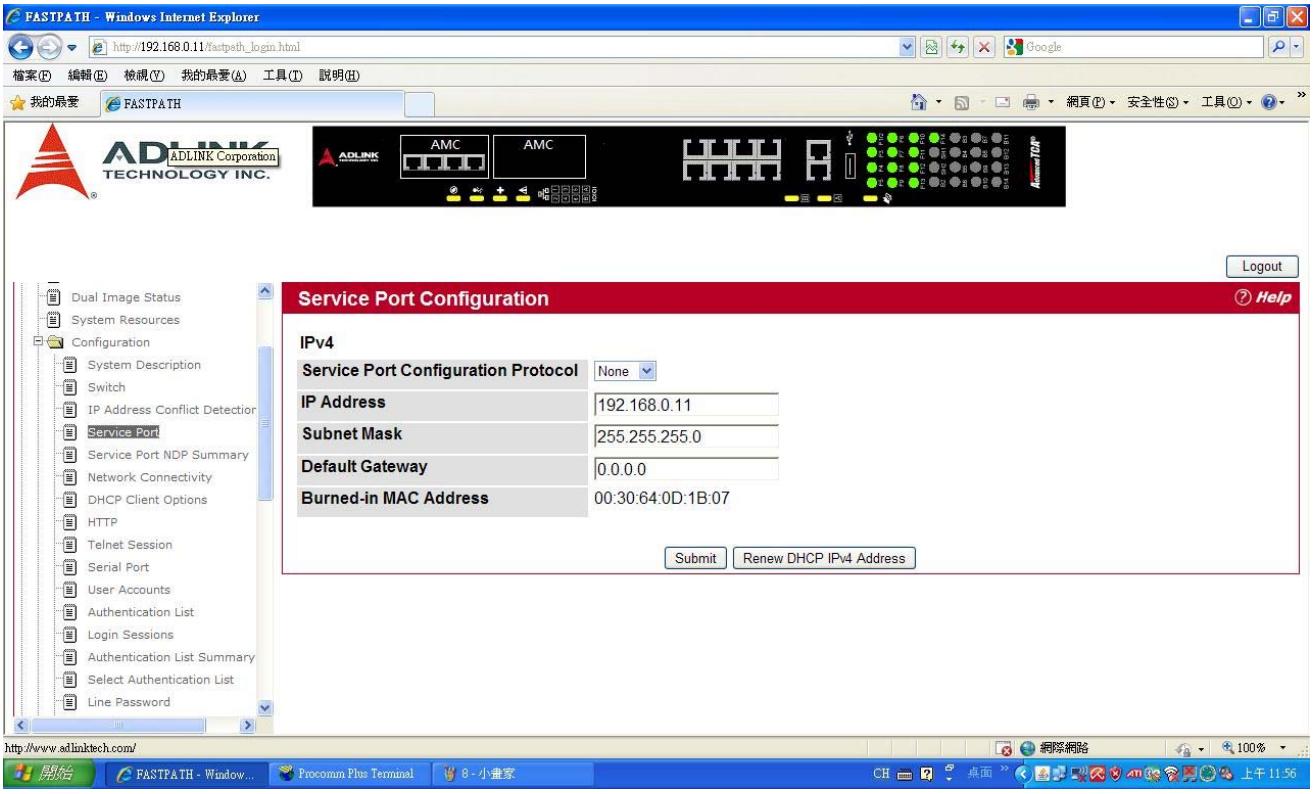
Field	Description
IEEE 802.3x Flow Control Mode	Enables or disables IEEE 802.3x flow control on the system. The factory default is disabled.
Enable	Enables flow control so that the switch can communicate with higher speed switches.
Disable	Disables flow control so that the switch does not send pause 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.

Service Port

Some platforms have a built-in service port that can serve as a dedicated network management interface. For systems that have the service port, the Service Port Configuration page allows you to configure network information for the switch.

To access the Service Port Configuration page, click **System > Configuration > Service Port** in the navigation tree.



Field	Description
Ipv4 Fields: These display Ipv4 configuration information.	
Service Port Configuration Protocol	Specify what the switch should do following power-up. The factory default is None. The options are as follows: • **BootP**: Transmit a Bootp request. • **DHCP**: Transmit a DHCP request. • **None**: Do not send any requests following power-up.
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.

Field	Description
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.

If you change any of the parameters on this 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.

Service Port NDP Summary

When Ipv6 is enabled on the service port, and a ping is initiated to a neighbor, the neighbor is added to the cache (if successful). This page displays data on these ports.

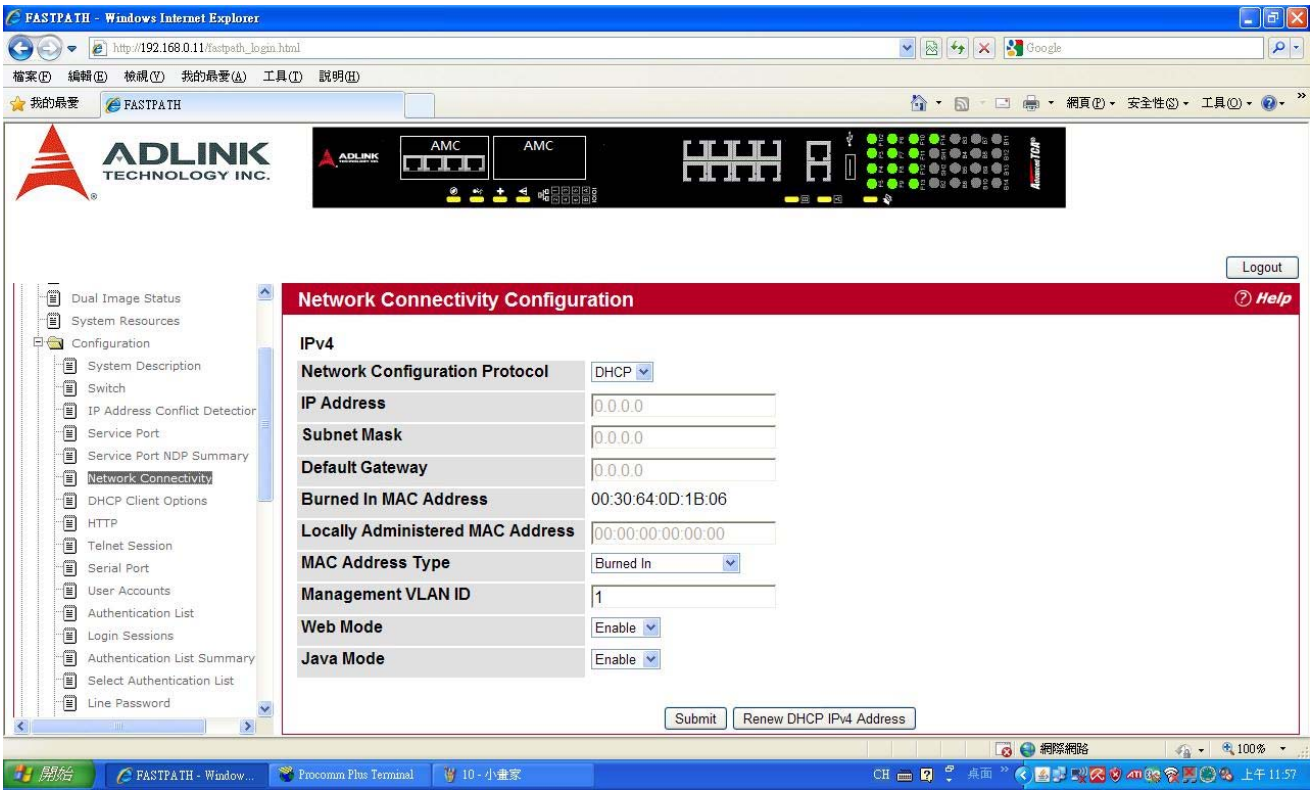
To display the page, click **System > Configuration > Service Port NDP Summary**.

Field	Description
Ipv6 Address	Displays the IP address of the neighbor.
MAC Address	Displays the MAC address of the neighbor.
isRtr	Indicates whether the neighbor is a router. If the neighbor is a router, the value is TRUE. If the neighbor is not a router, the value is FALSE.
Neighbor State	Specifies the state of the neighbor cache entry. Following are the states for dynamic entries in the Ipv6 neighbor discovery cache: • Icmp: Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received. • Reachable: Positive confirmation was received within the last Reachable Time milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent. • Stale: More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent. • Delay: More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE. • Probe: A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.
Last Updated	Displays the time since the address was confirmed to be reachable.

Network Connectivity

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 **System > Configuration > Network Connectivity** in the navigation tree.



Field	Description
Ipv4 Fields: These display Ipv4 configuration information.	
Network Configuration Protocol	Specify what the switch should do following power-up. The factory default is None. The options are as follows: • **BootP**: Transmit a Bootp request. • **DHCP**: Transmit a DHCP request. • **None**: Do not send any requests following power-up.
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

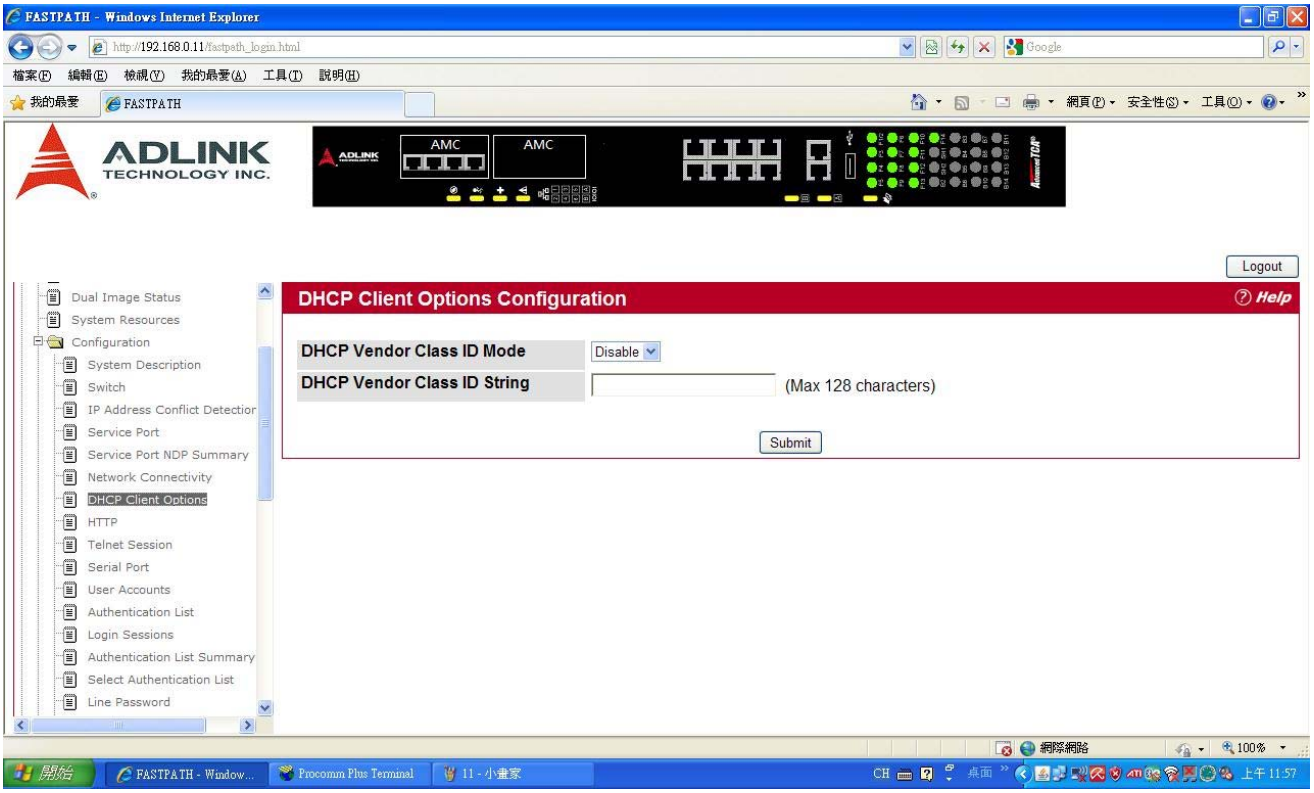
Field	Description
	0.0.0.0.
Burned-in MAC Address	This read-only field displays the MAC address that is burned-in to the network card at the factory. This MAC address is used for in-band connectivity if you choose not to configure a locally administered address.
Locally Administered MAC Address	Specifies 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	Specify whether the burned-in or the locally administered MAC address should be used for in-band connectivity. The factory default is to use the burned-in MAC address
Management VLAN ID	Specify the management VLAN ID of the switch. It may be configured to any value in the range of (1 to 4093). 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	Enables/Disables Web Mode on the switch.
Java Mode	Enables/Disables Java mode on the switch

If you change any of the network connectivity 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.

DHCP Client Options

Use the DHCP Client Options page to configure DHCP client settings on the system.

To access the DHCP Client Options page, click **System > Configuration > DHCP Client Options** in the navigation menu.

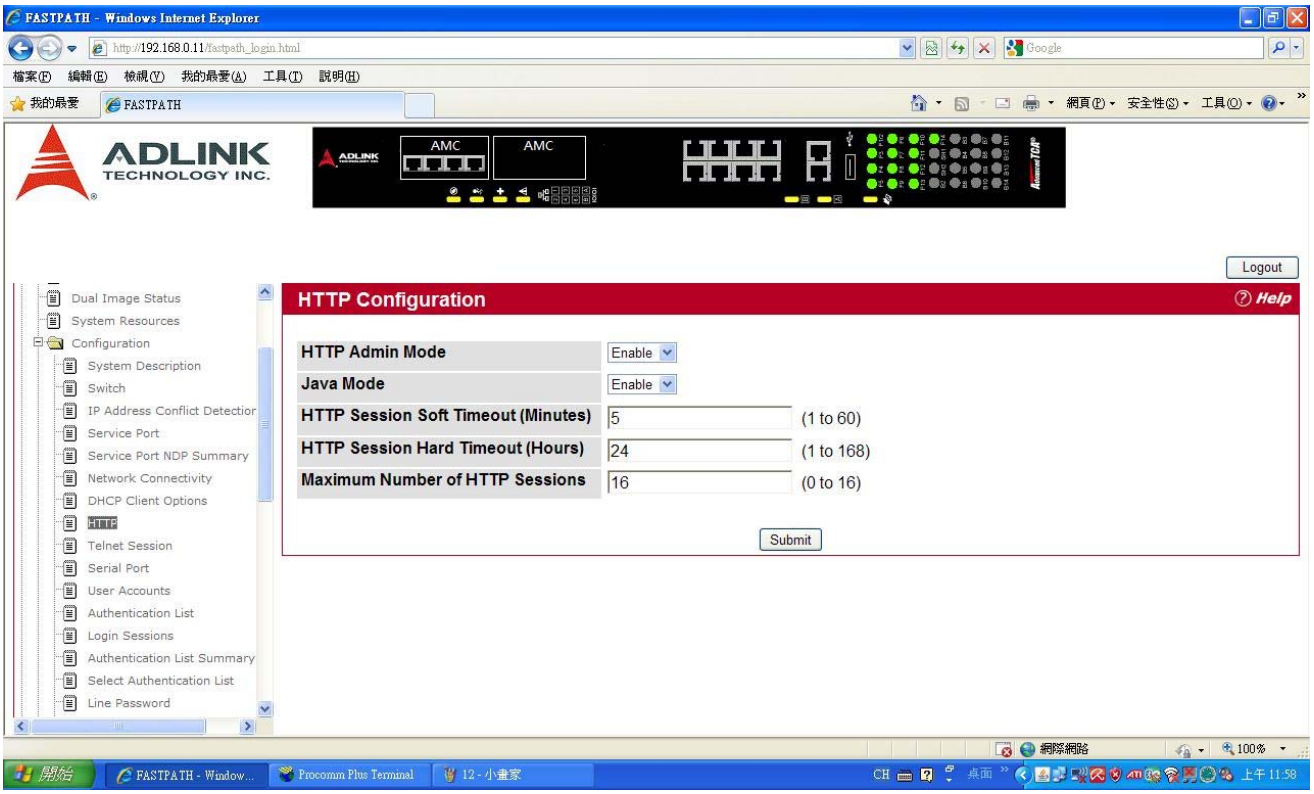


Field	Description
DHCP Vendor Class ID Mode	Enables/Disables the vendor class identifier mode.
DHCP Vendor Class ID String	The string added to DHCP requests as Option-60. i.e. Vendor Class Identifier option.

HTTP Configuration

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

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



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 (1 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.

Field	Description
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 (1 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.

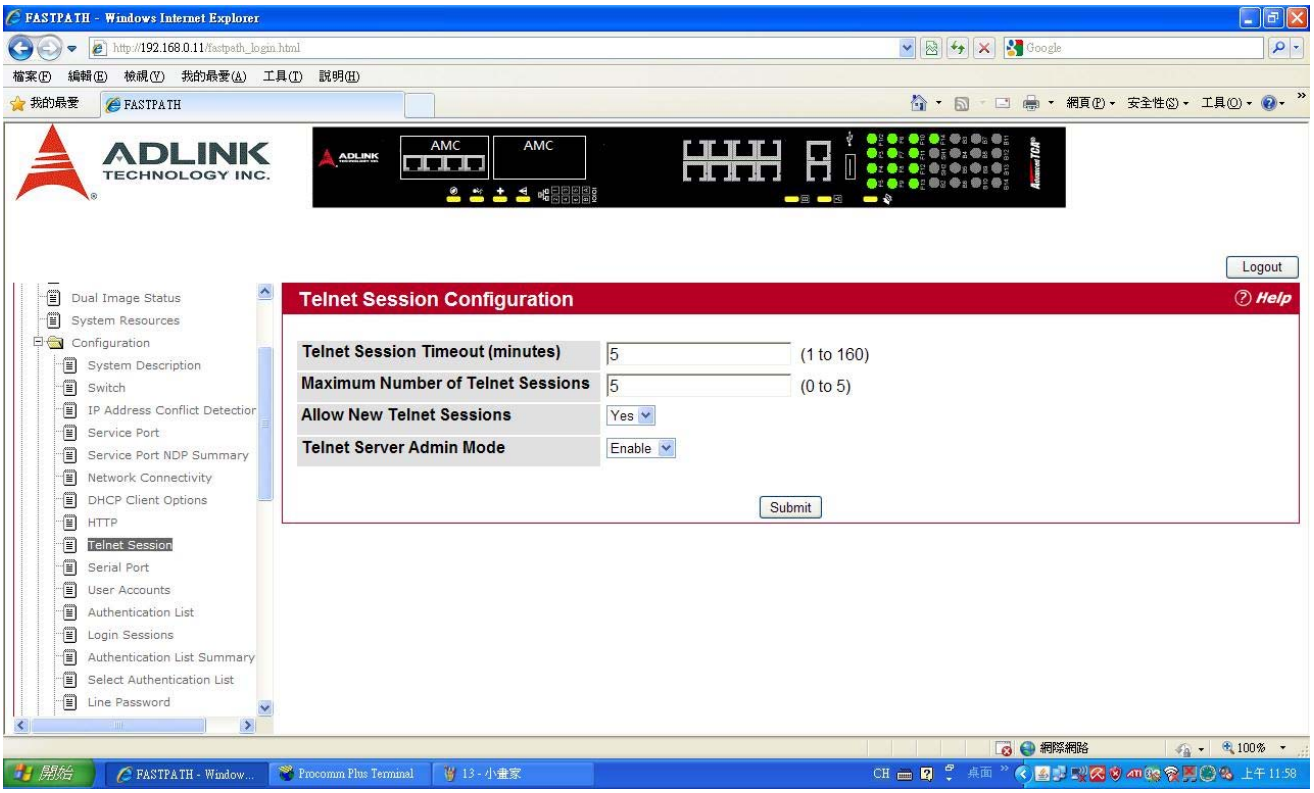
If you make changes to the page, click **Submit** to apply the changes to the system.

Telnet Session

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 display the Telnet Session Configuration page, click **System > Configuration > Telnet Session** in the navigation tree.



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.

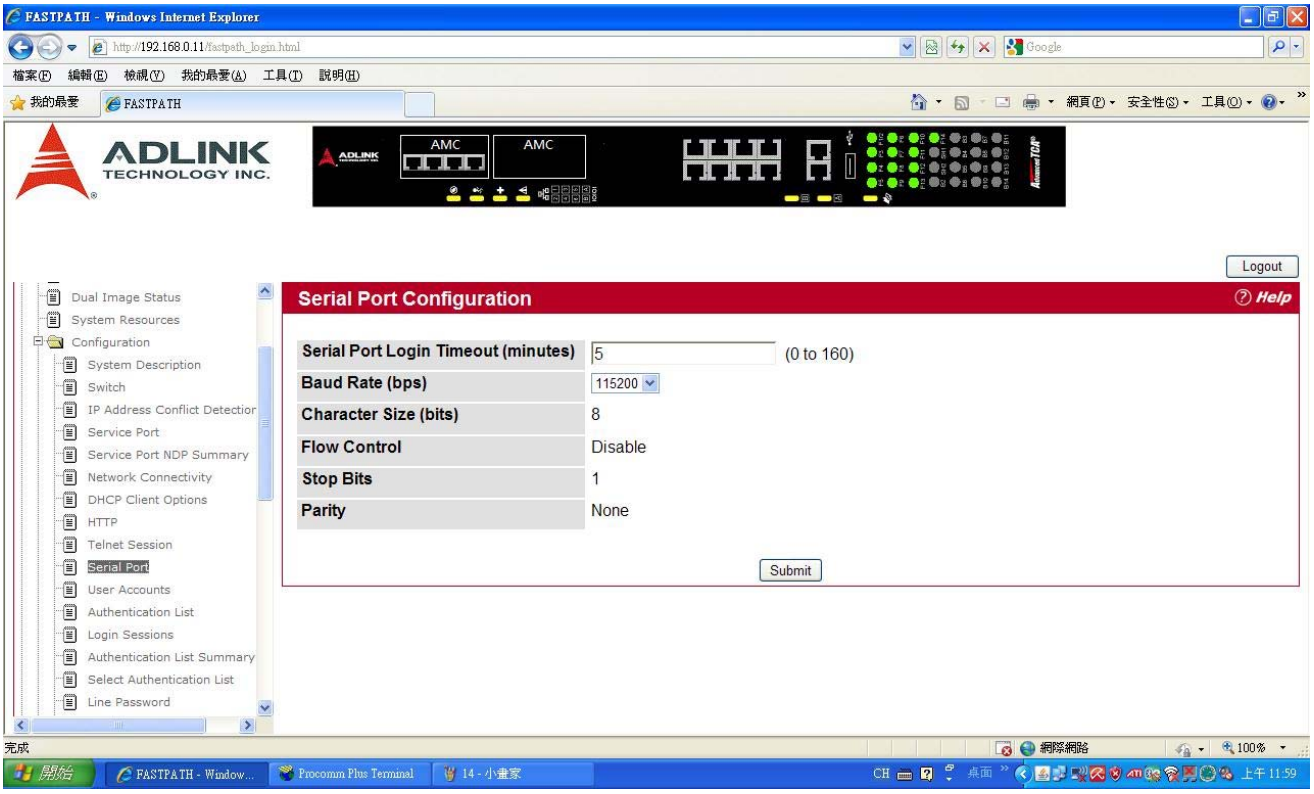
Field	Description
Allow New Telnet Sessions	Controls whether to allow new telnet sessions: • **Yes**: Permits new telnet sessions until the maximum number allowed is reached. • **No**: New telnet sessions will not be allowed, but existing sessions are not disconnected.
Telnet Server Admin Mode	Administrative 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.

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 **System > Configuration > Serial Port Configuration** in the navigation tree.



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 baud for Linux platforms and 9600 baud for VxWorks platforms.
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.

User Accounts

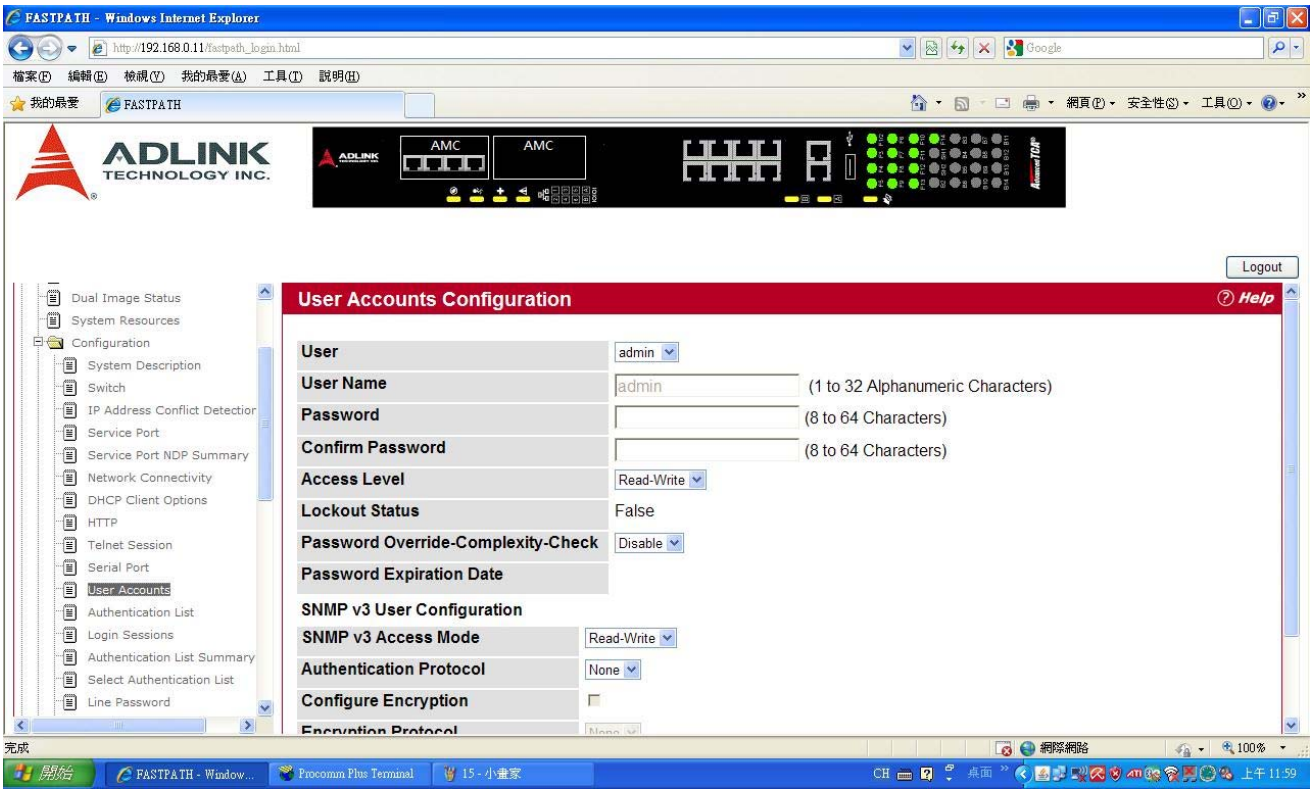
By default, the switch contains two user accounts:

- 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.

To access the User Accounts page, click **System > Configuration > User Accounts** in the navigation tree.



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 you want to give to the new account. (You can only enter data in this field when you are creating a new account.) User names are up to 32 alphanumeric characters in length and are not case sensitive. Valid characters include all the alphanumeric characters and the dash ('-') and underscore ('_') characters. User name default 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.

Field	Description
Password	Enter the optional new or changed password for the account. It will not display as it is typed, only asterisks (*) or dots(.) will show based on the browser used. Passwords must be greater than eight characters and can be up to 64 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 Level	Indicates the user's access level. 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 configurable number of failed login attempts. See “Password Management” for instructions on configuring this number.
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.
SNMP v3 User Configuration	
SNMP v3 Access Mode	Shows 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 specify a valid password.
Configure Encryption	Select the check box to change the Encryption Protocol and Encryption Key.
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** field is not active for input.
Encryption Key	If you selected **DES** in the **Encryption Protocol** field enter the SNMPv3 Encryption Key here. Otherwise this field is not active. Key should be 8 characters in length

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.

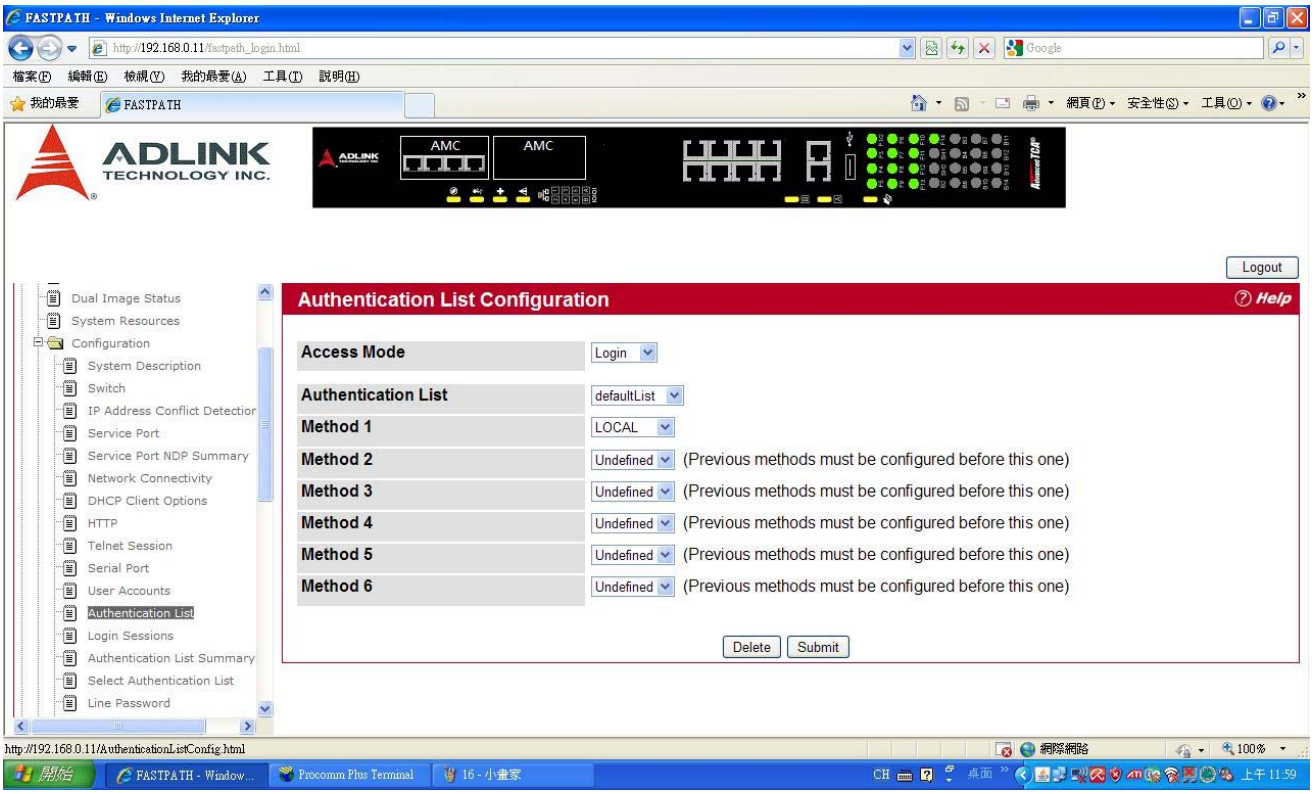
2. Click **Delete** to delete the user. This button is only visible when you have selected a user account with 'Read Only' access. You cannot delete the 'Read/ Write' user.

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 Configuration 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.

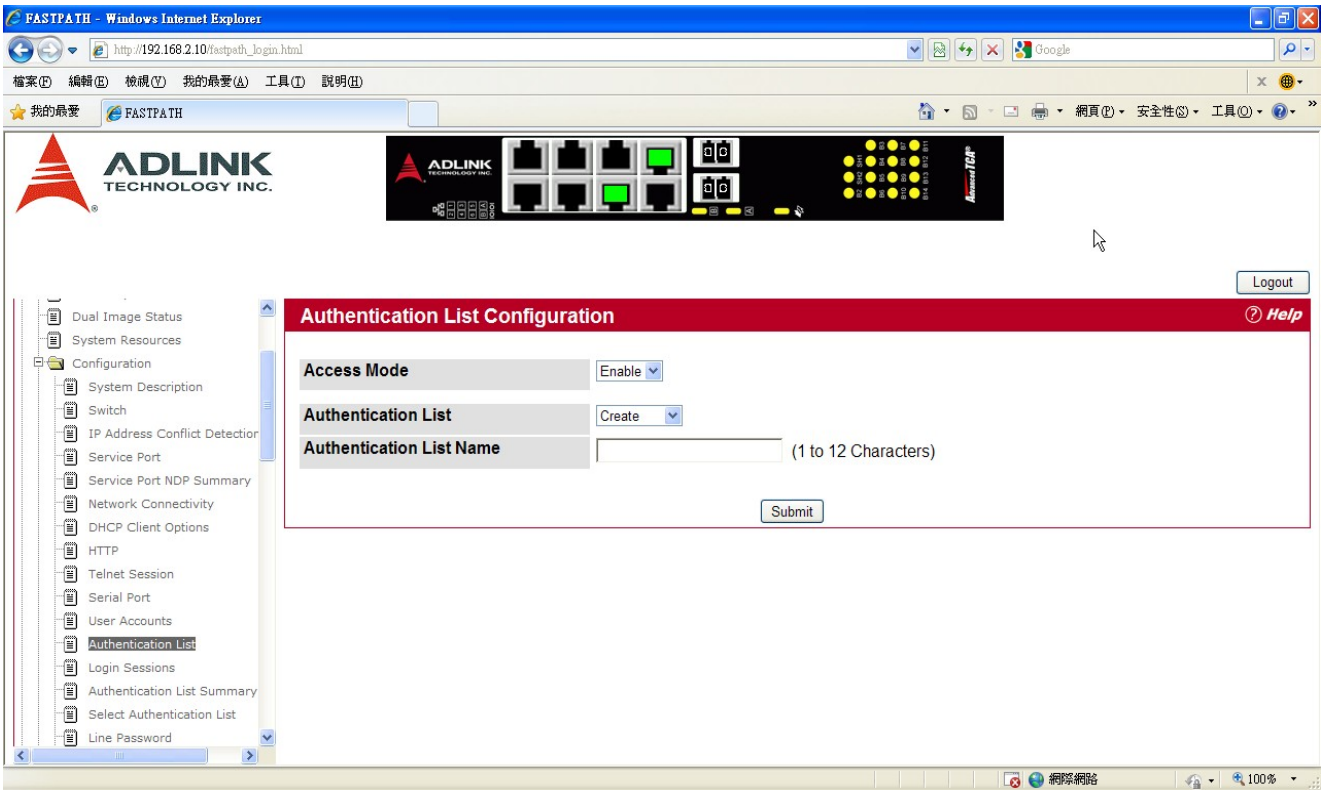
To access the Authentication List Configuration page, click **System > Configuration > Authentication List Configuration** in the navigation tree.



Field	Description
Access Mode	A **Login** or **Enable** list specifies the authentication method you want used to validate switch or port access for the users associated with the list. 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 assign them to a different list.
Authentication List	The menu allows you to create a new authentication list or to select an existing list to view or configure.

Field	Description
Method 1	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. Possible methods are as follows: • **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. • **none**: No authentication is used. **Radius**: The user's ID and password will be authenticated using the RADIUS server instead of locally. • **tacacs+**: The user's ID and password will be authenticated using the TACACS+ server. • **undefined**: The authentication method is unspecified. This option cannot be assigned as **Method 1**. **Note:** If you select a method that does not time out as the **Method 1** (such as **local**) no other method will be tried, even if you have specified more than one method.
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 **Method 2**, the **Method 3** 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. If you select a method that does not time out as the **Method 3**, the **Method 4** will not be tried.
Method 4	Use the menu to select the method, if any, that should appear fourth in the selected authentication login list. If you select a method that does not time out as the **Method 4**, the **Method 5** will not be tried.
Method 5	Use the menu to select the method, if any, that should appear fifth in the selected authentication login list. If you select a method that does not time out as the **Method 5**, the **Method 6** will not be tried.
Method 6	Use the menu to select the method, if any, that should appear sixth in the selected authentication login list.

When **Create** is selected from **Authentication List**, the **Create Authentication List Configuration** page displays.



Field	Description
Access Mode	A **Login** or **Enable** list specifies the authentication method you want used to validate switch or port access for the users associated with the list. 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 assign them to a different list.
Authentication List	The menu allows you to create a new authentication list or to select an existing list to view or configure.
Authentication List Name	If you are creating a new list, enter the name you want to assign. It can be up to 12 alphanumeric characters long and is not case sensitive.

Creating an Authentication List

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

1. Select **Create** from the **Authentication List** field.

2. Select an **Access Mode (Login** or **Enable)** from the drop-down list.

3. In the **Authentication List Name** field, enter a name of 1 to 12 characters. The name cannot include spaces.

4. 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 second through sixth login method from the **Method** fields.

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

1. Use the following procedures to remove an authentication login list from the configuration. Select an existing list from the **Authentication List** menu.
2. Click **Delete**.

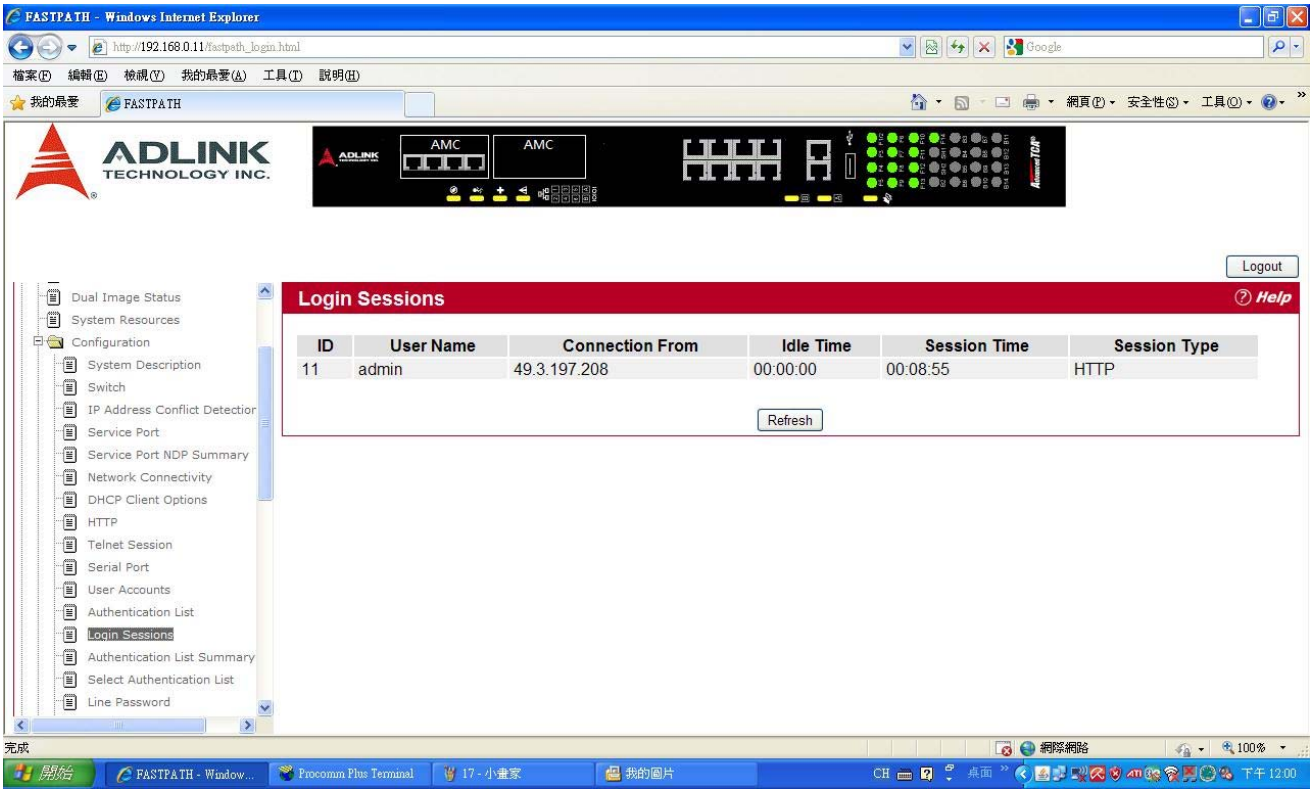
The delete will fail if the selected login list is assigned to any user (including the default user) for system login or IEEE 802.1x port access control. You can only use this button if you have Read/Write access.

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

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 **System > Configuration > Login Session** in the navigation tree.

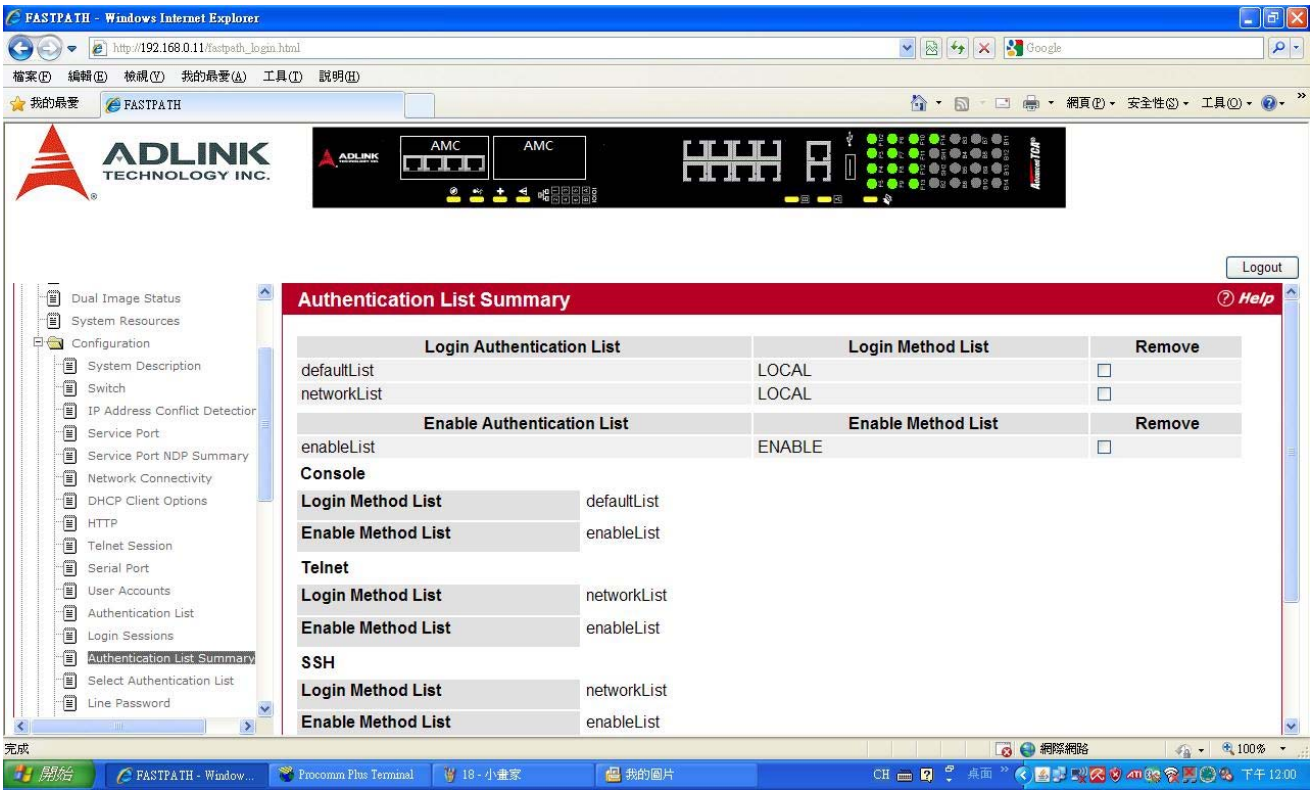


Field	Description
ID	Identifies the ID of this row.
User Name	Shows the user name of the user who is currently logged on to the switch.
Connection From	Shows the IP address of the system from which the user is connected. If the connection is a local serial connection, the **Connection From** field entry 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.

Authentication List Summary

Use the Authentication List Summary page to view information about the authentication lists on the system.

To access the Authentication List Summary page, click System > Configuration > Authentication List Summary in the navigation tree.



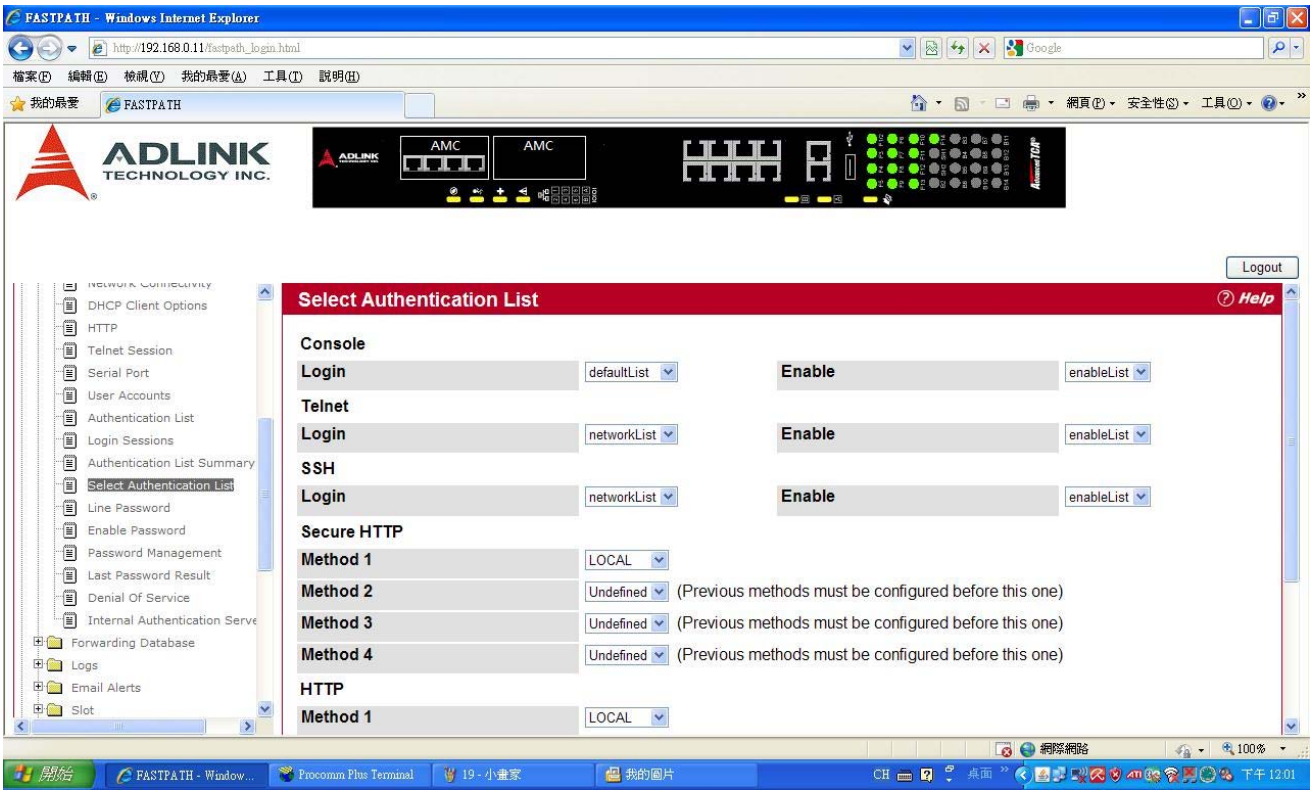
Field	Description
Login Authentication List	Shows the Login authentication profiles.
Enable Authentication List	Shows the Enable authentication profiles.
Note: Authentication profiles are also shown for: •Console •Telnet •SSH •HTTPS •HTTP •802.1x	

Field	Description
Login/Enable Method List	User authentication methods. Possible options are: • 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 • None: the user is not authenticated Radius: the user's ID and password will be authenticated using the RADIUS server • TACACS+: the user's ID and password will be authenticated using the TACACS+ server.
Remove	Removes the authentication profile when checked.

Select Authentication List

Use the Select Authentication List Configuration page to configure authentication methods for session logins.

To access the Select Authentication List page, click System > Configuration > Select Authentication List in the navigation tree.



Field	Description
Console	Authentication profiles used to authenticate console users.
Telnet	Authentication profiles used to authenticate Telnet users.
Secure Telnet (SSH)	Authentication profiles used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.

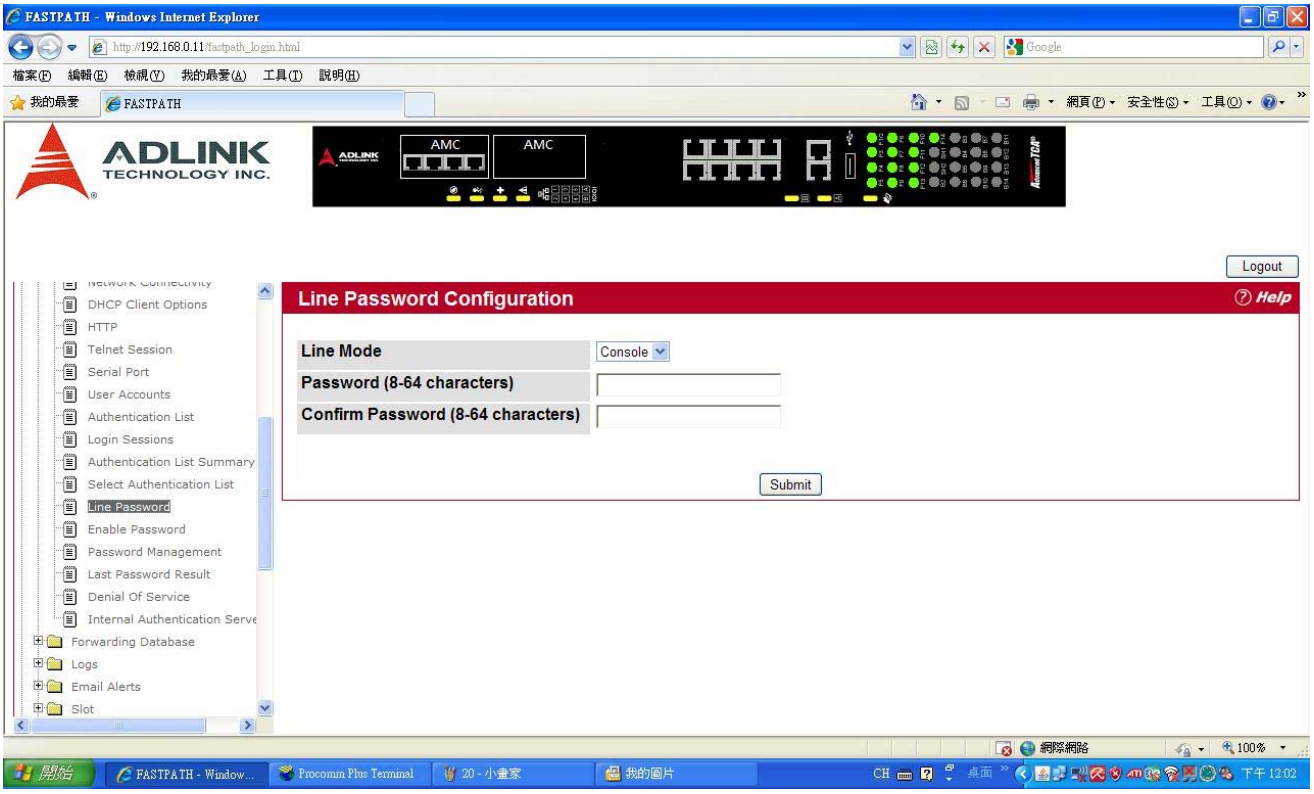
Field	Description
HTTP and Secure HTTP	Authentication method used for HTTP access and Secure HTTP access, respectively. Possible field values are: •Method 1 – Use the dropdown menu to select the method that should appear first in the selected authentication list. If you select a method that does not time out as the first method, such as 'local' no other method will be tried, even if you have specified more than one method. The options are: -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 -None: the user is not authenticated Radius: the user's ID and password will be authenticated using the RADIUS server instead of locally -TACACS+: the user's ID and password will be authenticated using the TACACS+ server -Reject: the user is never authenticated -Undefined: the authentication method is unspecified (this may not be assigned as the first method) •Method 2 – Use the dropdown menu to select the method, if any, that should appear second in the selected authentication 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 dropdown menu to select the method, if any, that should appear third in the selected authentication list. This is the method that will be used if the second method times out. If you select a method that does not time out as the third method, the fourth method will not be tried. •Method 4 – Use the dropdown menu to select the method, if any, that should appear fourth in the selected authentication list.

Field	Description
DOT1X	Authentication method used for Dot1x access. Possible field values are: •Method 1 – Use the dropdown menu to select the method that should appear first in the selected authentication list. If you select a method that does not time out as the first method, such as 'local' no other method will be tried, even if you have specified more than one method. The options are: -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 -None: the user is not authenticated Radius: the user's ID and password will be authenticated using the RADIUS server instead of locally -TACACS+: the user's ID and password will be authenticated using the TACACS+ server -Reject: the user is never authenticated -Undefined: the authentication method is unspecified (this may not be assigned as the first method) •Method 2 – Use the dropdown menu to select the method, if any, that should appear second in the selected authentication 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 dropdown menu to select the method, if any, that should appear third in the selected authentication list.

Line Password

Use the Line Password page to configure line mode passwords.

To display the page, click System > Configuration > Line Password in the navigation tree.



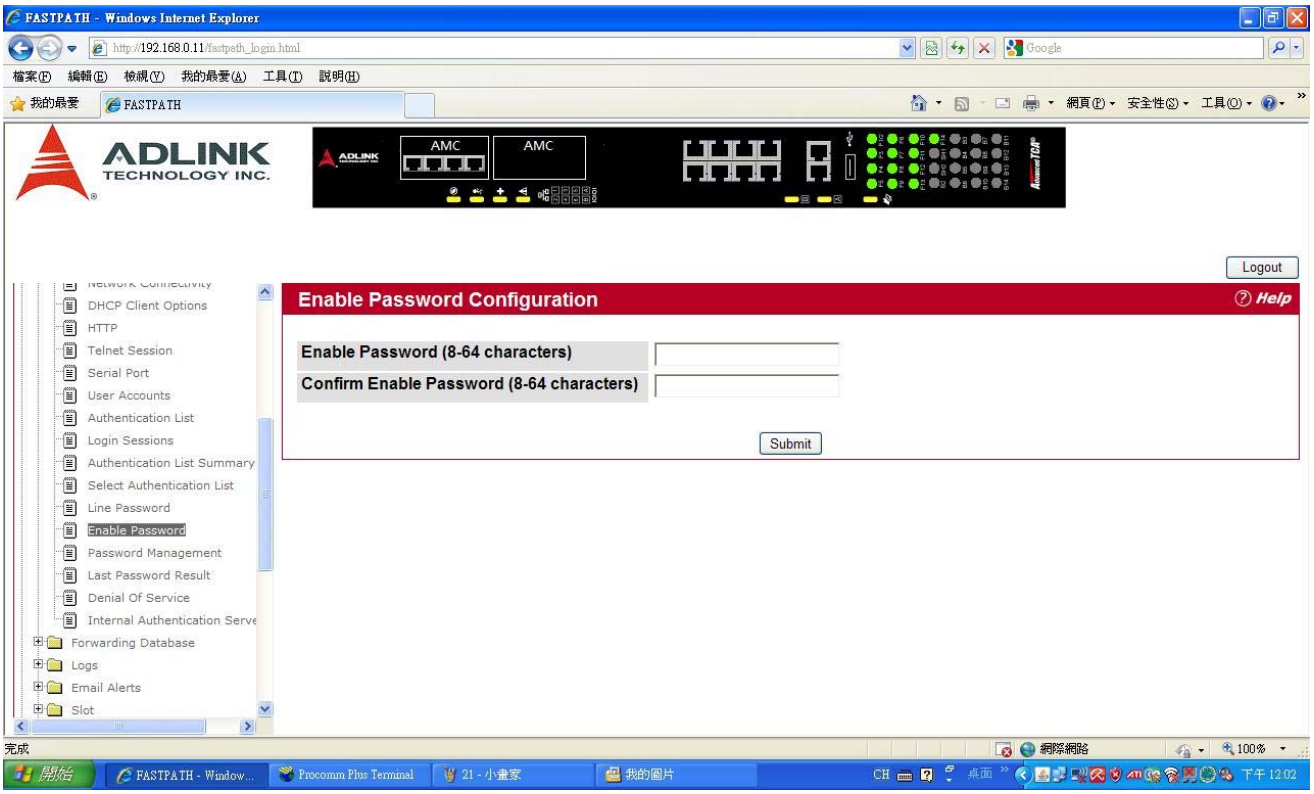
Field	Description
Line Mode	Select the Line Mode from the drop-down list.
Line Password (8-64 characters)	The line password for accessing the device via a console, Telnet, or Secure Telnet session.
Confirm Password (8-64 characters)	Confirms the new line password. The password appears in the ***** format.

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.

Enable Password

Use the Enable Password page to configure the enable password.

To display the page, click System > Configuration > Enable Password in the navigation tree.



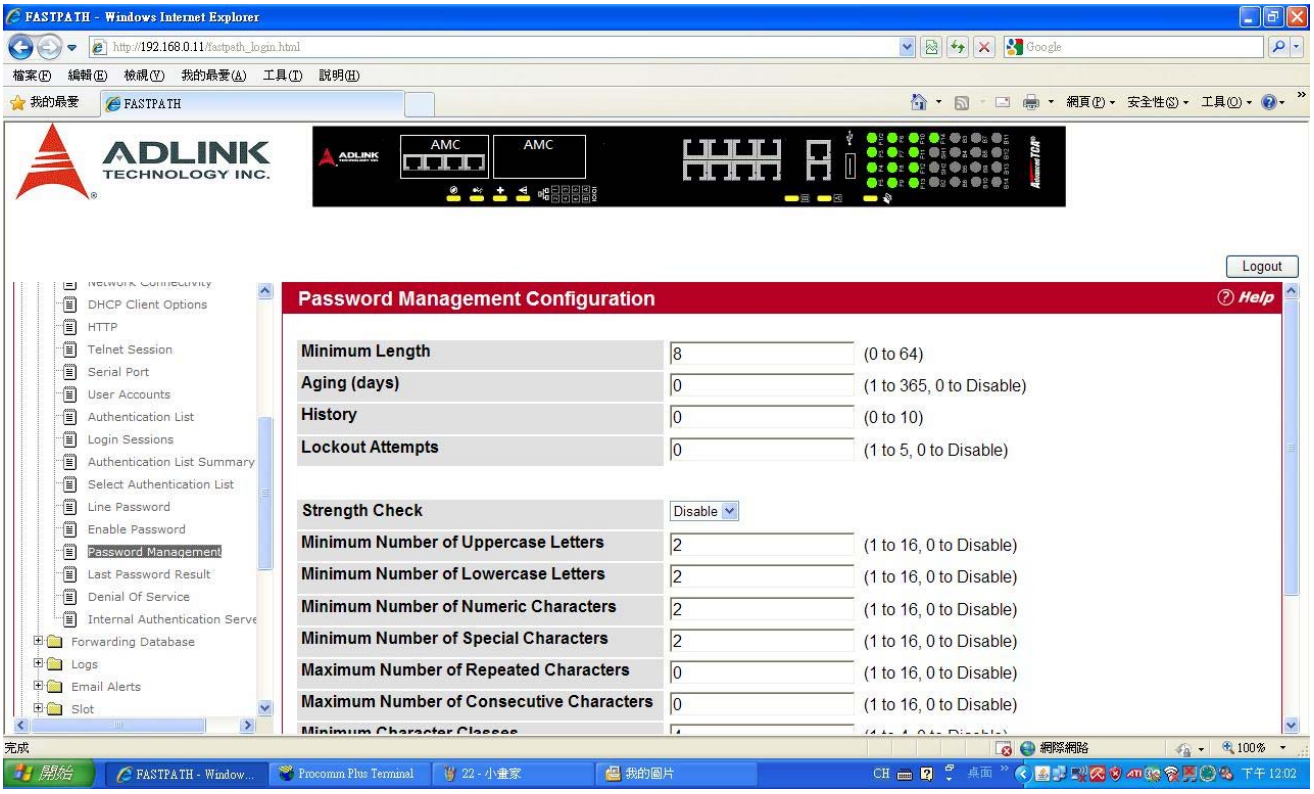
Field	Description
Enable Password (8-64 characters)	The enable password is for accessing the device via a console, Telnet, or Secure Telnet session.
Confirm Enable Password (8-64 characters)	Confirms the new enable password. The password appears in the ***** format.

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.

Password Management

Use this page to configure settings that apply to all user passwords.

To display the page, click Configuration > Password Management in the navigation tree.



Field	Description
Password Minimum Length	Passwords must have at least this many characters (8 to 64).
Password Aging (days)	Passwords will expire this many days after creation.
Password History	Users cannot reuse previous passwords up to this number.
Lockout Attempts	After a user fails to log in this number of times, the user is locked out until the password is reset by the administrator.

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.

Denial of Service

Use the Denial of Service (DoS) page to configure DoS control. FASTPATH® software provides support for classifying and blocking specific types of DoS attacks. You can configure your system to monitor and block these types of attacks:

• SIP=DIP: Source IP address = Destination IP address.

• First Fragment: TCP Header size smaller then configured value.

• TCP Fragment: IP Fragment Offset = 1.

• TCP Flag: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.

• L4 Port: Source TCP/UDP Port = Destination TCP/UDP Port.

• ICMP: Limiting the size of ICMP Ping packets.

•SMAC=DMAC: Source MAC address=Destination MAC address.

•TCP Port: Source TCP Port = Destination TCP Port.

•UDP Port: Source UDP Port = Destination UDP Port.

•TCP Flag & Sequence: TCP Flag SYN set and Source Port < 1024 or TCP Control Flags = 0 and TCP Sequence Number = 0 or TCP Flags FIN, URG, and PSH set and TCP Sequence Number = 0 or TCP Flags SYN and FIN set.

•TCP Offset: TCP Header Offset = 1.

•TCP SYN: TCP Flag SYN set.

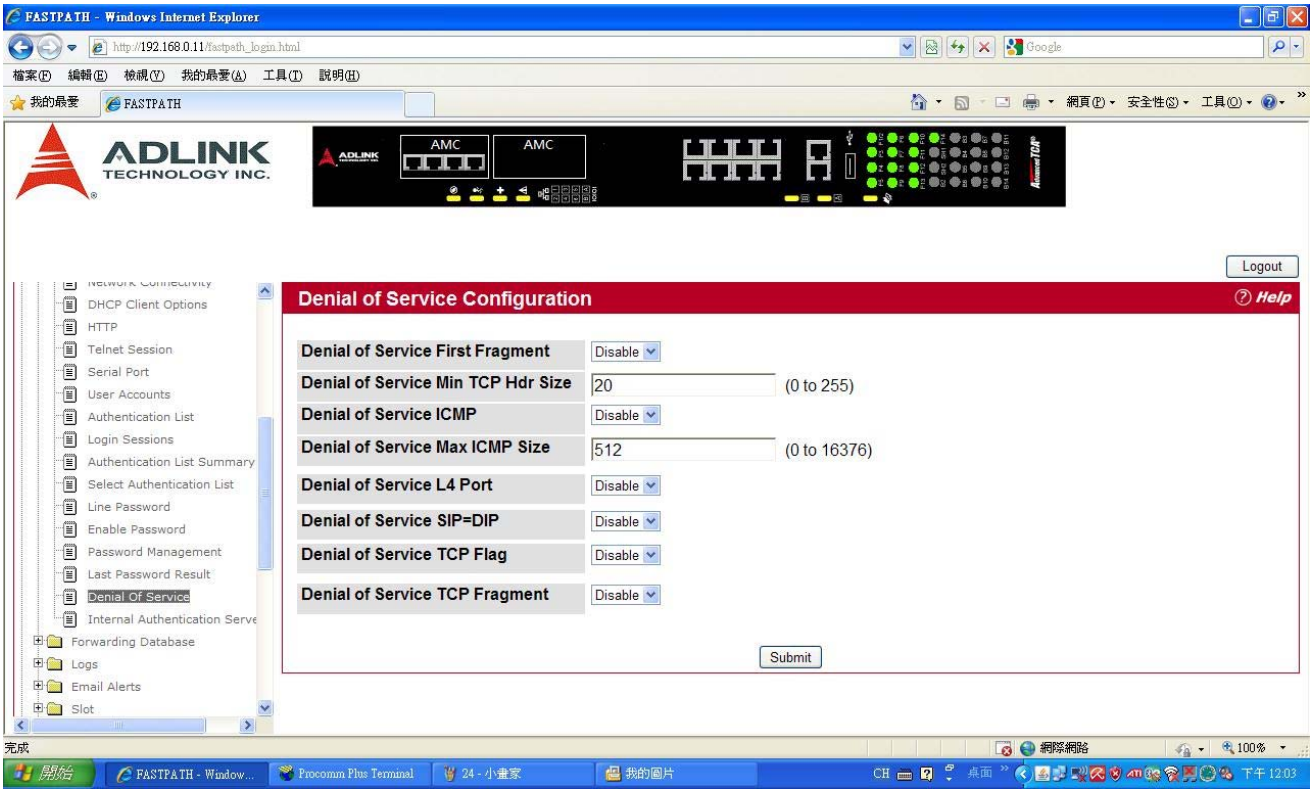
•TCP SYN & FIN: TCP Flags SYN and FIN set.

•TCP FIN & URG & PSH: TCP Flags FIN and URG and PSH set and TCP Sequence Number = 0.

•ICMP V6: Limiting the size of ICMPv6 Ping packets.

•ICMP Fragment: Checks for fragmented ICMP packets.

To access the Denial of Service page, click System > Configuration > Denial of Service in the navigation menu.



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 then 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 then 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 ICMPv4 Pkt Size	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Specify the Max ICMPv4 Pkt Size allowed. If ICMP DoS prevention is enabled, the switch will drop Ipv4 ICMP ping packets that have a size greater than this configured Max ICMP Pkt Size. The factory default is disabled.

Field	Description
Denial of Service Max ICMPv6 Pkt Size	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Specify the Max ICMPv6 ICMP Pkt Size allowed. If ICMP DoS prevention is enabled, the switch will drop Ipv6 ICMP ping packets that have a size greater than this configured Max ICMP Pkt Size. The factory default is disabled.
Denial of Service ICMP Fragment	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling ICMP Fragment DoS prevention causes the switch to drop ICMP Fragmented packets. 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 SMAC=DMAC	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling SMAC=DMAC DoS prevention causes the switch to drop packets that have a source MAC address equal to the destination MAC address. The factory default is disabled.
Denial of Service TCP FIN&URG&PSH	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP FIN & URG & PSH DoS prevention causes the switch to drop packets that have TCP flags FIN, URG, and PSH set and TCP Sequence Number = 0. The factory default is disabled.
Denial of Service TCP Flag&Sequence	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. 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 control flags set to 0 and TCP sequence number set to 0. 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.
Denial of Service TCP Offset	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Offset DoS prevention causes the switch to drop packets that have a TCP header Offset equal to 1. The factory default is disabled.

Field	Description
Denial of Service TCP Port	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP Port DoS prevention causes the switch to drop packets that have TCP source port equal to TCP destination port. The factory default is disabled.
Denial of Service TCP SYN	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP SYN DoS prevention causes the switch to drop packets that have TCP Flags SYN set. The factory default is disabled.
Denial of Service TCP SYN&FIN	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling TCP SYN & FIN DoS prevention causes the switch to drop packets that have TCP Flags SYN and FIN set. The factory default is disabled.
Denial of Service UDP Port	**Note:** This field is only supported on the BCM56514, BCM56624, BCM56820, BCM56224, BCM56634, and BCM56636 platforms. Enable or disable this option by selecting the corresponding line on the pulldown entry field. Enabling UDP Port DoS prevention causes the switch to drop packets that have UDP source port equal to UDP destination port. 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.

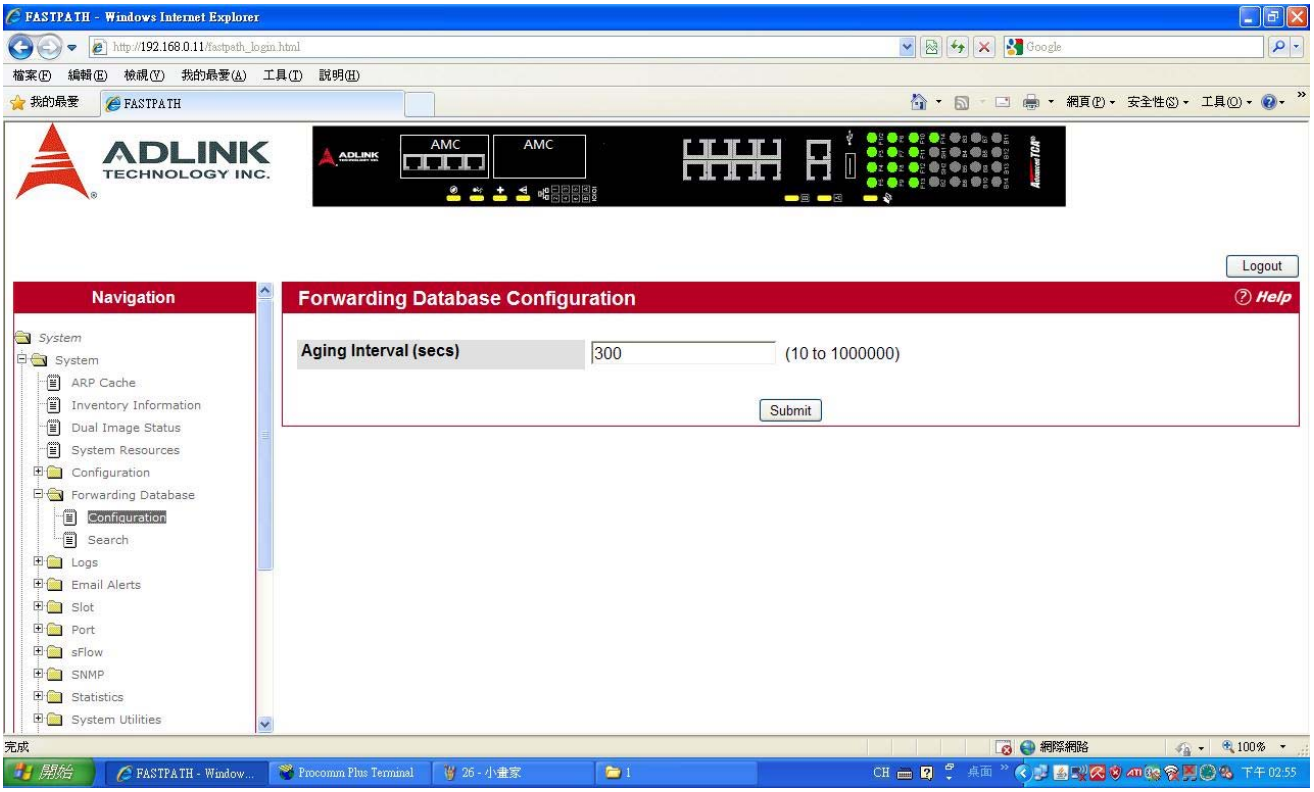
Configuring and Searching the Forwarding Database

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 **System > Forwarding Database > Configuration** in the navigation tree.

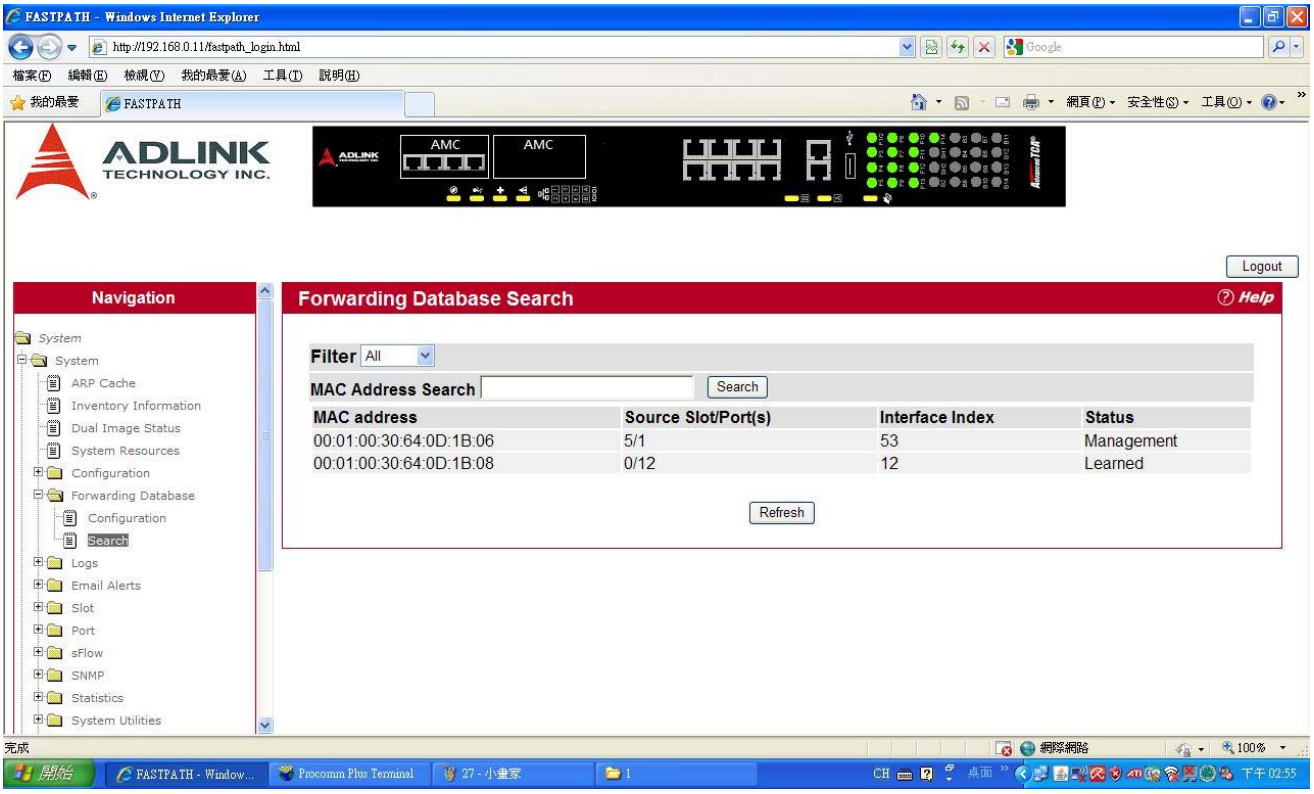


Field	Description
Aging Interval (secs)	Specify the number of seconds the forwarding database should wait before deleting a learned entry that has not been updated. You may enter any number of seconds between 10 and 1000000.

Search

Use the Search page to display information about entries in the forwarding database.

To access the Search page, click **System > Forwarding Database > Search** in the navigation tree.



Field	Description
Management Unit	For stacking systems, this field displays management unit for which Forwarding Database Table is to be displayed. This field is not present in systems that do not support stacking.
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: • **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.

Field	Description
Source Port	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: • **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.

5.3. Managing Logs

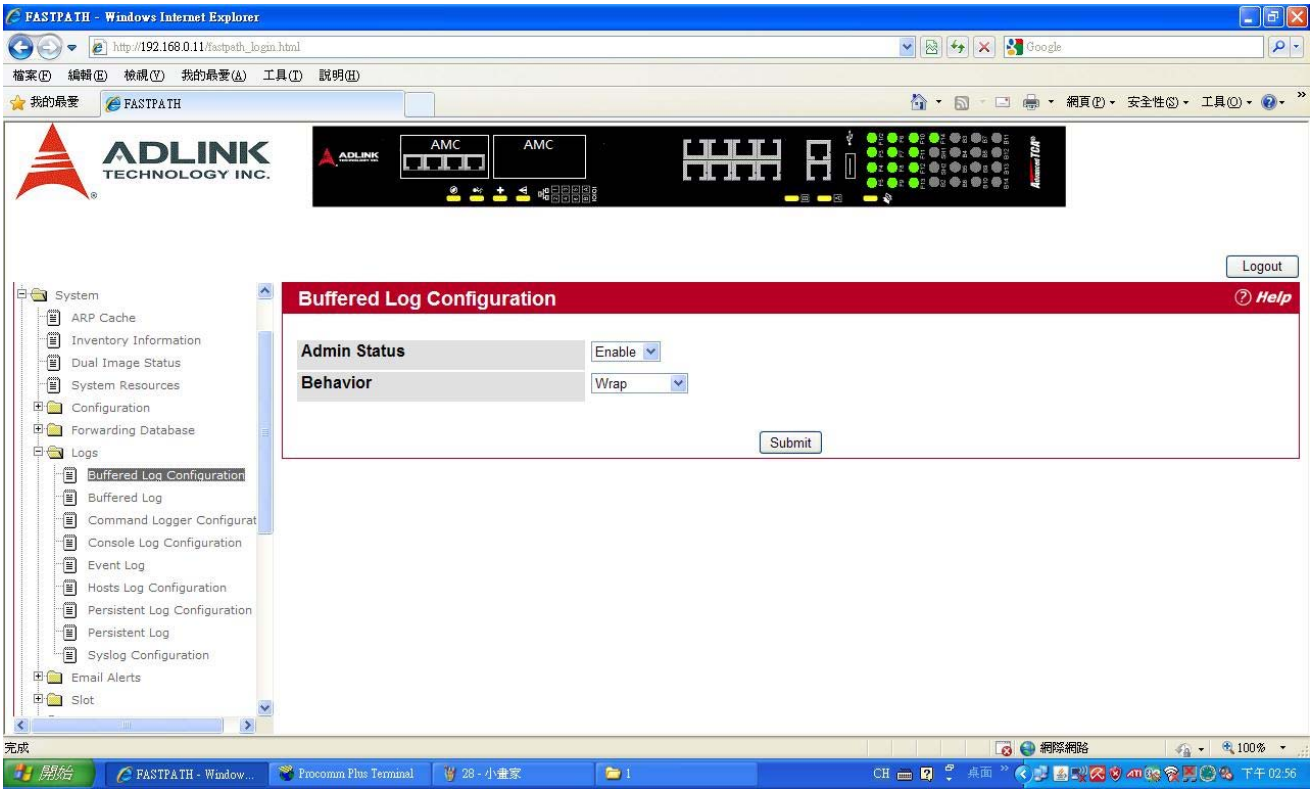
The switch may generate messages in response to events, faults, or errors occurring on the platform as well as changes in configuration or other occurrences. These messages are stored both locally on the platform and forwarded to one or more centralized points of collection for monitoring purposes as 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. On stackable systems, this log exists only on the management unit. Other platforms in the stack forward their messages to the management unit log. Access to in-memory logs on other than the management unit is not supported. The Log folder contains links to the following pages:

- Buffered Log Configuration
- Buffered Log
- Command Logger Configuration
- Console Log Configuration
- Event Log
- Hosts Configuration
- Persistent Log Configuration
- Persistent Log
- Syslog Configuration

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 **System > Log > Buffered Log Configuration** in the navigation tree.



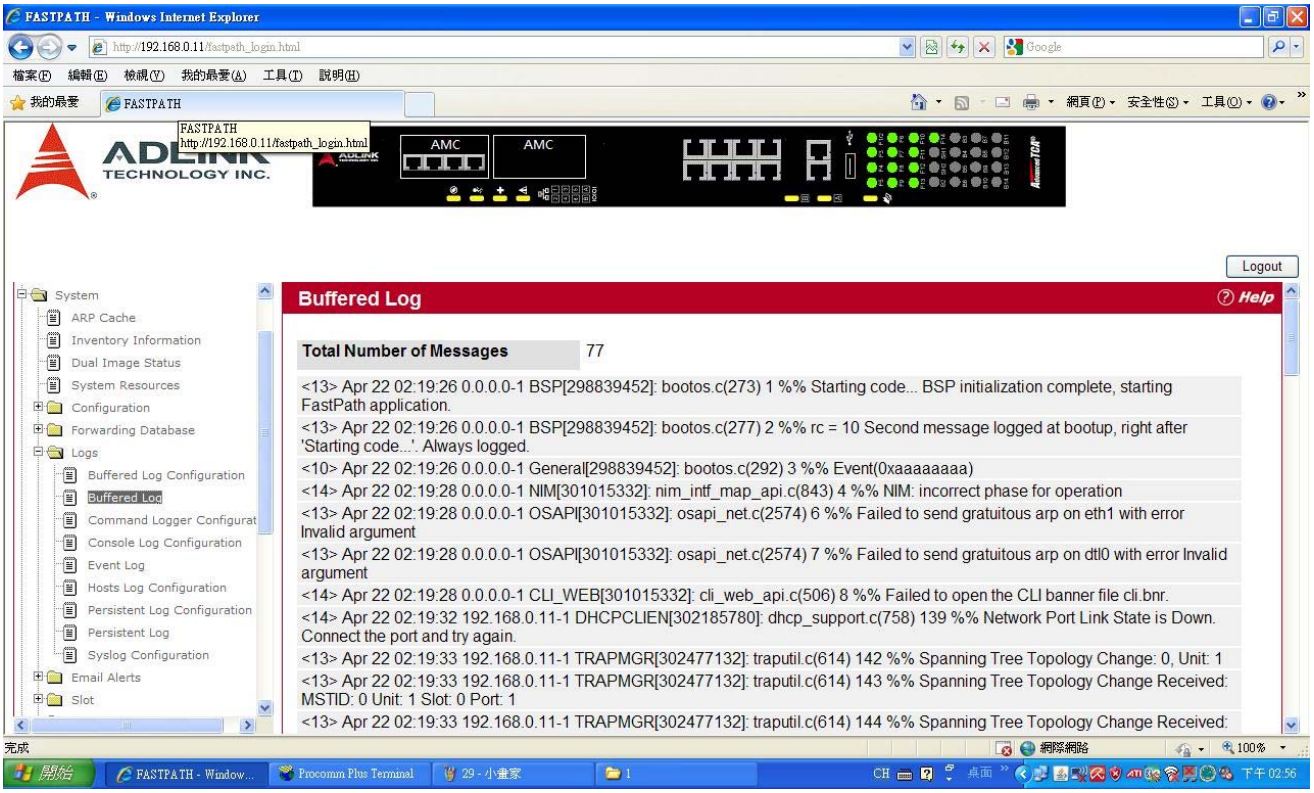
Field	Description
Admin Status	Determines whether to log messages. • **Enable**: Enables system logging. • **Disable**: Prevents the system from logging messages.
Behavior	Indicates the behavior of the log when it is full. • **Wrap**: When the buffer is full, the oldest log messages are deleted as the system logs new messages. • **Stop on Full**: When the buffer is full, the system stops logging new messages and preserves all existing log messages.

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.

Buffered Log

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 **System > Log > Buffered Log** in the navigation menu.



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 for a non-stacking system:

<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 mstp_api.c. This is the 237th message logged. The following example shows a log message generated on a system that supports stacking:

<15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry

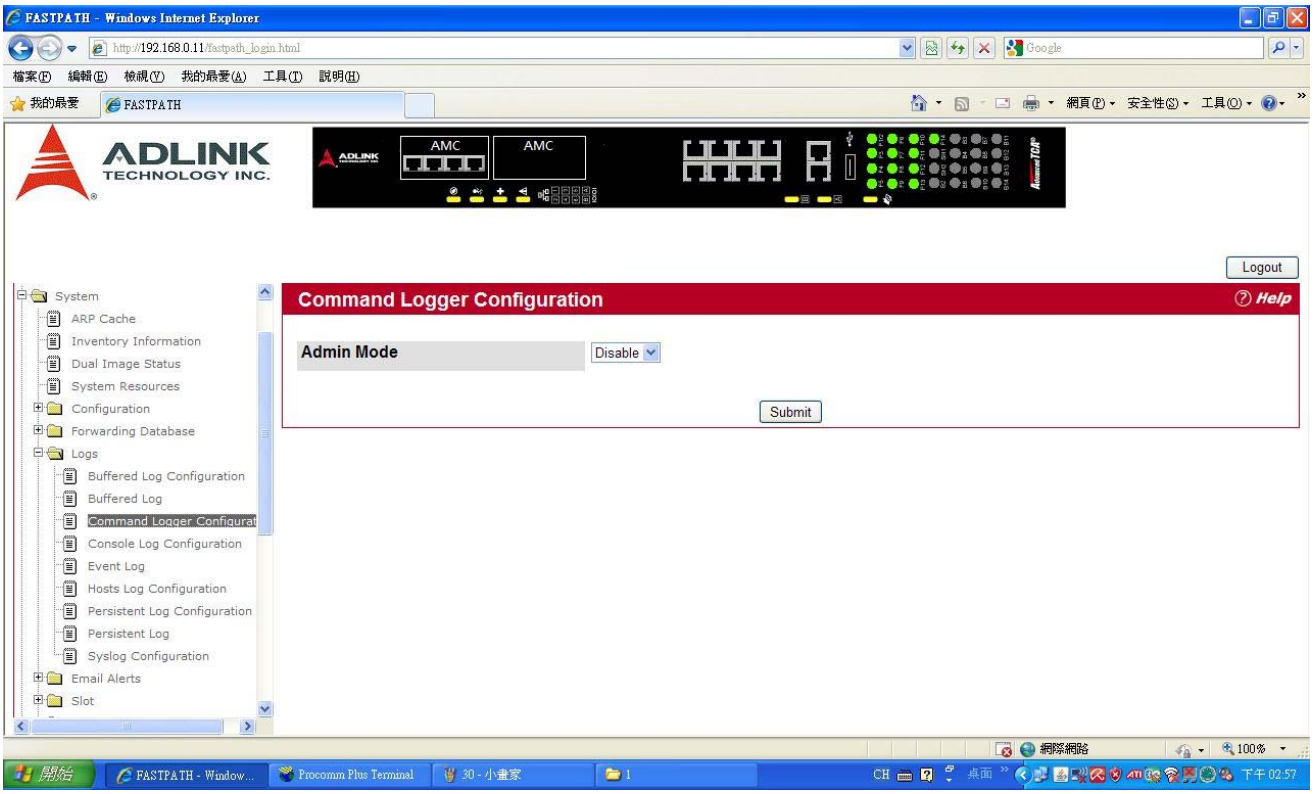
This log message has a severity level of 7 (15 mod 8), which is a debug message. The message was generated by the MSTP component running in thread id 2110. The message was generated on August 24 05:34:05 by line 318 of file mstp_api.c. This is the 237th message logged with system IP 0.0.0.0 and unit number 1.

Click **Refresh** to update the screen and associated 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 **System > Log > Command Logger Configuration** in the navigation menu.



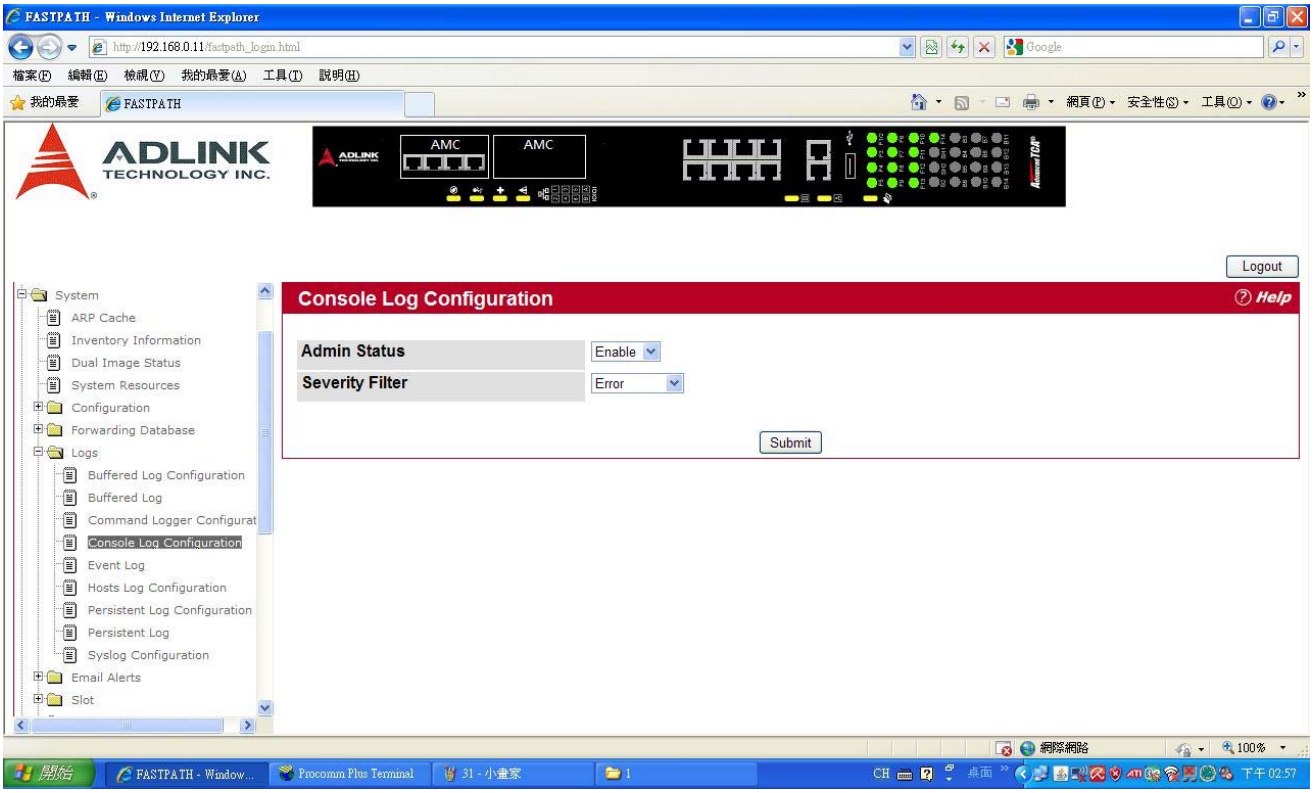
Field	Description
Admin Mode	This field determines whether to log CLI commands in the system log file. • **Enable**: The system logs CLI commands. The commands appear in messages on the Buffered Log page. For example, the following log messages shows when the CLI command show logging buffered was issued, from which IP address the command was issued, and the name of the user who issued the command: <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 • **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 **System > Log > Console Log Configuration** in the navigation menu.



Field	Description
Admin Status	From the menu, select whether to enable or disable console logging. The default is disabled. • **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	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: • **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.

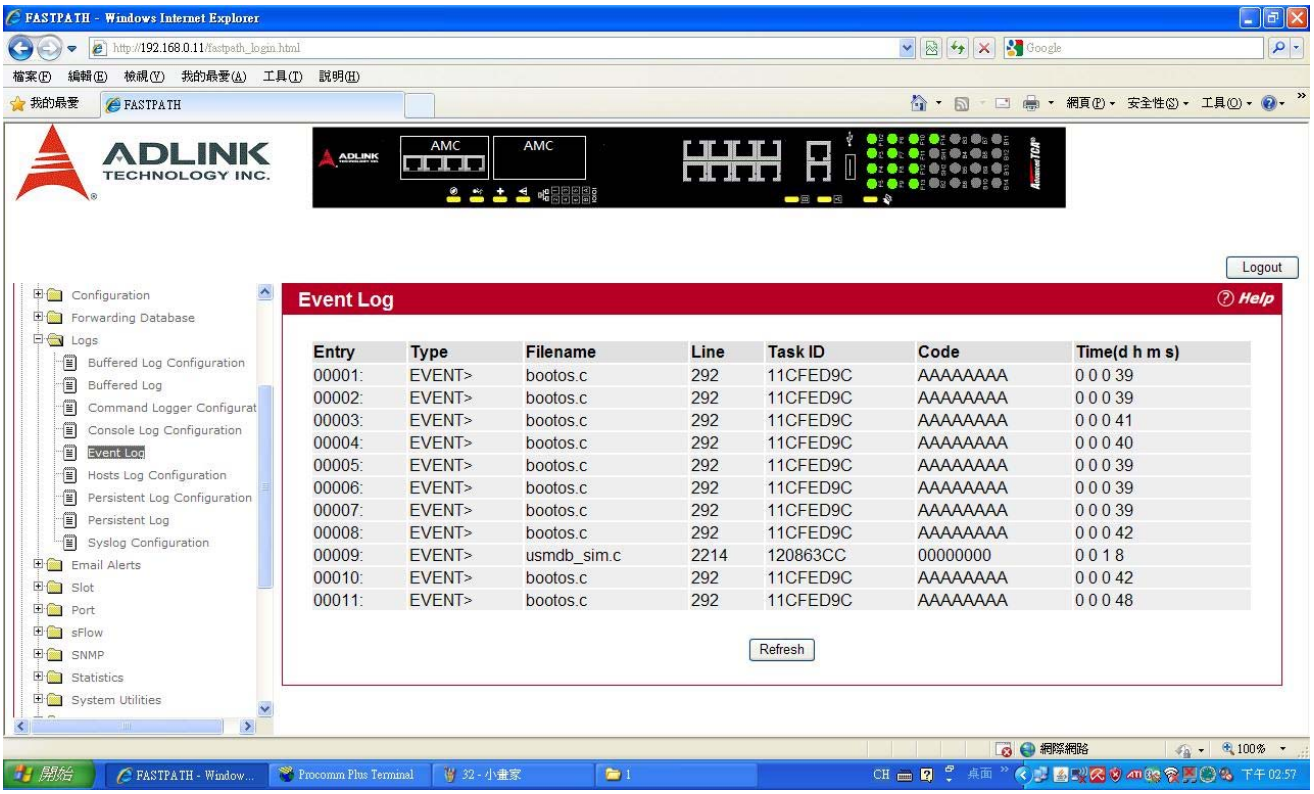
Field	Description
	• **Critical (2)**: The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional. • **Error (3)**: A device error has occurred, such as if a 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.

zIf 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 **System > Log > Event Log** in the navigation tree.



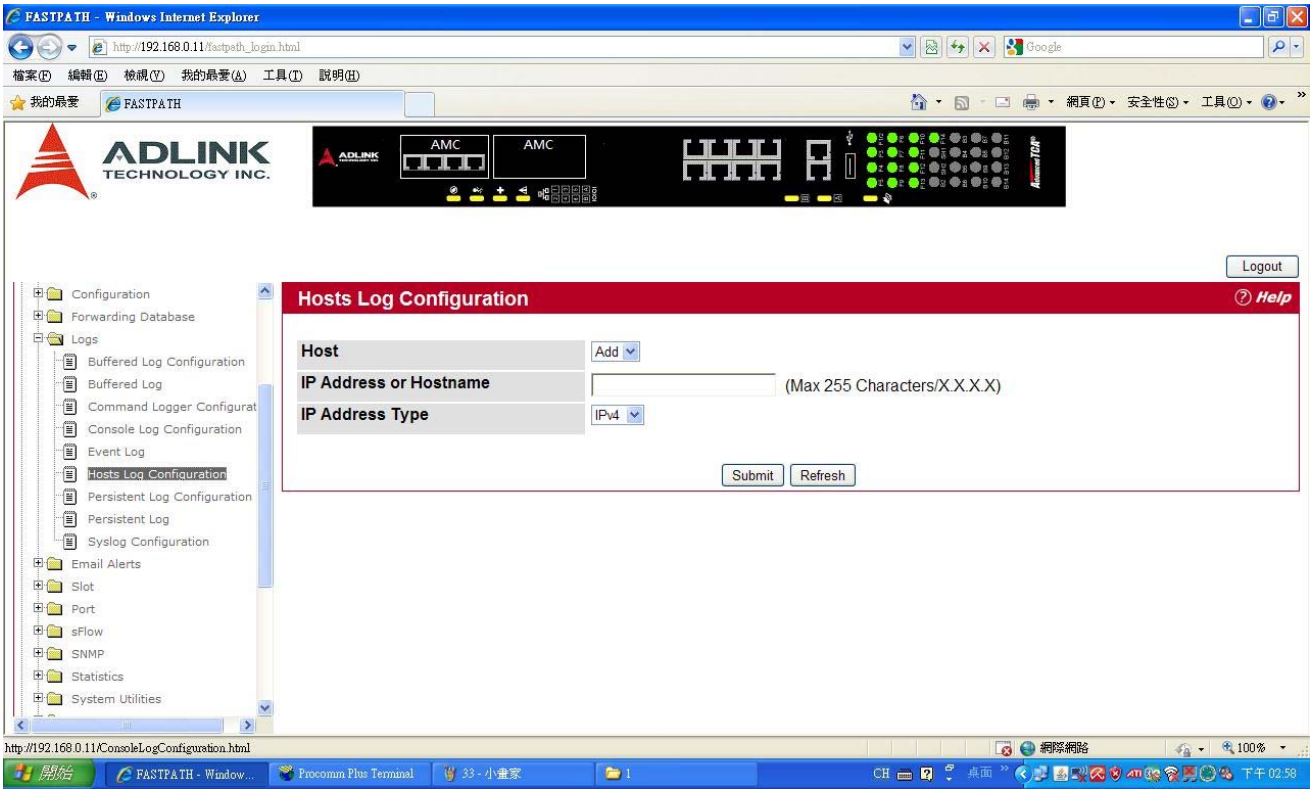
Field	Description
Entry	The number of the entry within the event log. The most recent entry is first.
Filename	The FASTPATH® source code filename identifying the code that detected the event.
Line	The line number within the source file of the code that detected the event.
Task ID	The OS-assigned ID of 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 screen and associated messages

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”.

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



Field	Description
Host	Select a host from the list of hosts that have been configured to receive log messages. Select **Add** to add a new host, or select the IP address of an existing host to view or change the settings.
IP Address or Hostname	Enter the IP address or hostname of the host configured for syslog.
IP Address Type	Select the form of the address entered above: • IPv4: The address is specified in standard dot notation. • DNS: The address is specified as a host name.
Status	Shows whether the remote logging host is currently active.
Port	Identifies the port on the host to which syslog messages are sent. The default port is 514. Specify the port in the text field.
Severity Filter	Use the menu to select the severity of the logs to send to the logging host. Logs with the selected severity level and all logs of greater severity are sent to the host. 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

Field	Description
	following levels: • **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.

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.

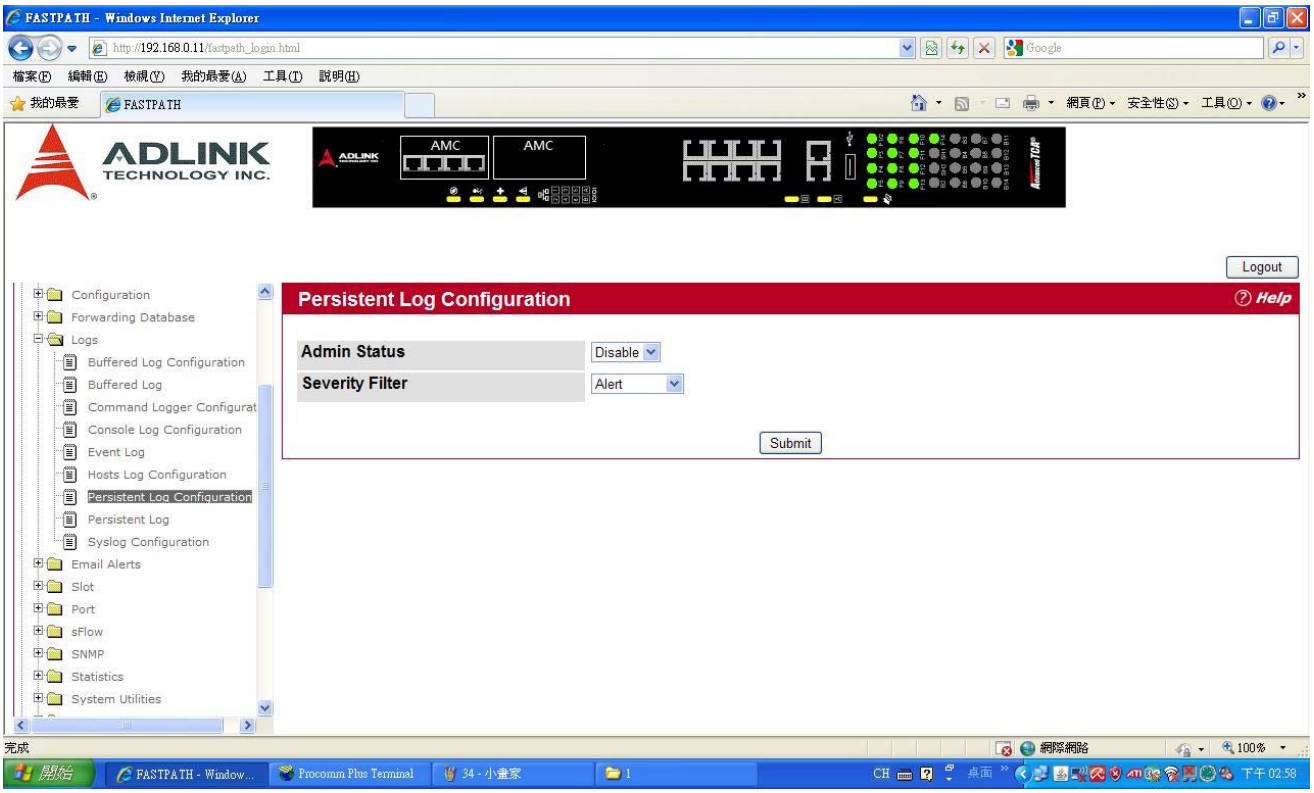
Either the system startup log or the system operation log stores a message received by the log subsystem that meets the storage criteria, but not both. In other words, on system startup, if the startup log is configured, it stores messages up to its limit. The operation log, if configured, then begins 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 olog for the operation log and slog 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 **System > Log > Persistent Log Configuration** in the navigation menu.



Field	Description
Admin Status	Select whether to enable or disable persistent logging. The default is disabled. • **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	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: • **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.

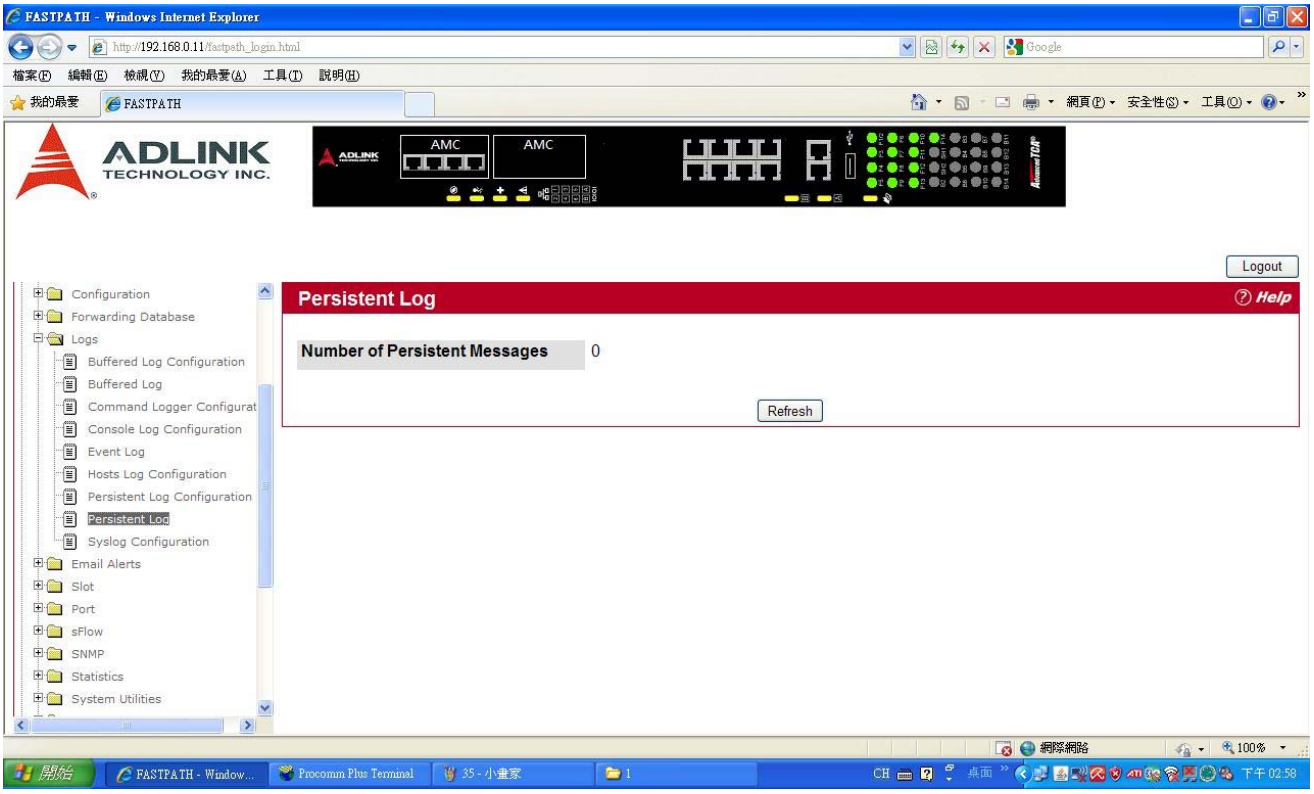
Field	Description
	• **Warning (4)**: The lowest level of a device warning. • **Notice (5)**: Provides the network administrators with device information. • **Informational (6)**: Provides device information. • **Debug (7)**: Provides detailed information about the log. Debugging should only be entered 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 **System > Log > Persistent Log** in the navigation tree menu.



Field	Description
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 for a non-stacking system:

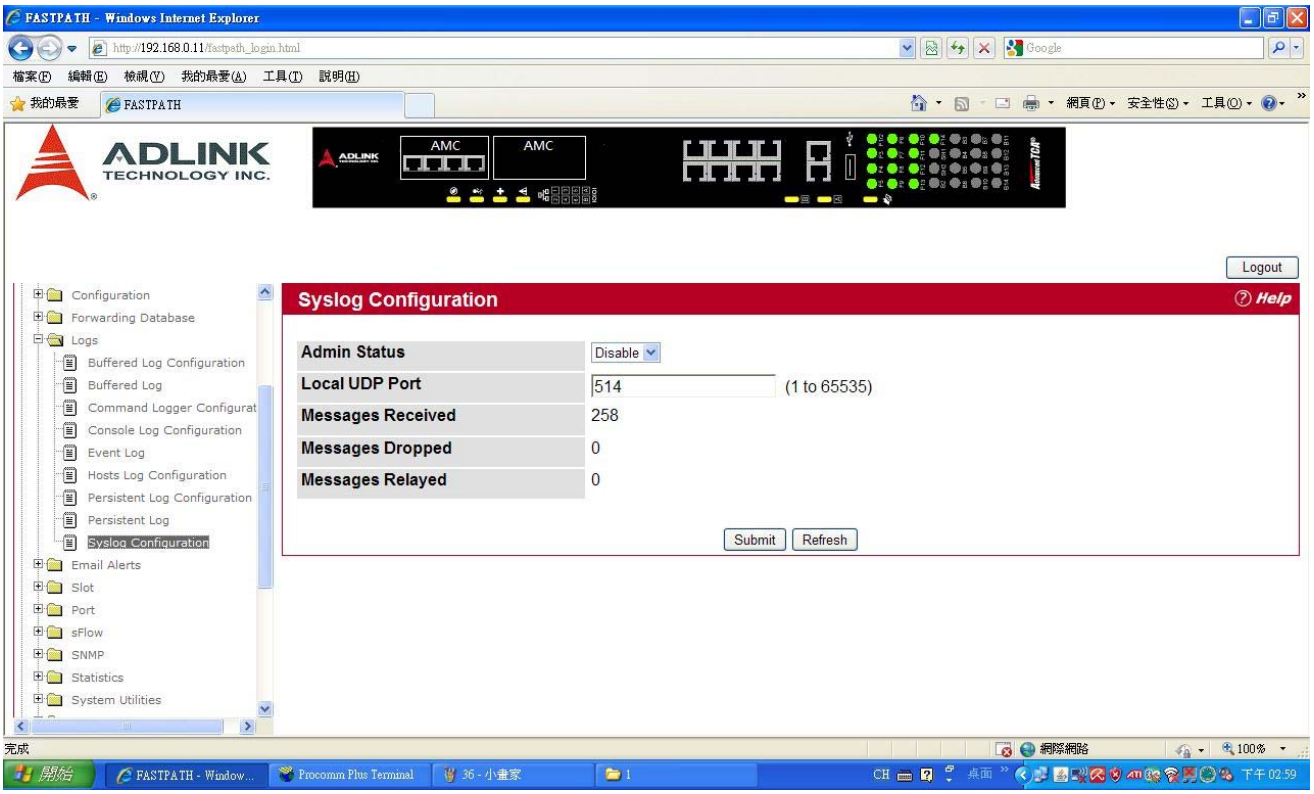
<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root state on message age timer expiry

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 mstp_api.c. This is the 237th message logged.

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 Syslog Configuration page, click **System > Log > Syslog Configuration** in the navigation tree.



Field	Description
Admin Status	Specifies whether to send log messages to the remote syslog hosts configured on the switch: • **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” . • **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.

Field	Description
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.

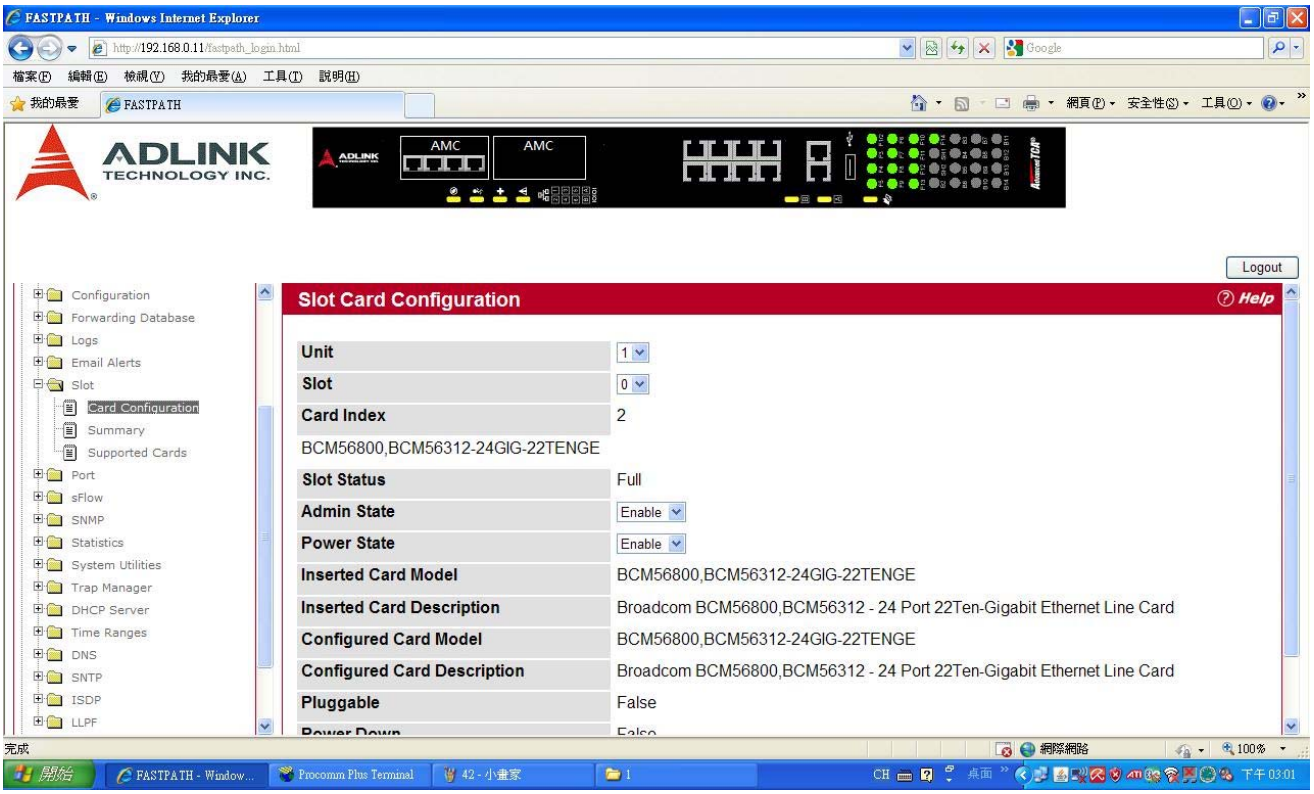
Configuring And Viewing Device Slot Information

The pages in the Slot folder provide information about the cards installed in the slots on the switch. The physical location of the slots depends on the hardware on which FASTPATH® software is running. From the Configuration page, you can also manually configure information about cards on some platforms.

Configuration

Use the Card Configuration page to view information about the cards installed in a switch. On some platforms, you can manually configure information about slots.

To access the Card Configuration page, click **System > Slot > Card Configuration** in the navigation menu.



Field	Description
Unit	Indicates the unit in the stack for which data is to be displayed or configured.
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.

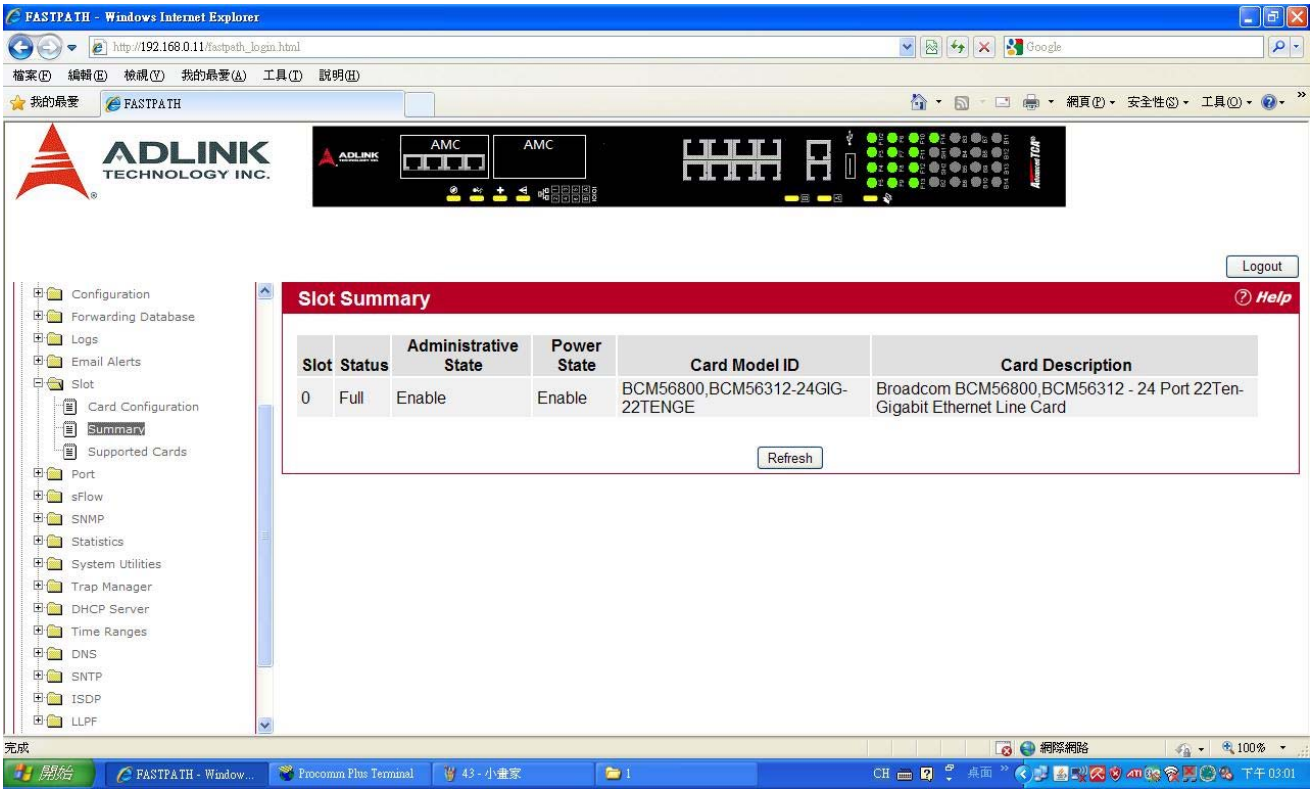
Field	Description
Power State	Displays whether the slot is powered on of off. This field is non-configurable for read-only users.
Card Type	Displays a list of possible supported card types which can be plugged into the slot. This is visible only for slots which do not have any cards plugged into them and which have not already been pre-configured. This field is not visible to 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 **Refresh** to redisplay the page with the current data from the switch.

Slot Summary

The Slot Summary page displays information about the different slots in each unit in the stack.

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



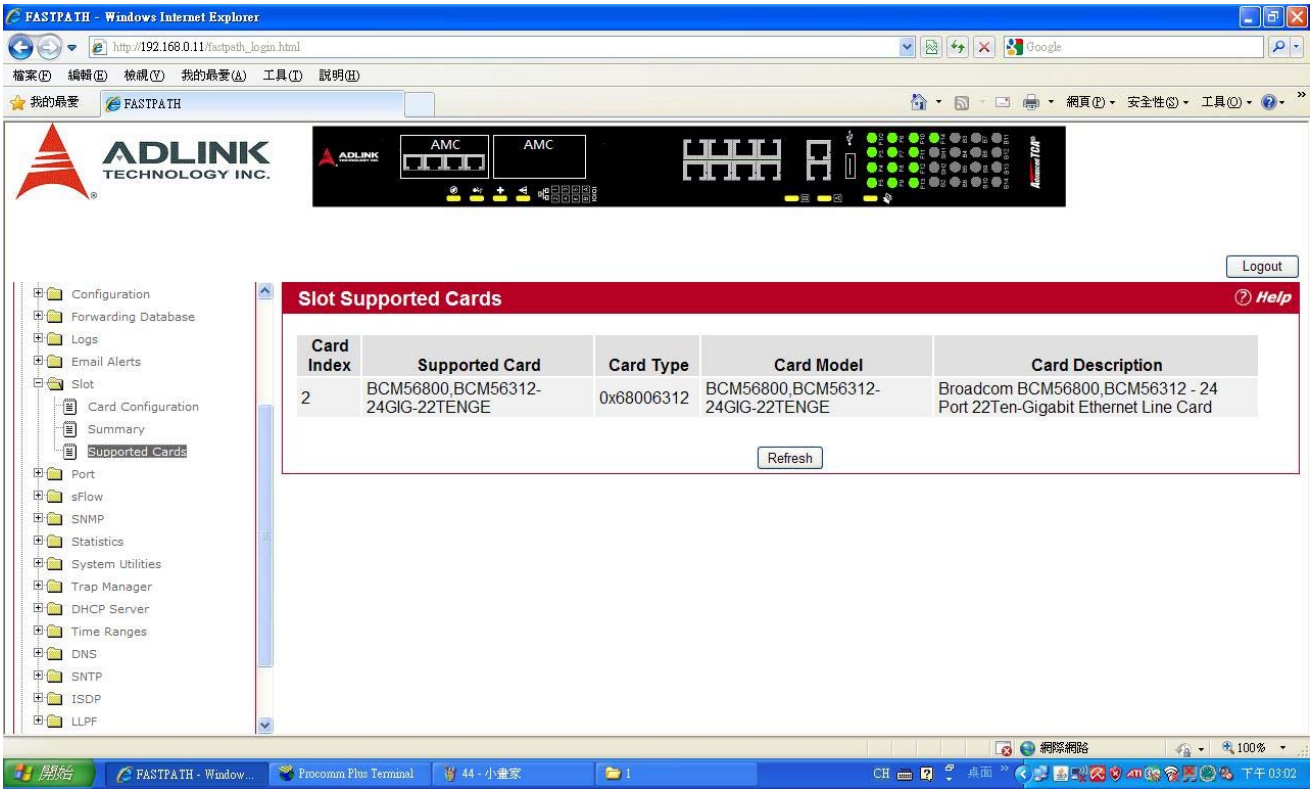
Field	Description
Slot	Identifies the slot using the format unit/slot.
Status	Displays whether the slot is empty or full.
Administrative State	Displays whether the slot is administratively enabled or disabled
Power State	Displays whether the slot is powered on of off.
Card Model ID	Displays the model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

Click **Refresh** to redisplay the most current information from the router.

Supported Cards

The Supported Cards page provides information about the cards that your platform supports.

To access the Supported Cards page, click **System > Slot > Supported Cards** in the navigation menu.



Field	Description
Card Index	Displays the index assigned to the selected card type.
Supported Cards	The menu contains the list of all cards that the system can support. To view information about a card, select it from the drop-down list. The screen refreshes, and the information about that card appears in the other fields on the page.
Card Type	Displays the hardware type of this supported card. This is a 32-bit data field.
Card Model ID	Displays the string to identify the model of the supported card.
Card Descriptor	Displays a data field used to identify the supported card.

Click **Refresh** to redisplay the most current information from the router.

5.4. Configuring And Viewing Device Port Information

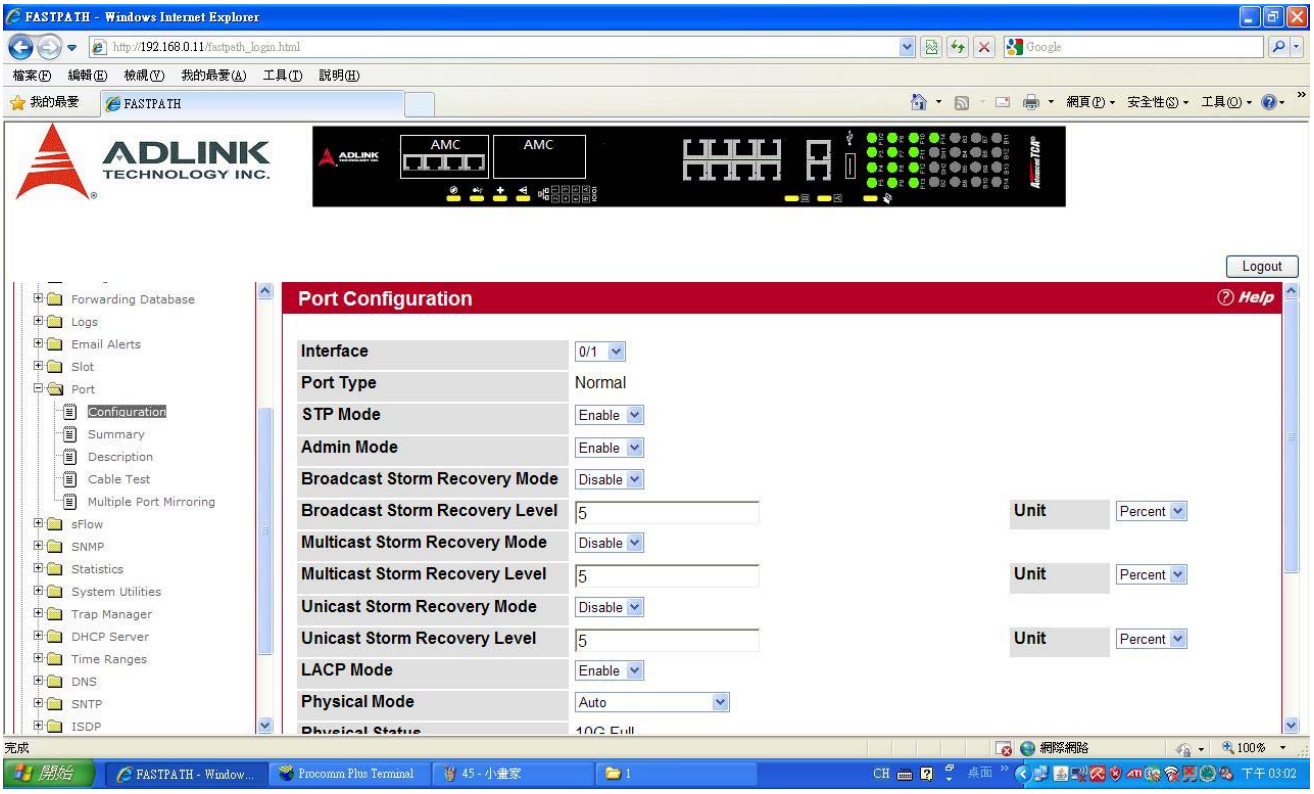
The pages in the Port folder allow you to view and monitor the physical port information for the ports available on the switch. The Port folder has links to the following pages:

- Configuration
- Summary
- Port Description
- Cable Test
- Multiple Port Mirroring

Configuration

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

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



Field	Description
Interface	Select the port from the menu to display or configure data for that port. The field is **Slot/ Port** for non-stacking platforms. 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: • **Mirrored**: Indicates that the port has been configured as a monitoring port and is the source port in a port mirroring session. For more information about port monitoring and probe ports, see “Multiple Port Mirroring” . • **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” . • **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” .

Field	Description
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” . The possible values for this field are: • **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: • **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: • **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 factory default is 5 percent of port speed. The level units can be set to percent or packets-per-second.
Multicast Storm Recovery Mode	Enable or disable this option by selecting one of the following options on the pulldown entry field: • **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 factory default is 5 percent of port speed. The level units can be set to percent or packets-per-second.
Unicast Storm Recovery Mode	Enable or disable this option by selecting one of the following options on the pulldown entry field: • **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.

Field	Description
Unicast Storm Recovery Level	Specify the data rate at which storm control activates. The factory default is 5 percent of port speed. The level units can be set to percent or packets-per-second.
LACP Mode	Selects the Link Aggregation Control Protocol administration state: • **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 **Interface** or **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: • **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 FASTPATH® 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 FASTPATH® 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: • **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 **Interface** field is set to **All**, this field is blank.

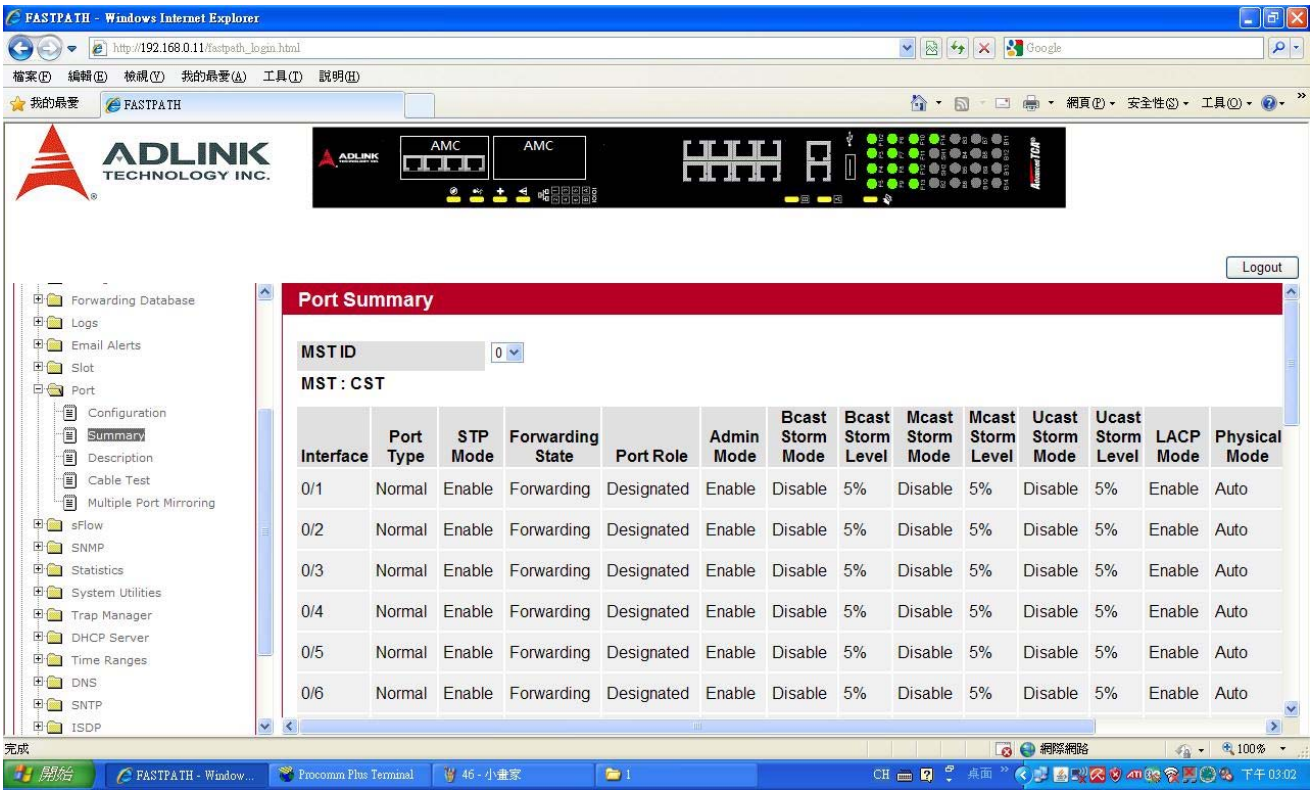
If you make any changes to the page, click **Submit** to apply the changes to the system.

Summary

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

To access the Port Summary page, click **System > Port > Summary** 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 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.



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.
Interface	Identifies the port that the information in the rest of the row is associated with. The field is **Slot/Port** for non-stacking platforms.
Port Type	For most ports this field is blank. Otherwise, the possible values are: • **Mirrored**: Indicates that the port has been configured as a monitoring port and is the source port in a port mirroring session. For more information about port monitoring and probe ports, see “Multiple Port Mirroring” .

Field	Description
	• **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” . • **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” .
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” .
Forwarding State	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: • Disabled • Blocking • Listening • Learning • Forwarding • Broken
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.
Admin Mode	Shows the port control administration state, which can be one of the following: • **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	Shows whether the Broadcast Storm Recovery Mode, which can be one of the following: • **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

Field	Description
	speed.
Mcast Storm Mode	Shows the Multicast Storm Recovery Mode, which is one of the following: • **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	Shows the Unicast Storm Recovery Mode, which can be one of the following: • **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.
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: • **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: • **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 FASTPATH® 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

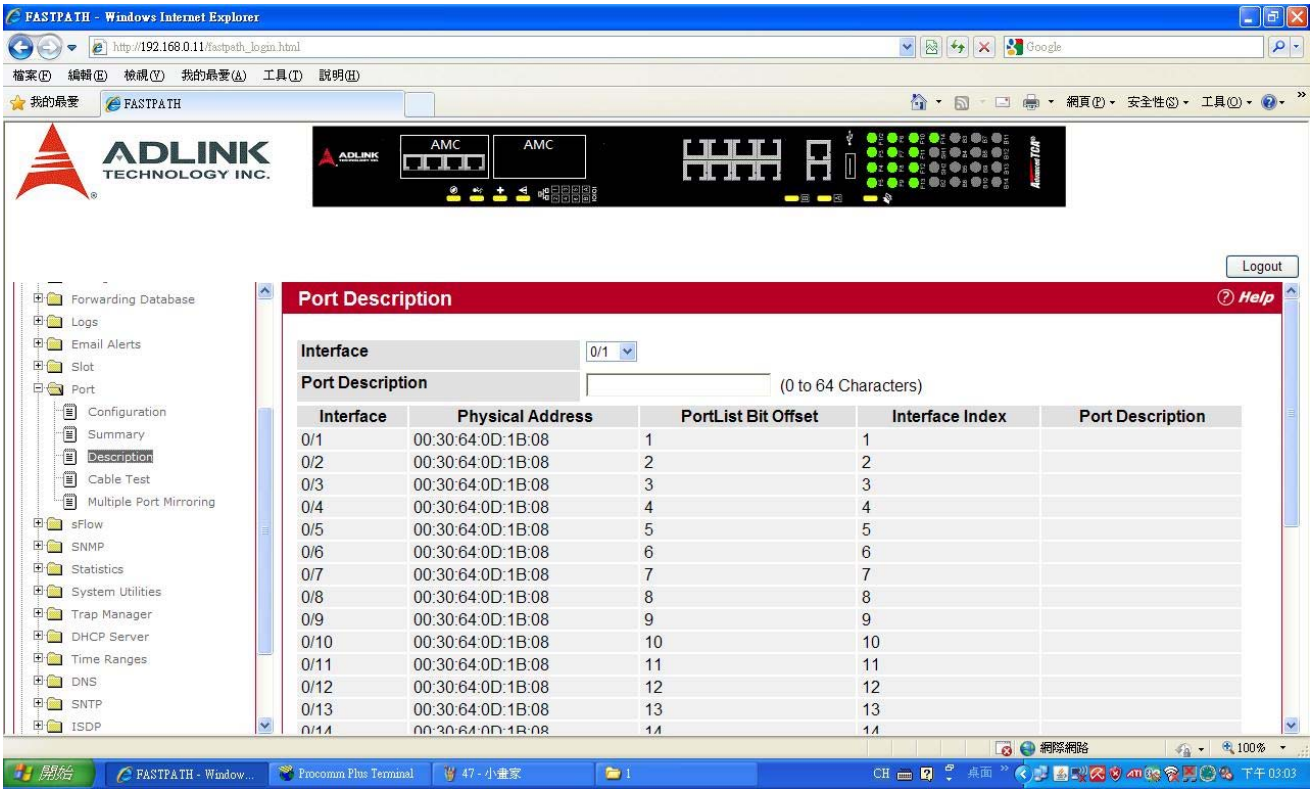
Field	Description
	depend on the platform on which the FASTPATH® software is running and which port you select. In half-duplex mode, the transmissions are two-way. In other words, the port can send and receive traffic at the same time.
Physical Status	Indicates the port speed and duplex mode at which 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. • **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 redisplay 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 **System > Port > Port Description** in the navigation tree.



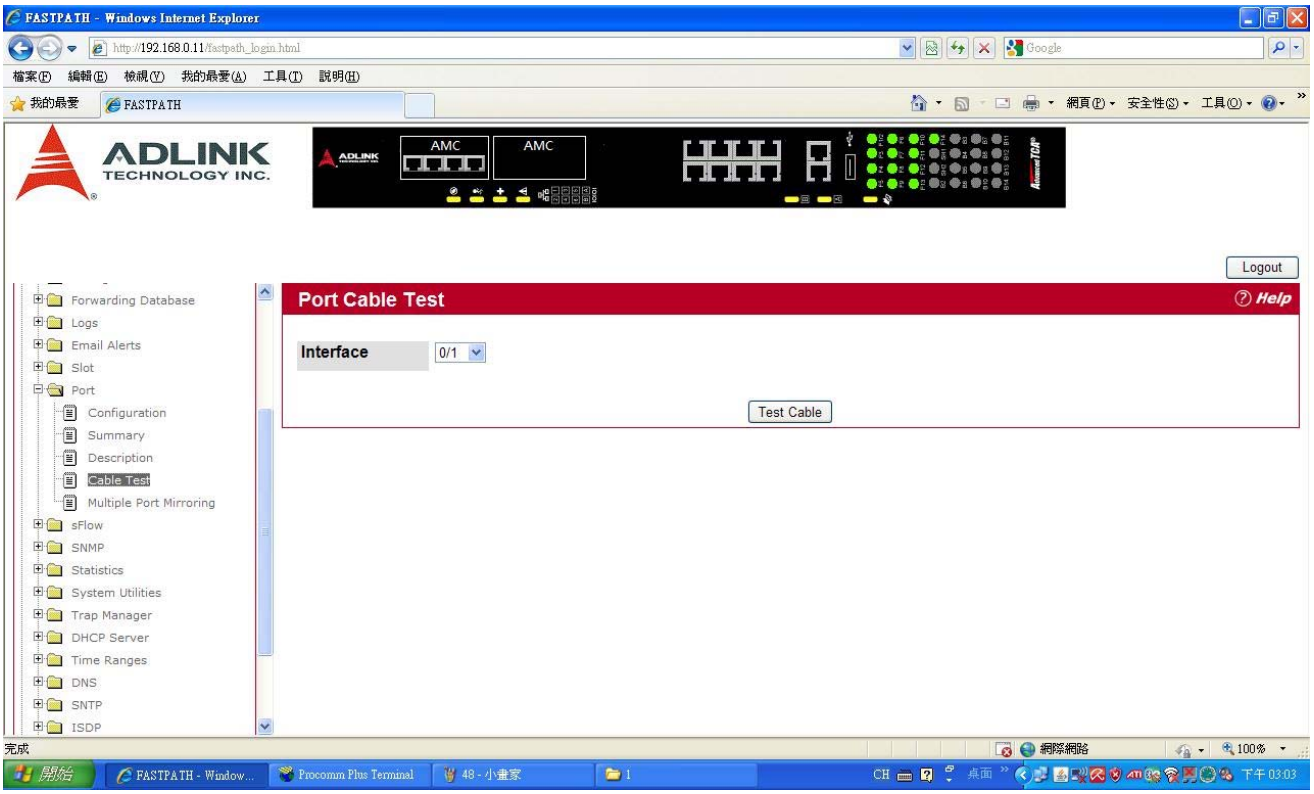
Field	Description
Interface	Select the interface for which data is to be displayed or configured. For non-stacking systems, the field is **Slot/Port**.
Port Description	Enter text to describe a port. It can be up to 64 characters in length. The description can contain spaces and non-alphanumeric characters.
Interface	Identifies the port. For non-stacking systems, the field is **Slot/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 redisplay the page with the latest information from the router.

Cable Test

The cable test feature enables you to determine the cable connection status on a selected port. You can also obtain an estimate of the length of the cable connected to the port, if the PHY on the ports supports this functionality.

To access the Cable Test feature, click **System > Port > Cable Test**.



Field	Description
Interface	This field indicates the interface to which the cable to be tested is connected.
Interface	Displays the interface tested in the Interface notation.
Cable Status	This displays the cable status as Normal, Open, or Short. • **Normal**: The cable is working correctly. • **Open**: The cable is disconnected or there is a faulty connector. • **Short**: There is an electrical short in the cable. • **Cable Test Failed**: The cable status could not be determined. The cable may in fact be working. This field is displayed after you click Test Cable and results are available.

Field	Description
Cable Length	Displays the estimated length of the cable in meters. The length is displayed as a range between the shortest estimated length and the longest estimated length. Unknown is displayed if the cable length could not be determined. This field is displayed only when the cable status is Normal.
Failure Location	The estimated distance in meters from the end of the cable to the failure location. The failure location is only displayed if the cable status is Open or Short.

Select a port and click **Test Cable** to display its status.

If the port has an active link while the cable test is run, the link can go down for the duration of the test. The test may take several seconds to run.

The command returns a cable length estimate if this feature is supported by the PHY for the current link speed. Note that if the link is down and a cable is attached to a 10/100 Ethernet adapter, then the cable status may display as Open or Short because some Ethernet adapters leave unused wire pairs unterminated or grounded.

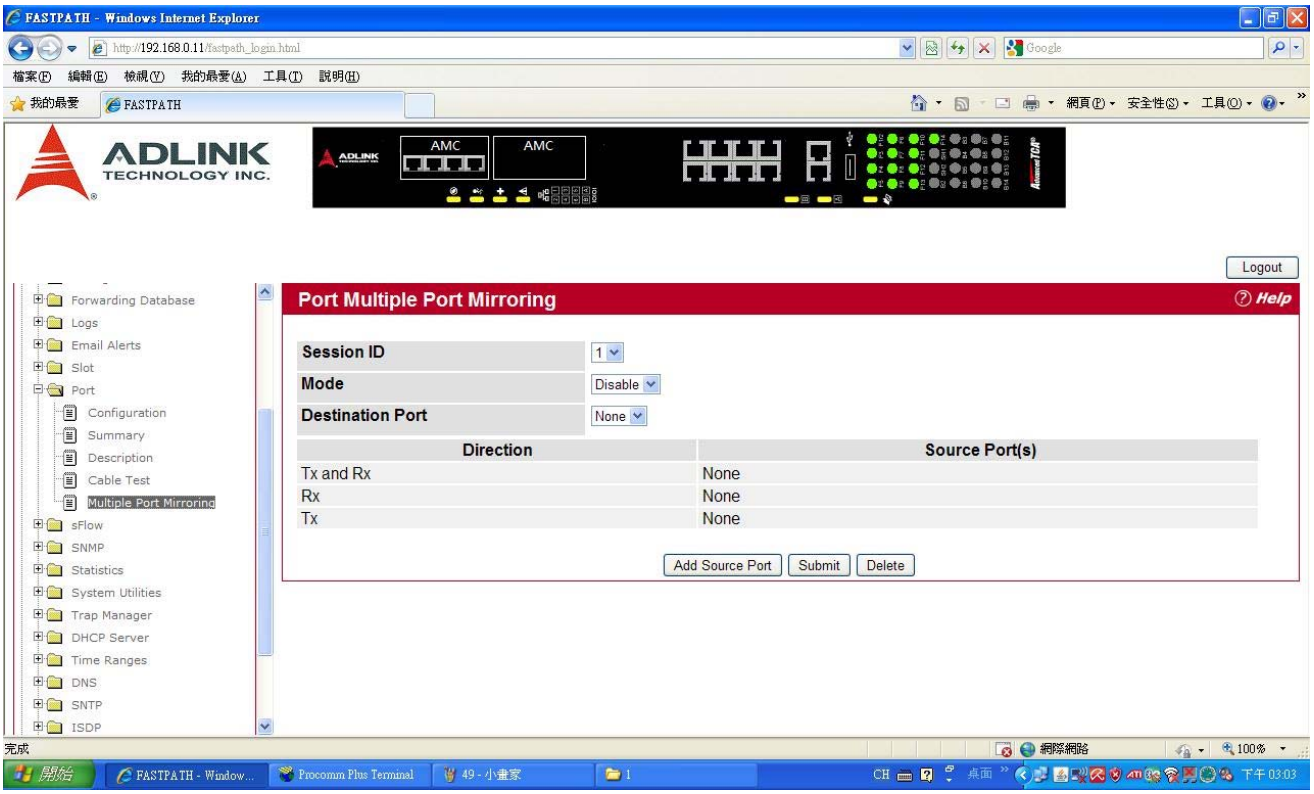
Multiple Port Mirroring

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 **System > Port > Multiple Port Mirroring** in the navigation menu.



Field	Description
Session	Specifies the monitoring session.
Mode	Enables you to turn on of off Multiple Port Mirroring. The default is Disabled (off).
Destination Port	Select the port to which port traffic may be copied.

Field	Description
Direction	Specifies the direction of traffic on source port(s) which will be sent to the probe port. Possible values are: • Tx and Rx: Both Ingress and Egress traffic. • Rx: Ingress traffic only. • Tx: Egress traffic only.

Adding a Port Mirroring Session

1. From the Port Mirroring page, click **Add** to display the **Add Source Ports** page.
2. Configure the following 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: • **Tx and Rx**: Monitors transmitted and received packets. • **Rx**: Monitors received packets only. • **Tx**: Monitors transmitted packets only.

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.

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.

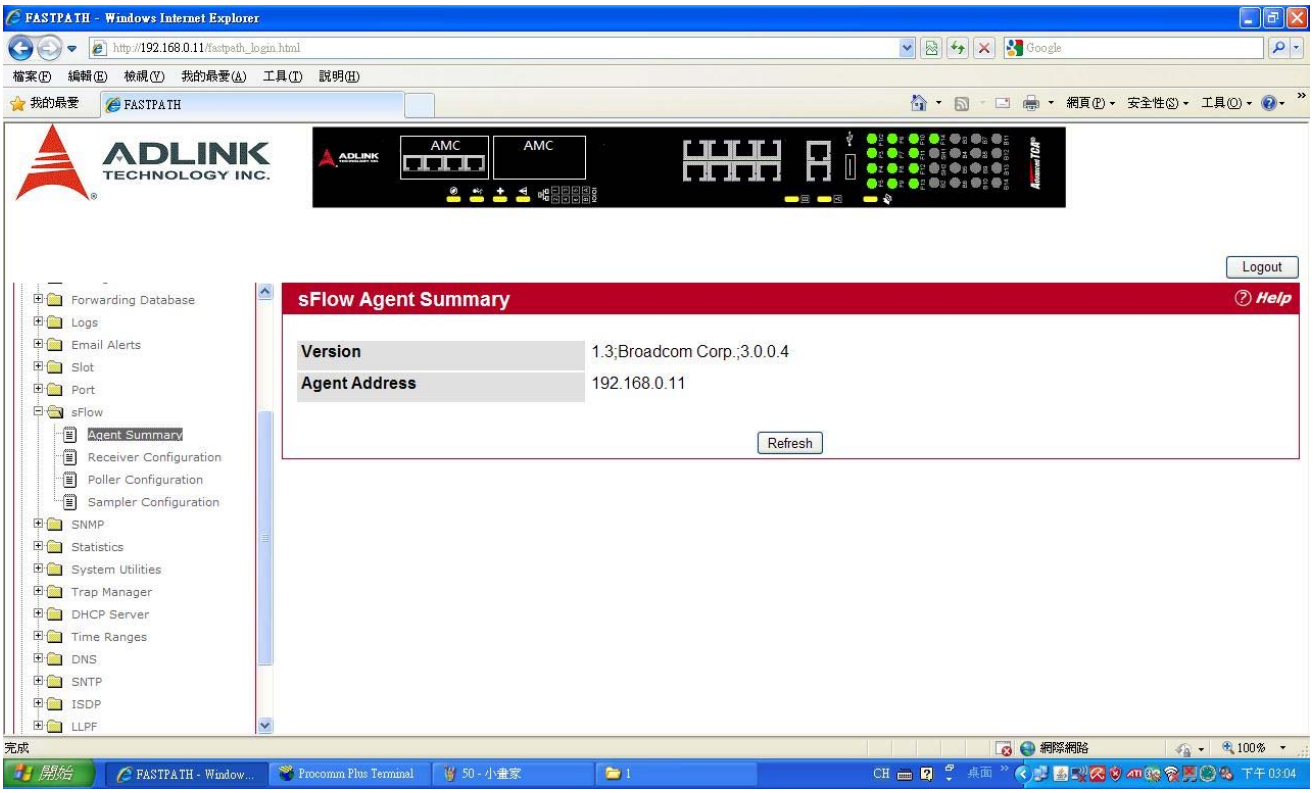
The sFlow Agent uses two forms of sampling: statistical packet-based sampling of switched or routed Packet Flows, and time-based sampling of counters.

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 **System > sFlow > Agent Summary** in the navigation tree.



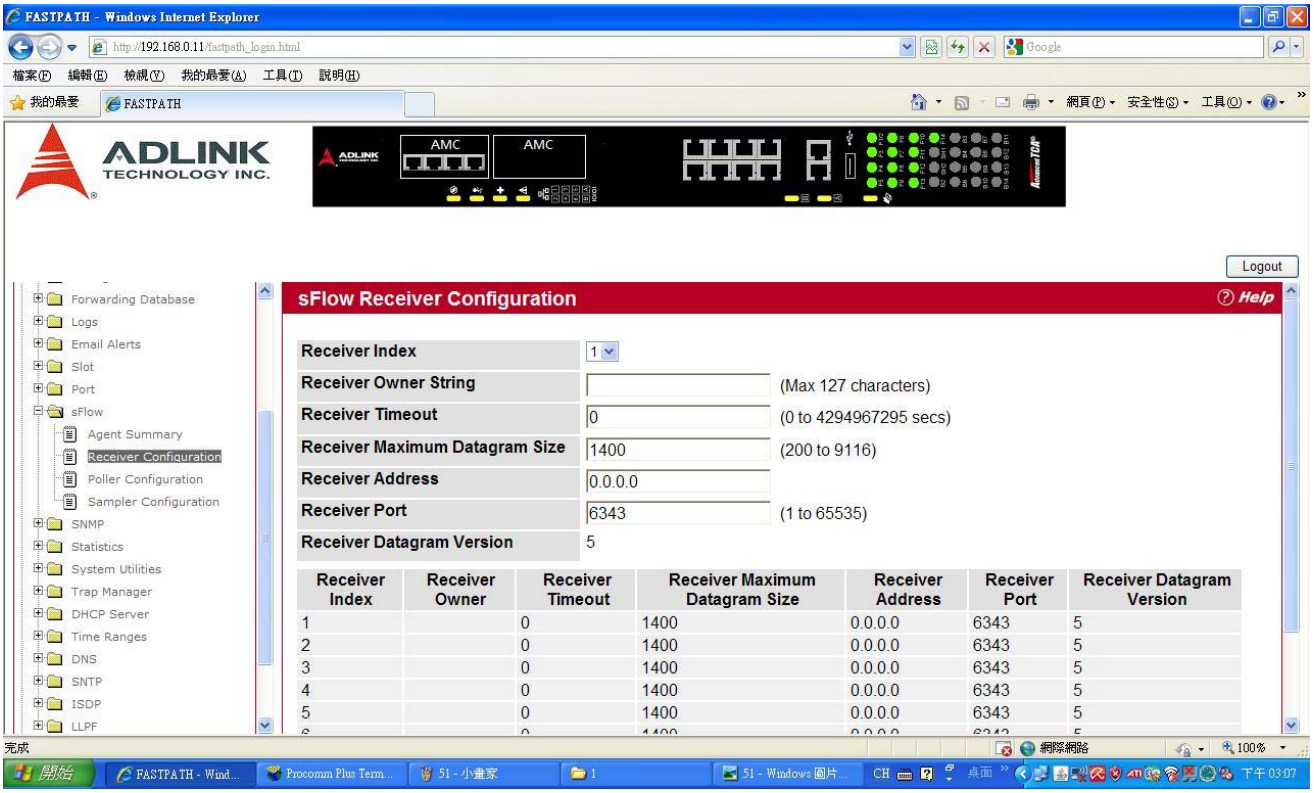
Field	Description
Version	Uniquely identifies the version and implementation of this MIB. The version string must have the following structure: MIB Version;Organization;Software Revision where: • MIB Version: '1.3', the version of this MIB. • Organization: Broadcom Corp. • Revision: 1.0
Agent Address	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 **System > sFlow > Receiver Configuration** in the navigation tree.



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.)

Field	Description
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.

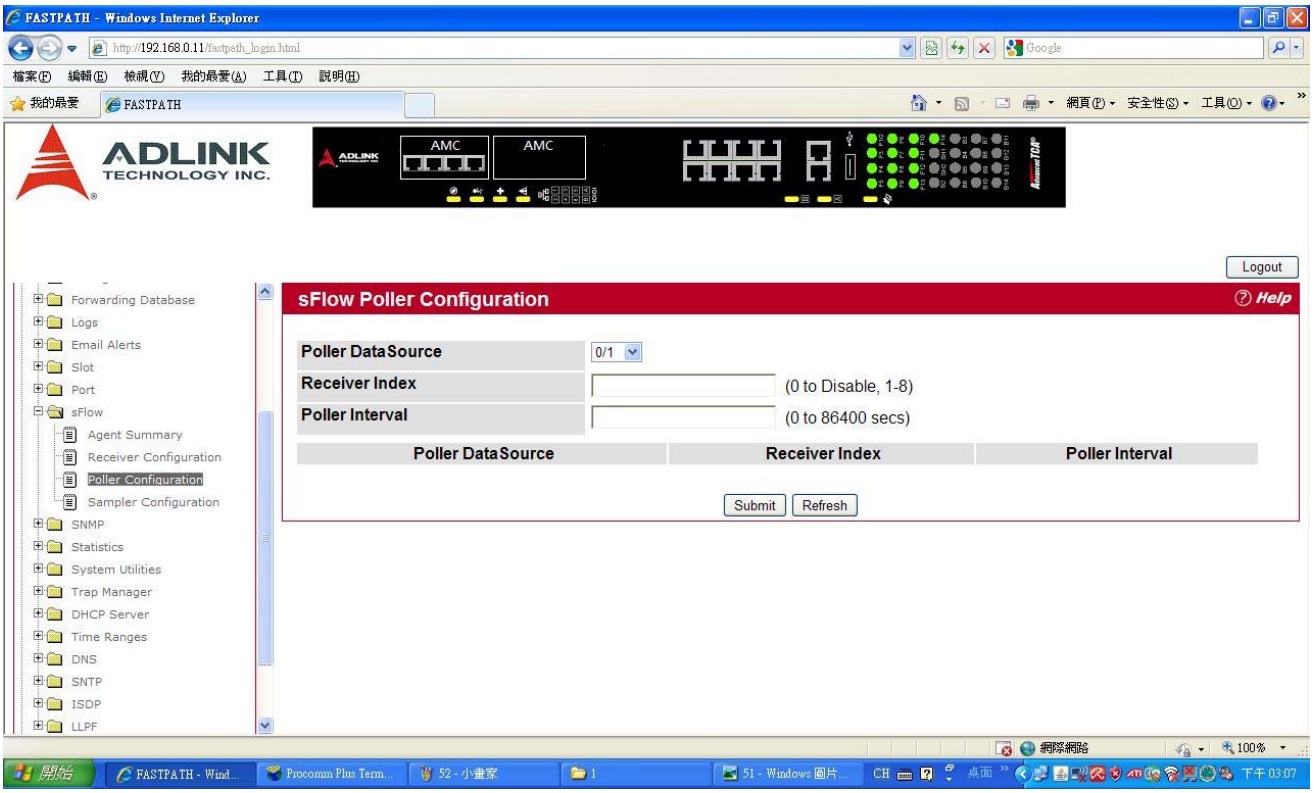
Counter Sampling

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 **System > sFlow > Poller Configuration** in the navigation tree.



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.

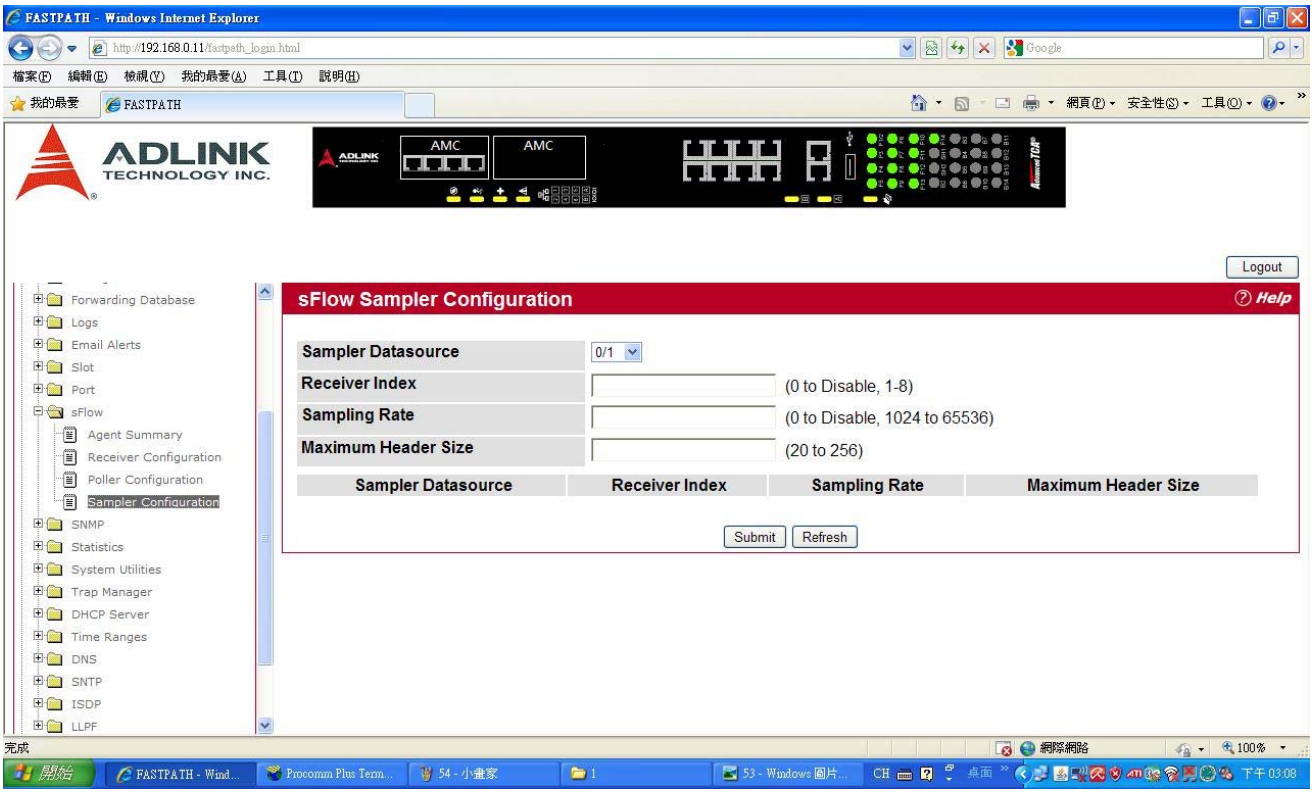
Packet Flow Sampling

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 **System > sFlow > Sampler Configuration** in the navigation tree.



Field	Description
Poller 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.

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 theMIB 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-Bock-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).

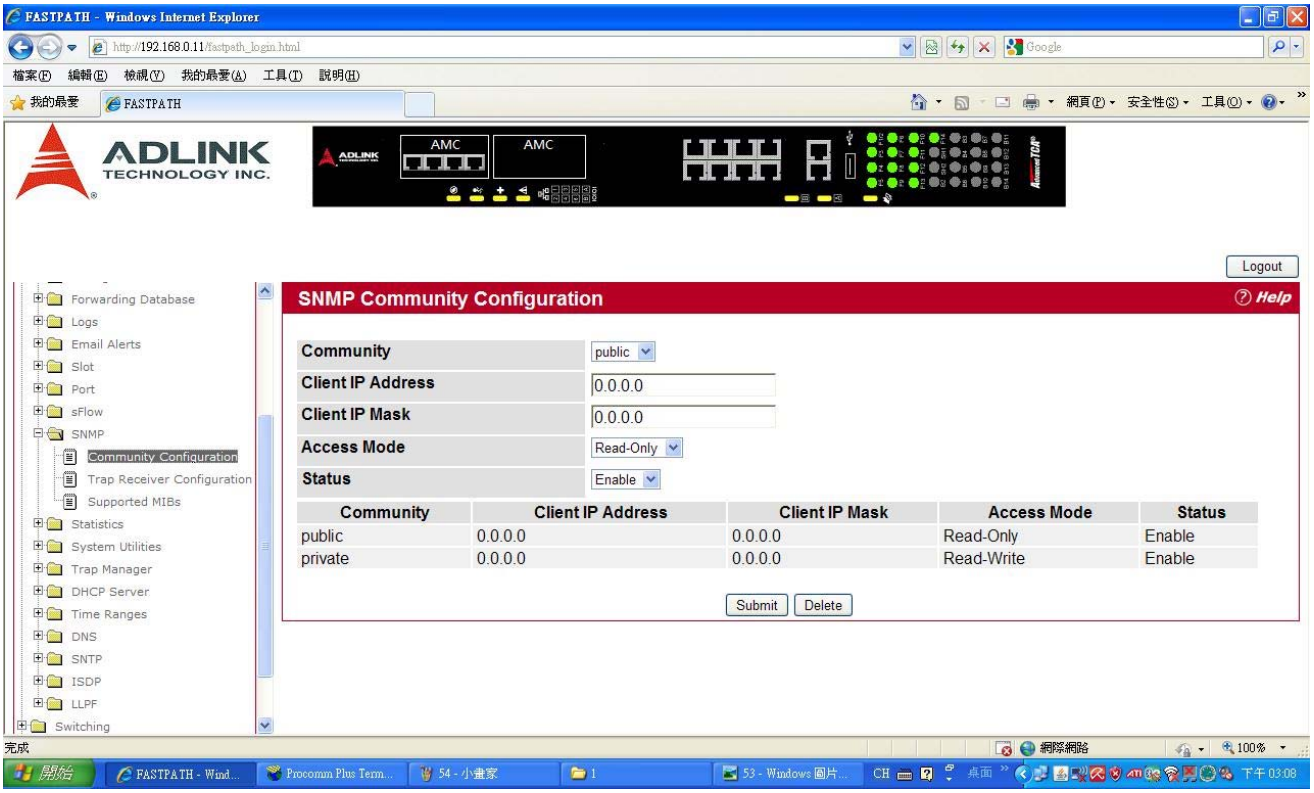
Use the SNMP page to define SNMP parameters. To display the SNMP page, click **System > SNMP** in the navigation tree.

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 **System > SNMP > Community Configuration** in the navigation tree.



Field	Description
Community	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: • **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.
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.

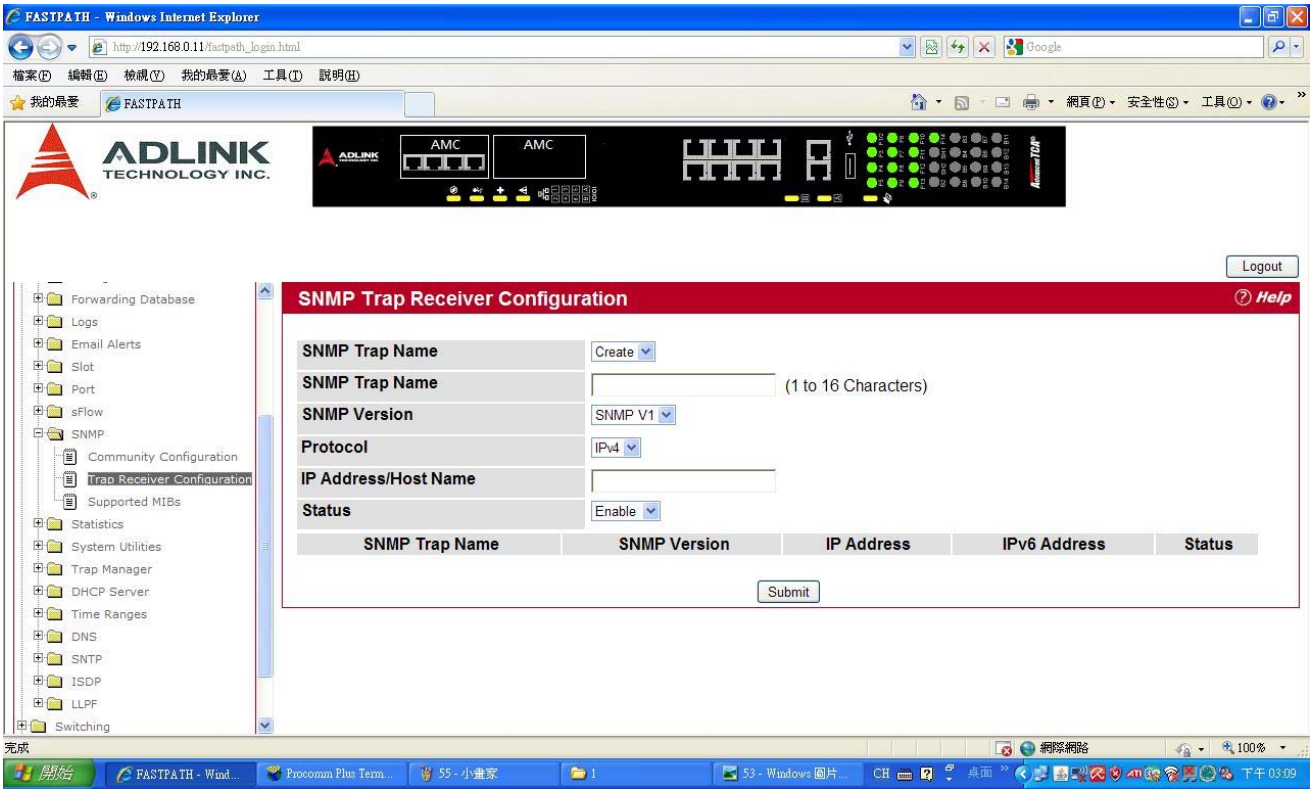
Field	Description
Client IP Address	Taken together, the **Client IP Address** and **Client IP Mask** denote a range of IP addresses from which SNMP clients may use that community to access this device. If either (IP Address or IP Mask) value is 0.0.0.0, access is allowed from any IP address. Otherwise, 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.
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: • **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: • **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 **System > SNMP > Trap Receiver Configuration** from the navigation tree.



Field	Description
(Create) SNMP Community Name	When this field is set to **Create**, you can configure new SNMP trap receiver information in the rest of the fields. If you have already configured an SNMP trap receiver, you can select it from the drop-down menu to change the settings or delete it.
SNMP Community Name	Enter the community string 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: • **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: • **IPv4**. Choose IPv4 to enter the address in IPv4 format. • **IPv6**. Choose IPv6 to enter the address in IPv6 format.

Field	Description
IP Address	Enter the IP address in dotted-decimal format to receive SNMP traps from this device.
Status	Select the receiver's status from the pulldown menu: • **Enable**: Send traps to the receiver • **Disable**: Do not send traps to the receiver.

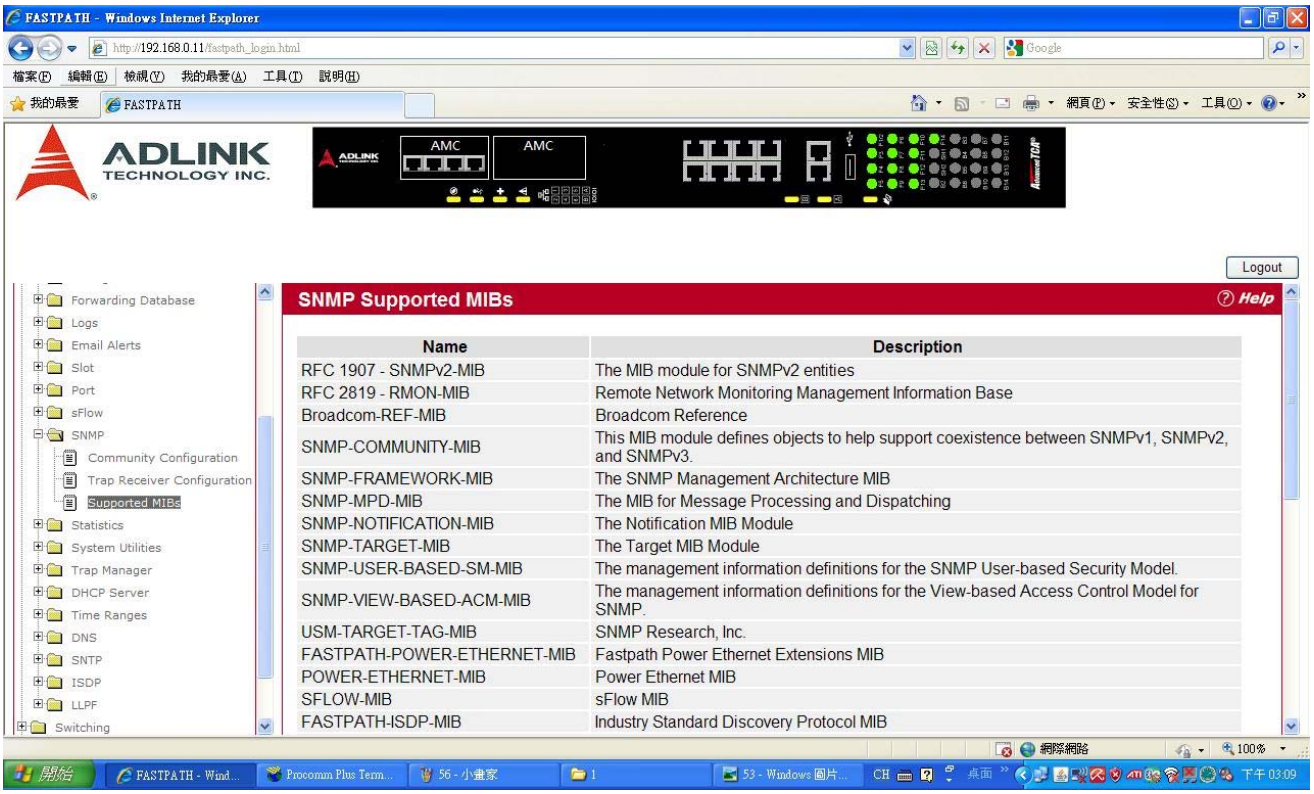
If you make any changes to the page, click **Submit** to apply the changes to the system. If you want the switch to retain the new values across a power cycle, you must perform a **save**.

Supported MIBS

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

To access the Supported MIBs page, click **System > SNMP > Supported MIBs** in the navigation menu.

.



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

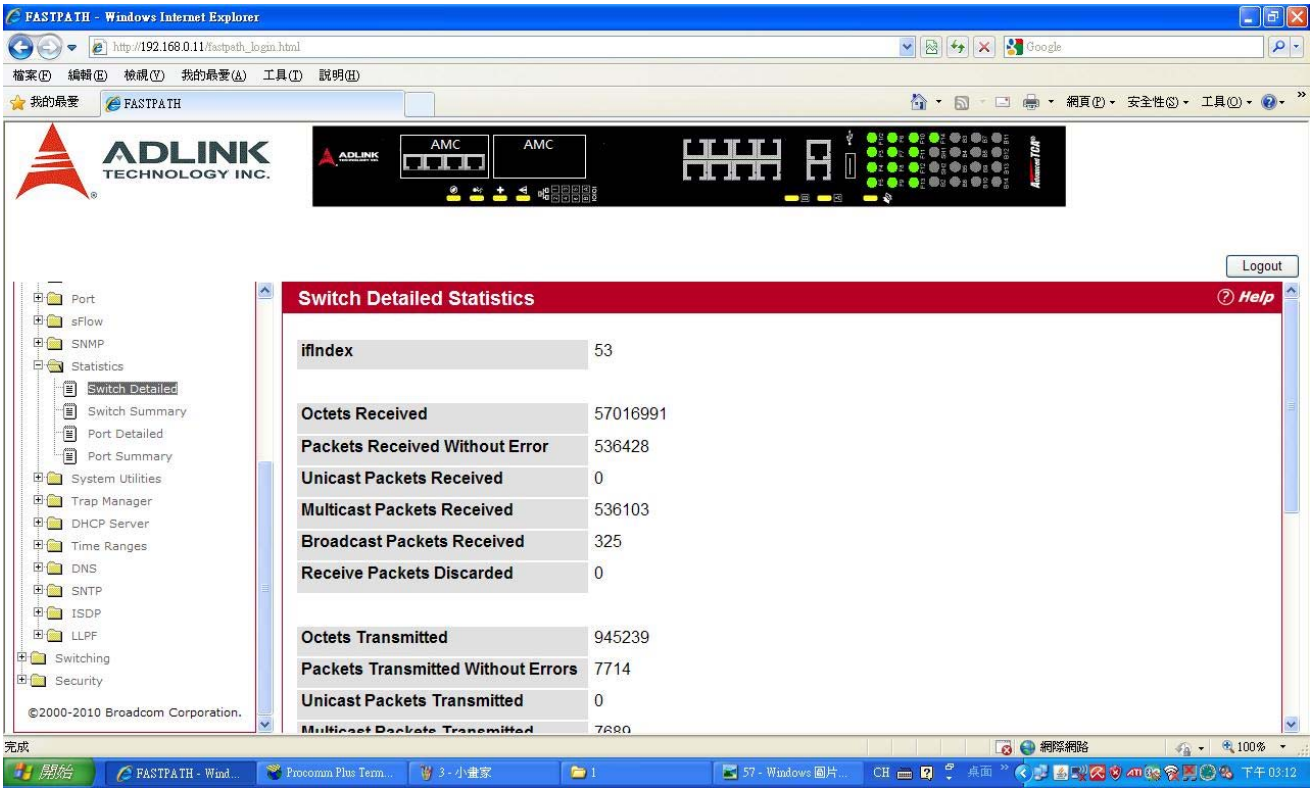
Viewing System Statistics

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 **System > Statistics > Switch Detailed** in the navigation menu.



Field	Description
fIndex	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.

Field	Description
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.
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.

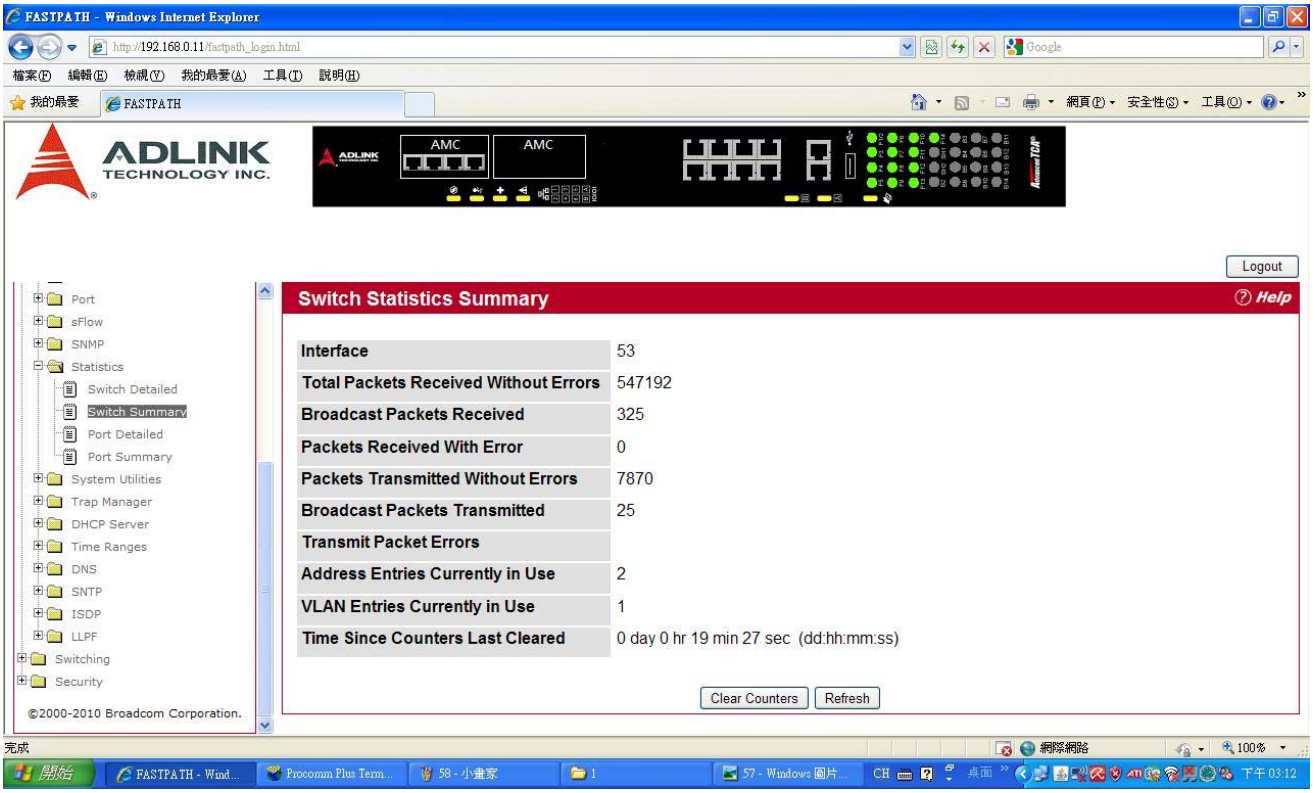
Click **Refresh** to refresh the data on the screen with the present state of the data in the switch.

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 **System > Statistics > Switch Summary** in the navigation tree.



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.
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.

Field	Description
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.

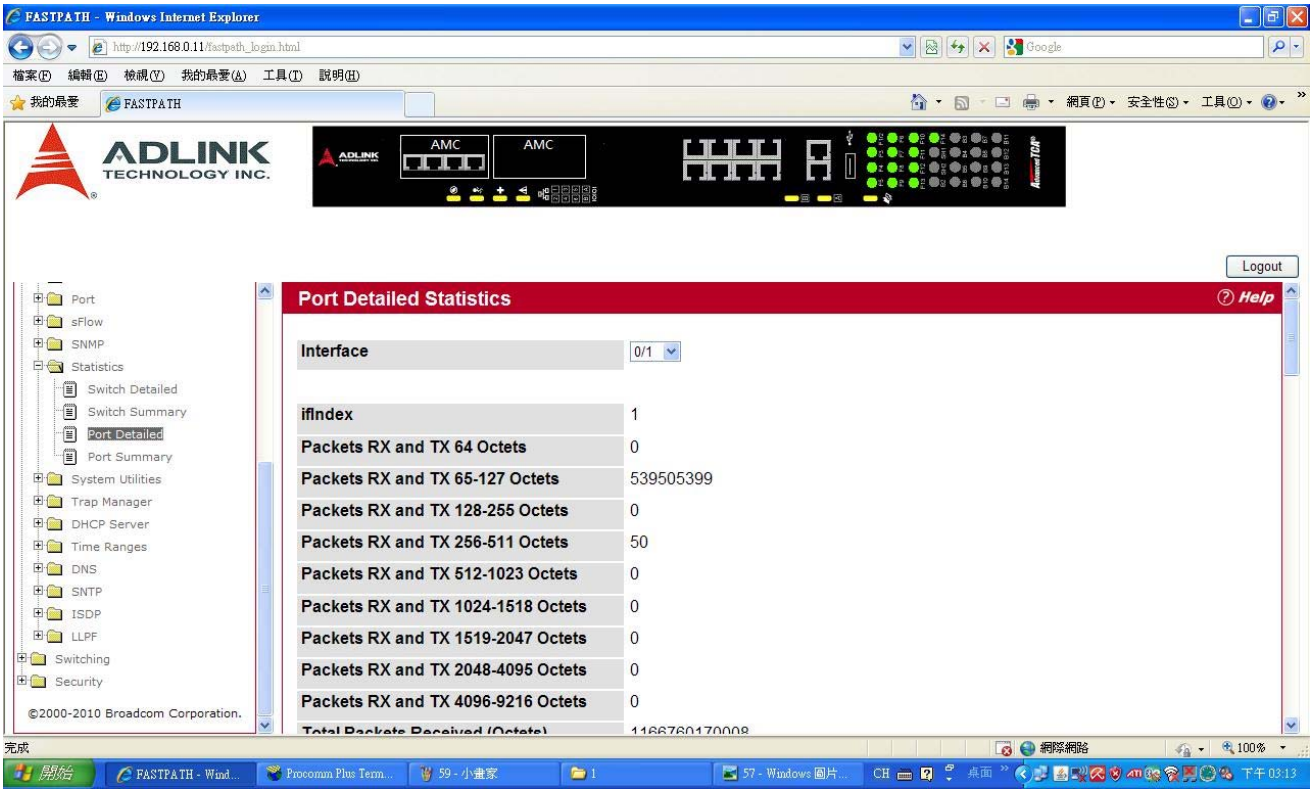
Click **Clear Counters** to clear all the statistics counters, resetting all summary and detailed statistics for this switch to default values. The discarded packets count cannot be cleared.

Click **Clear All Counters** to clear counters for all switches in the stack.

Port Detailed

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

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



Field	Description
Interface	Use the drop-down menu to select the interface for which data is to be displayed or configured. For non-stacking systems, this field is **Slot/Port**.
ifIndex	This field indicates the ifIndex of the interface table entry associated with this port on an adapter.
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).
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).

Field	Description
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).
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

Field	Description
	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.
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.
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 Received Packets Not Forwarded	A count of valid frames received which were discarded (i.e., filtered) by the forwarding process.

Field	Description
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.
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).

Field	Description
Packets Transmitted 1523-2047 Octets	The total number of packets (including bad packets) received that were between 1523 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 2048-4095 Octets	The total number of packets (including bad packets) received that were between 2048 and 4095 octets in length inclusive (excluding framing bits but including FCS octets).
Packets Transmitted 4096-9216 Octets	The total number of packets (including bad packets) received that were between 4096 and 9216 octets in length inclusive (excluding framing bits but including FCS octets).
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.
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.
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.
Total Transmit Packets Discarded	The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
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.

Field	Description
Excessive Collision Frames	A count of frames for which transmission on a particular interface fails due to excessive collisions.
Port Membership Discards	The number of frames discarded on egress for this port due to egress filtering being enabled.
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.

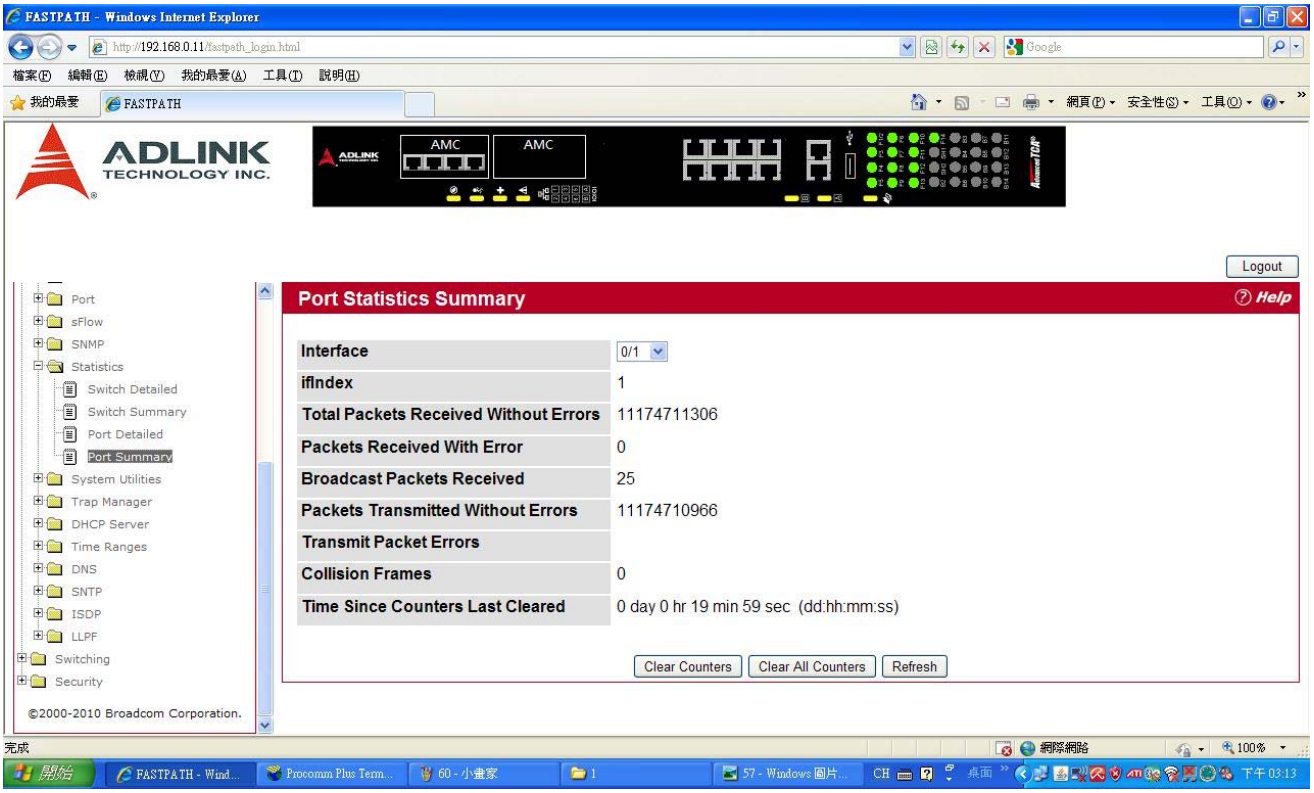
Click **Clear Counters** to clear all the counters. This resets all statistics for this port to the default values. Click **Clear All Counters** to clear all the counters for all ports on the switch. The button resets all statistics for all ports to default values.

Click **Refresh** to refresh the data on the screen and display the most current statistics.

Port Summary

The Port Summary page shows a summary of per-port traffic statistics on the switch.

To access the Port Summary page, click **System > Statistics > Port Summary** in the navigation tree.



Field	Description
Interface	Use the drop-down menu to select the interface for which data is to be displayed or configured. For non-stacking systems, this field is **Slot/Port**.
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.

Field	Description
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.

5.5. Using System Utilities

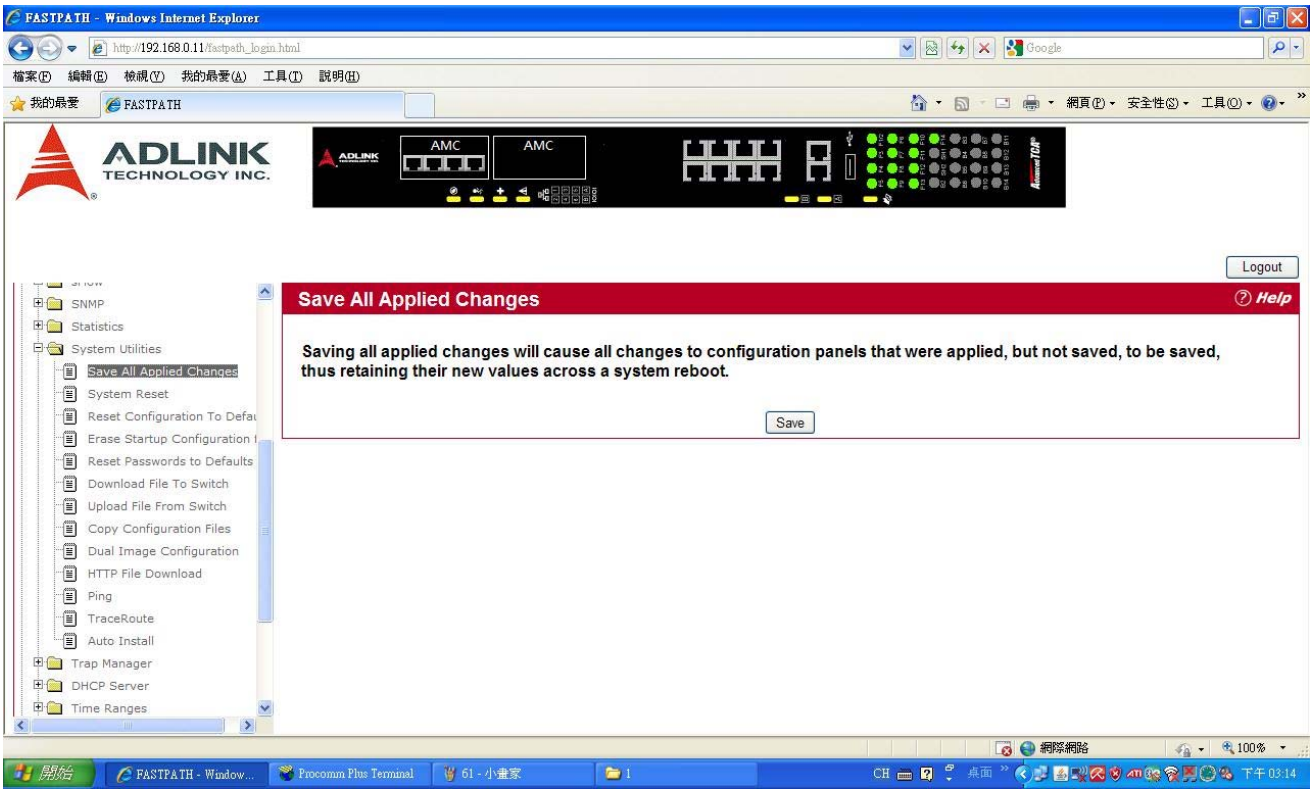
The System Utilities folder contains links to the following Web pages that help you manage the switch:

- Save All Applied Changes
- System Reset
- Reset Configuration to Defaults
- Erase Startup Config File
- Reset Passwords to Defaults
- Download File To Switch (TFTP)
- Upload File From Switch (TFTP)
- Dual Image Configuration
- HTTP File Download
- Ping
- TraceRoute
- Ping
- AutoInstall

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 **System > System Utilities > Save All Applied Changes** in the navigation tree.

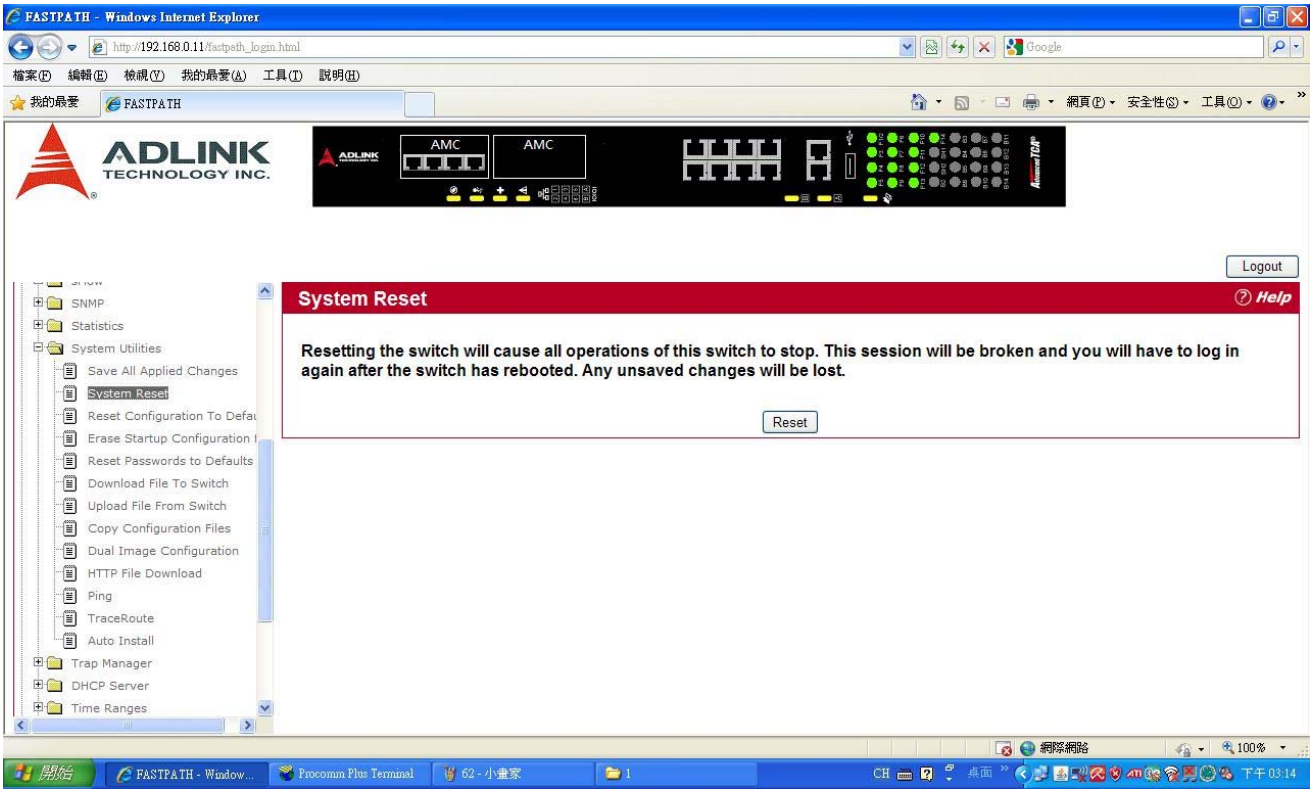


Click **Save** to save all changes applied to the system to NVRAM so that they are retained if the system reboots.

System Reset

Use the System Reset page to reboot the system. If the platform supports stacking, you can reset any of the switches in the stack, or all switches in the stack from this page.

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



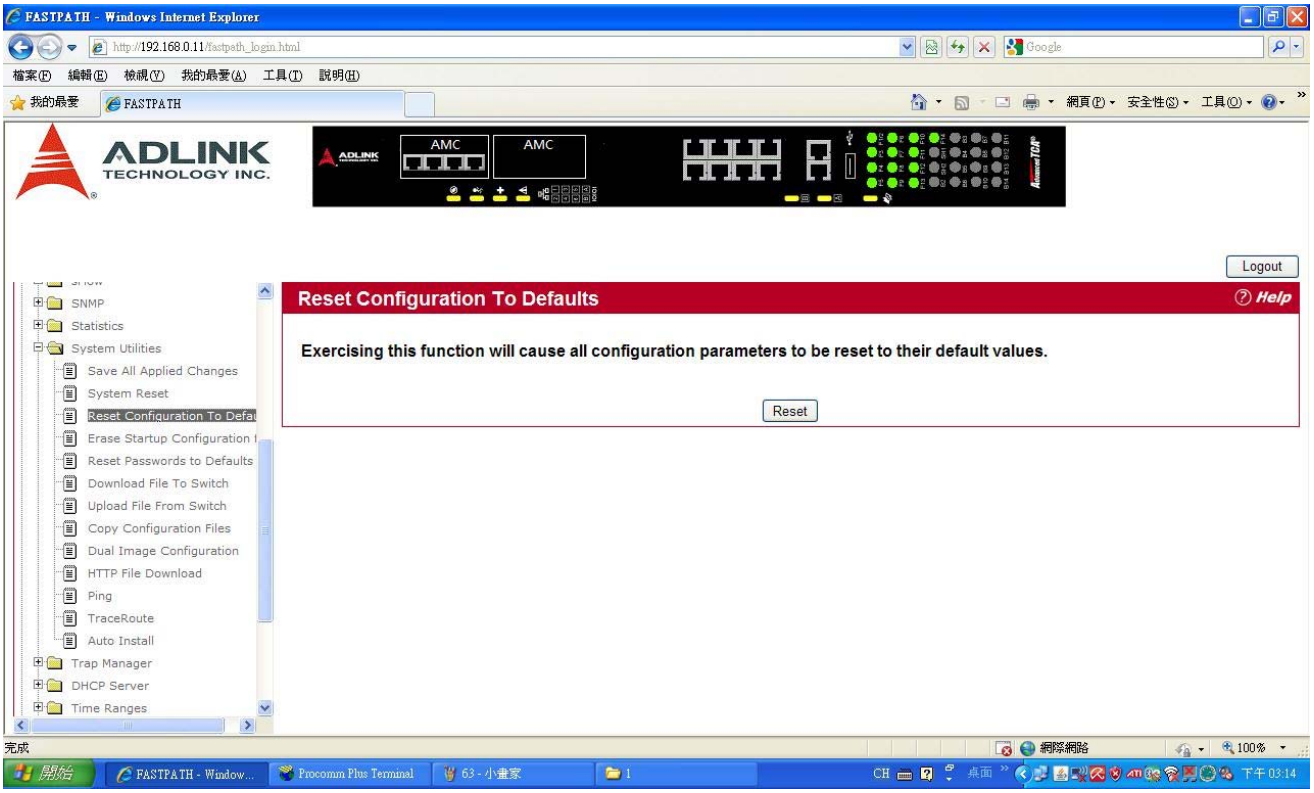
For Stacking platforms, you can select one or all switches in the stack to reset from the drop-down menu. For platforms that do not support stacking, this field is not present.

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.

Reset Configuration To Defaults

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

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

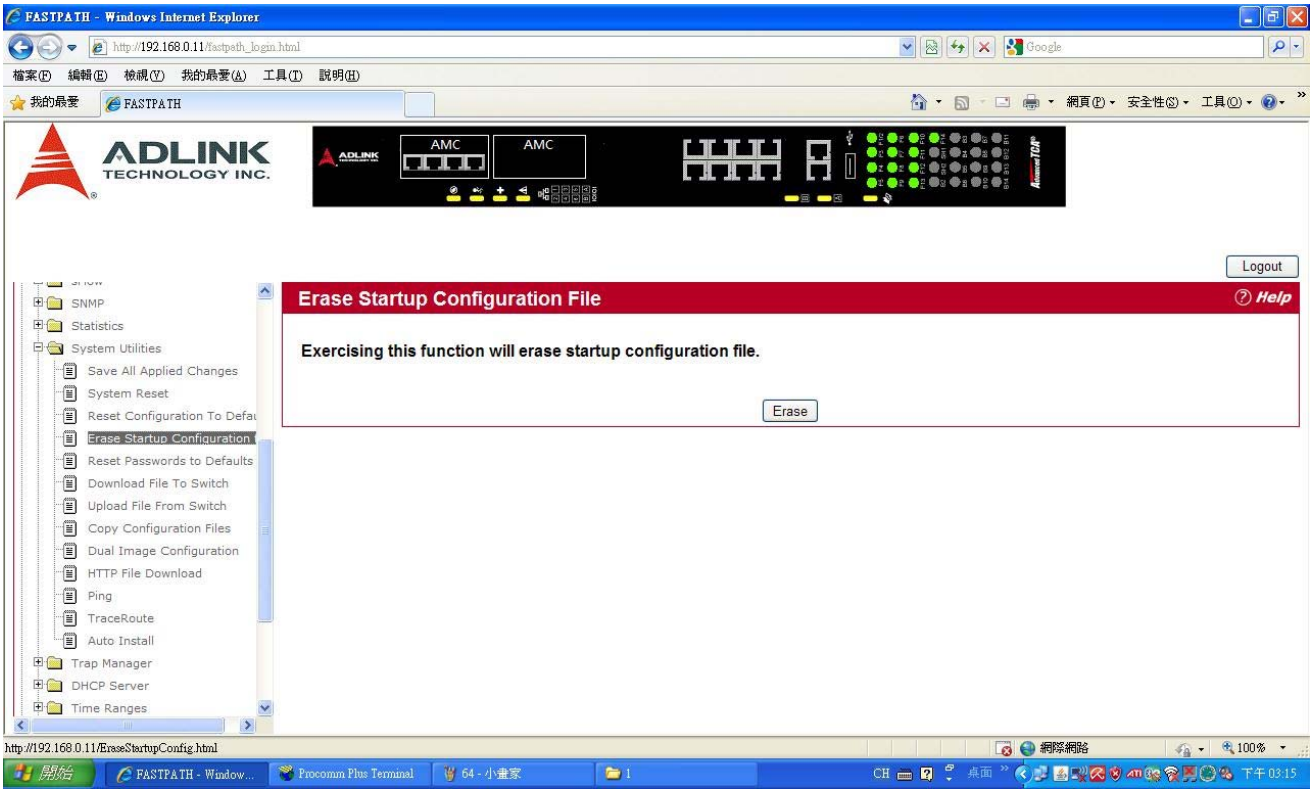


Click **Reset** to restore the factory default settings. The screen refreshes and asks you to confirm the reset. Click **Reset** again to complete the action.

Erase Startup Config File

Use the Erase Startup Config File page to erase the text-based configuration file stored in non-volatile memory. A confirmation screen displays after you select the **Erase** button.

To access the Erase Startup Config File page, click **System > System Utilities > Erase Startup Config File** in the navigation tree.

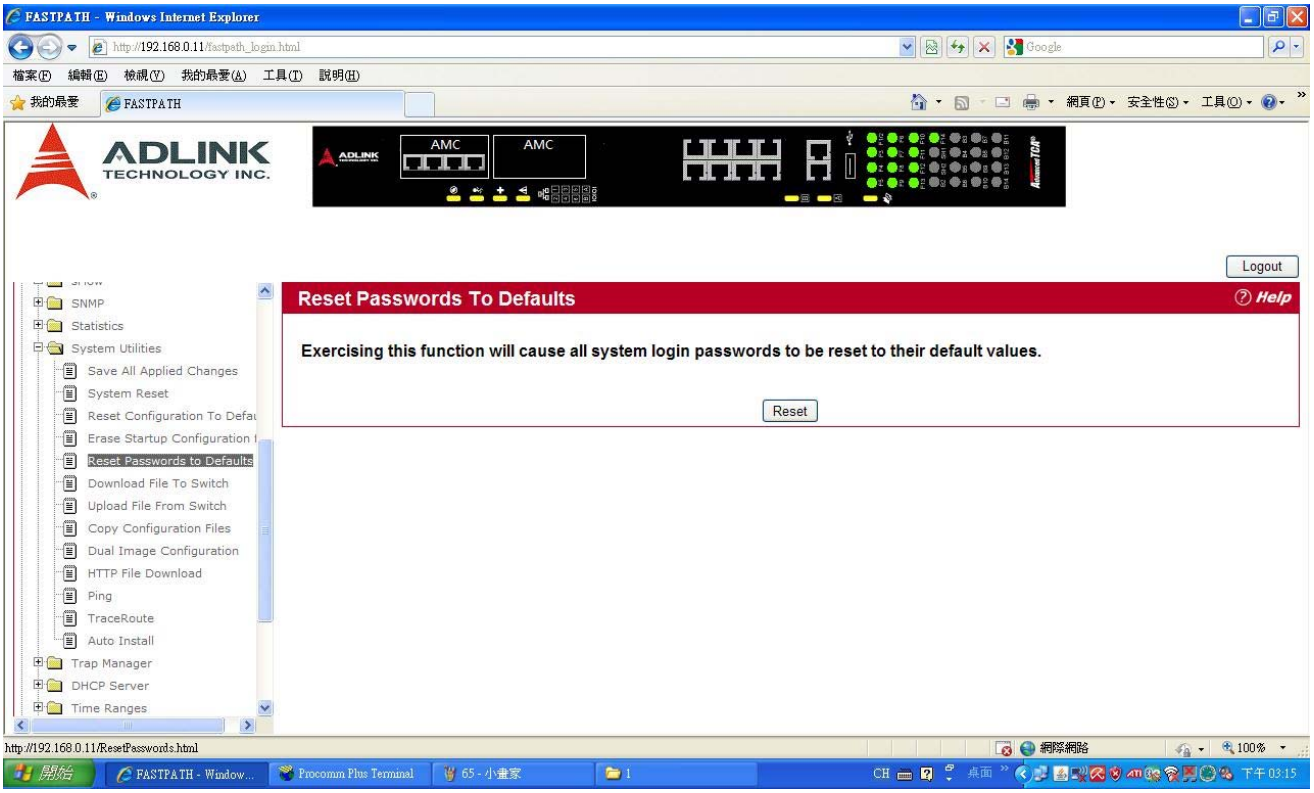


Click **Erase** to initiate the process.

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 **System > System Utilities > Reset Passwords to Defaults** in the navigation tree.



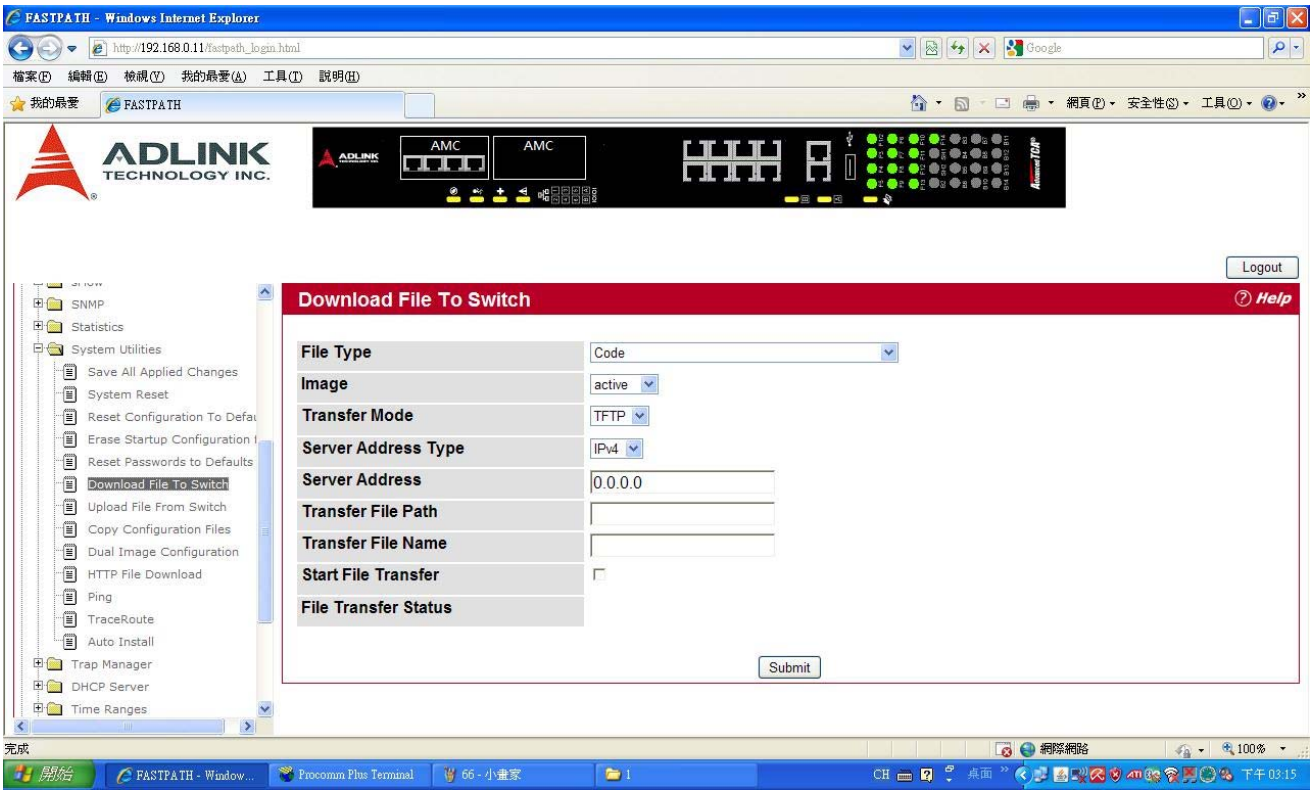
Click **Reset** to restore the passwords for the default users to the factory defaults.

Download File To Switch (TFTP)

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

You can also download files via HTTP. See “HTTP File Download” for more information.

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



Field	Description
File Type	Specify what type of file you want to download to the switch: • **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 designated files in the file system 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 FASTPATH® configuration file (FASTPATH®.cfg) on a TFTP server, you can download it to the switch to overwrite the running and startup configuration files. Upon a successful file transfer, the settings in the

Field	Description
	configuration file you upload are applied to the switch, and the configuration persists across a system reset. If the file has errors, the update is stopped. The configuration file is not a text file and cannot be edited by using a text editor. • **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 FASTPATH® 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.
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 FASTPATH® 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.

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.

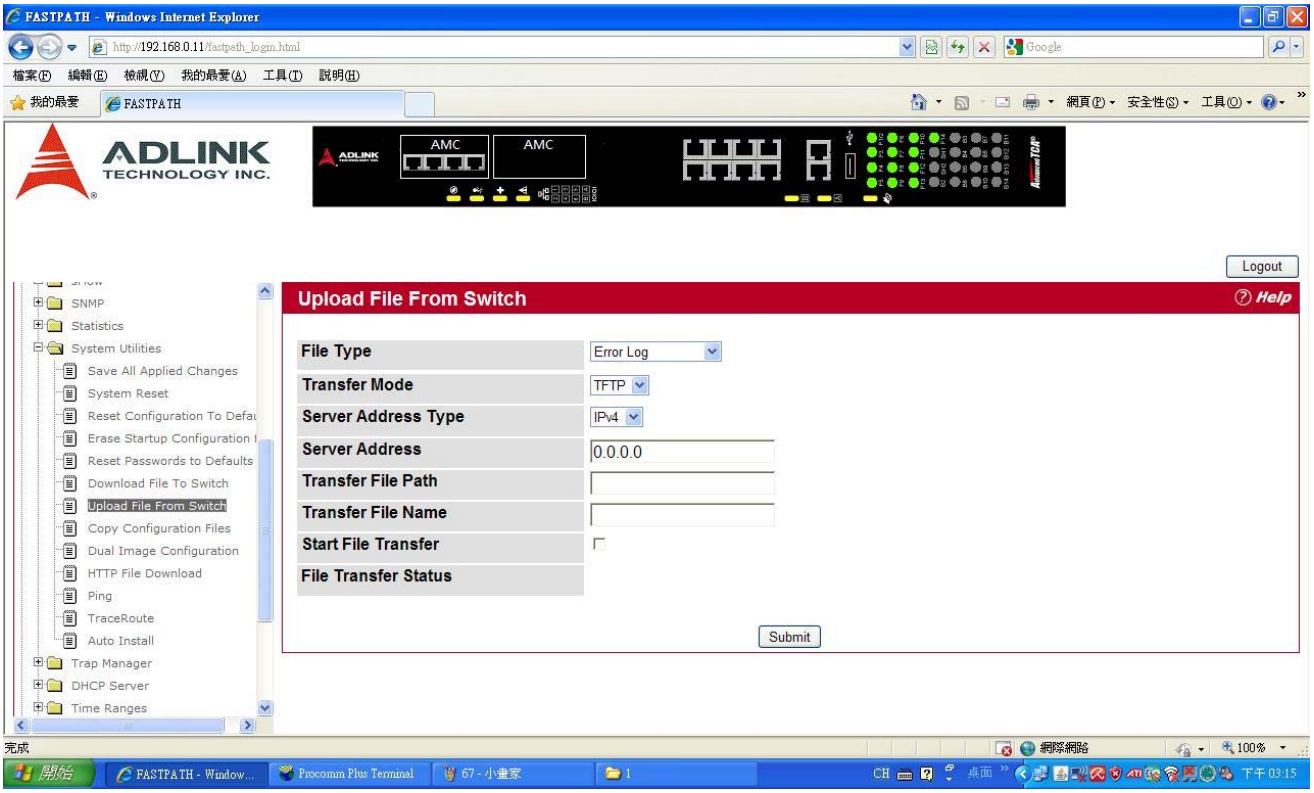
5. Click the Start File Transfer check box, and then click **Submit**. After you click **Submit**, the screen refreshes and a “File transfer operation started” message appears.

After the software is downloaded to the device, a message appears indicating that the file transfer operation completed successfully.

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 **System > System Utilities > Upload File from Switch** in the navigation tree.



Field	Description
File Type	Specify what type of file you want to upload: • **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.

Field	Description
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.
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 FASTPATH® 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 Transfe**r check box, and then click **Submit**.

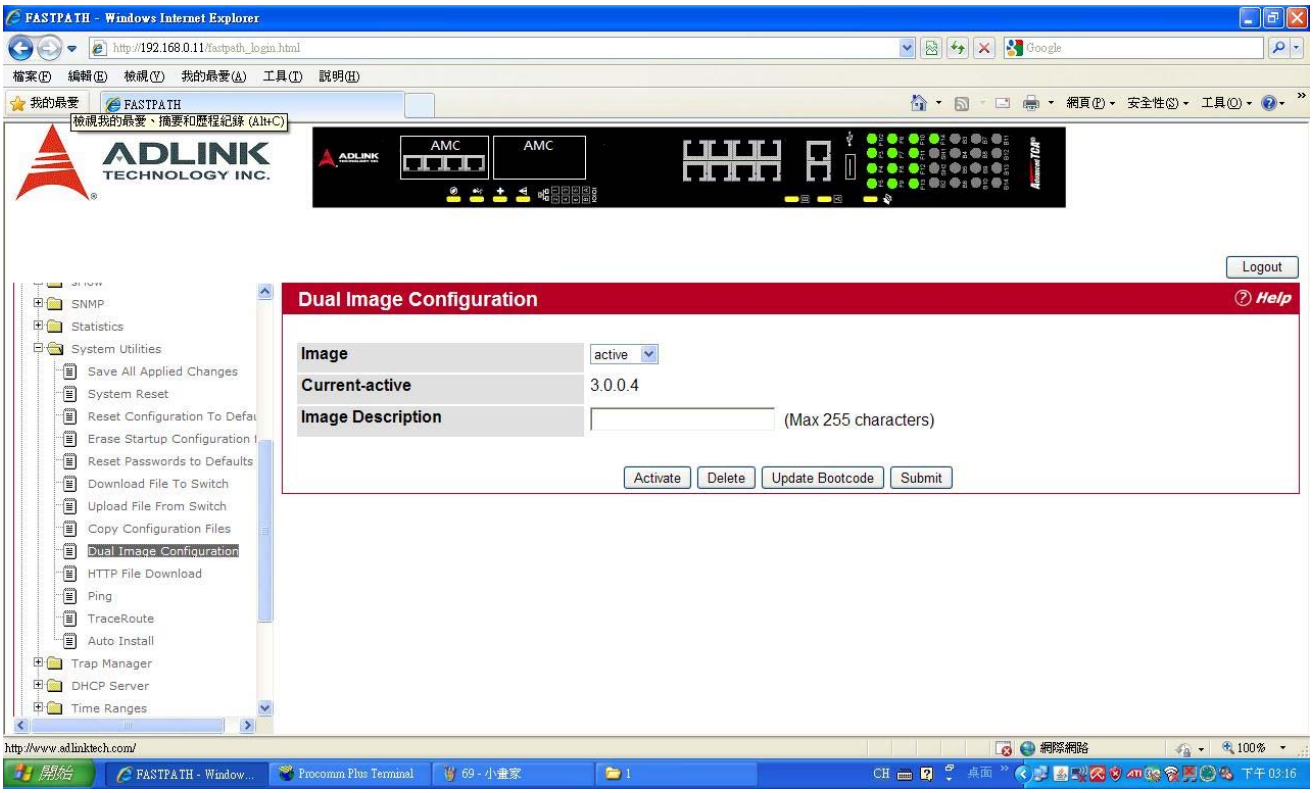
After you click **Submit**, the screen refreshes and a “File transfer operation started” message appears. After the software is downloaded to the device, a message appears indicating that the file transfer operation completed successfully.

Dual Image Configuration

The system maintains two versions of the FASTPATH® 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 FASTPATH® 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 Dual Image Configuration page to set the boot image.

To display the Dual Image Configuration page, click **System > System Utilities > Dual Image Configuration** in the navigation menu.



The Active Image page contains the following fields:

Field	Description
Image Name	Select image1 or image2 from the drop-down menu to display or configure information about that software image.
Current Active	Displays name of current active image.
Image Description	If desired, enter a descriptive name for the software image.

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

Click **Delete** to remove the selected image from permanent storage on the switch.You cannot delete the active image.

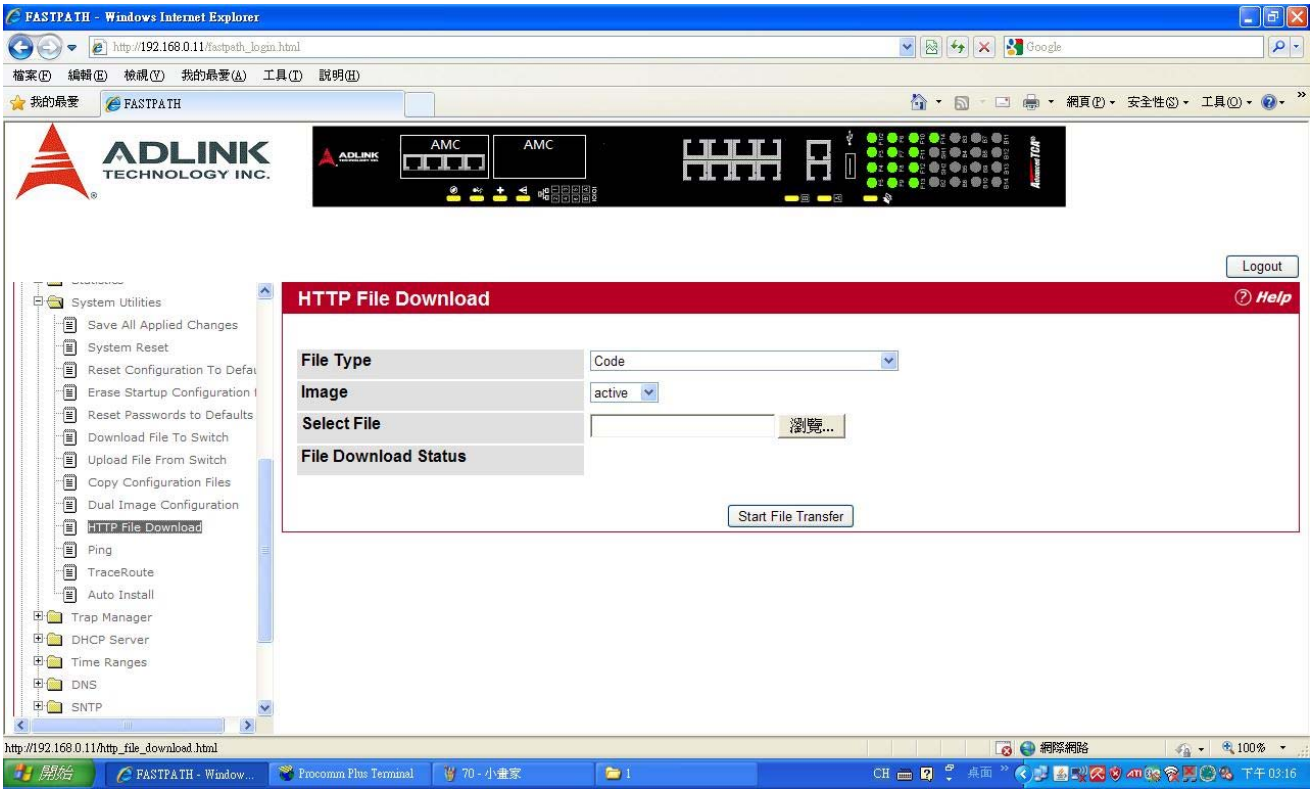
If the file you uploaded contains the boot loader code only, click **Update Bootcode**.

Click **Submit** to update the image description on the switch.

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 **System > System Utilities > HTTP File Download** in the navigation menu.



Field	Description
File Type	Specify the type of file you want to download: • **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)

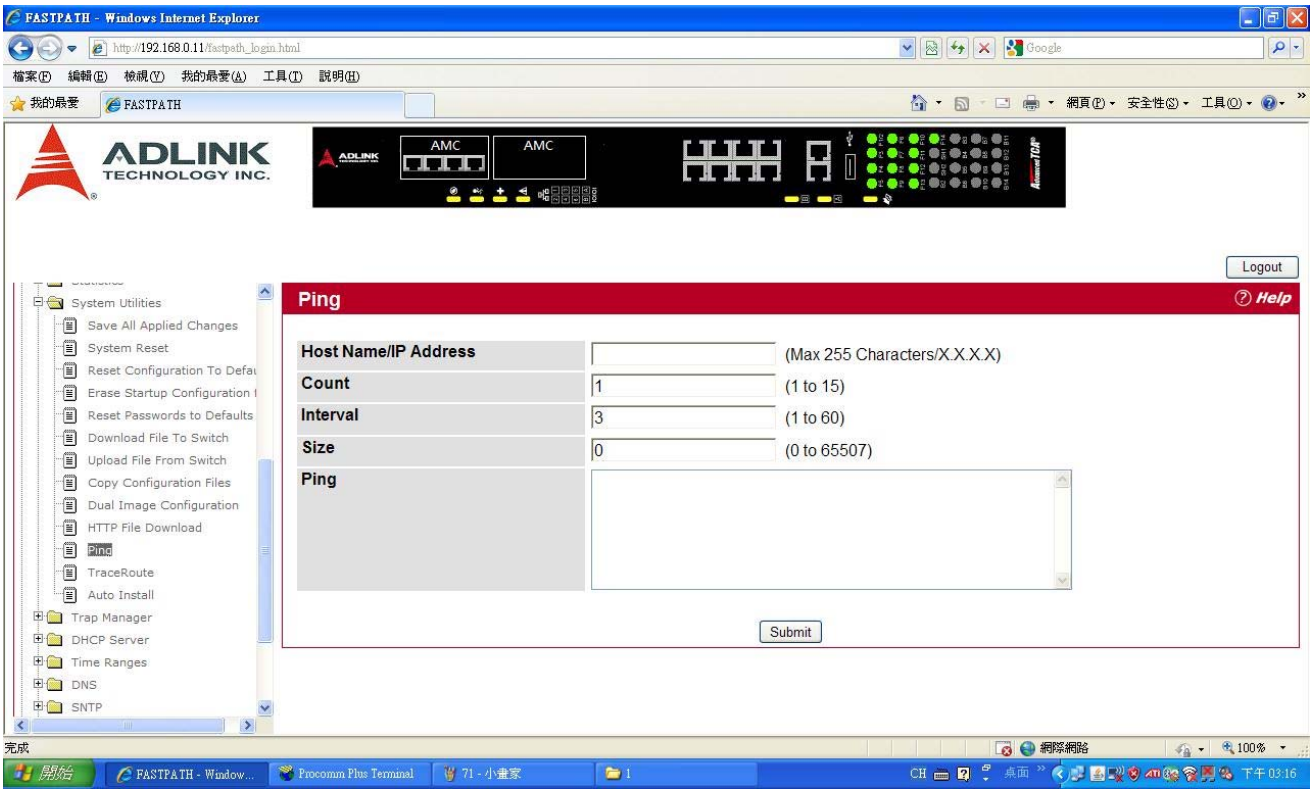
Field	Description
	• **SSL Server Certificate PEM File**: SSL Server Certificate File (PEM Encoded) • **SSL DH Weak Encryption Parameter PEM File**: SSL Diffie-Hellman Weak Encryption Parameter File (PEM Encoded) • **SSL DH Strong Encryption Parameter PEM File**: SSL Diffie-Hellman Strong Encryption Parameter File (PEM Encoded) • **CLI Banner**: Choose this option to download a banner file to be displayed before the login prompt appears. **Note:** To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.
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.

Ping

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 **System > System Utilities > Ping** in the navigation menu.



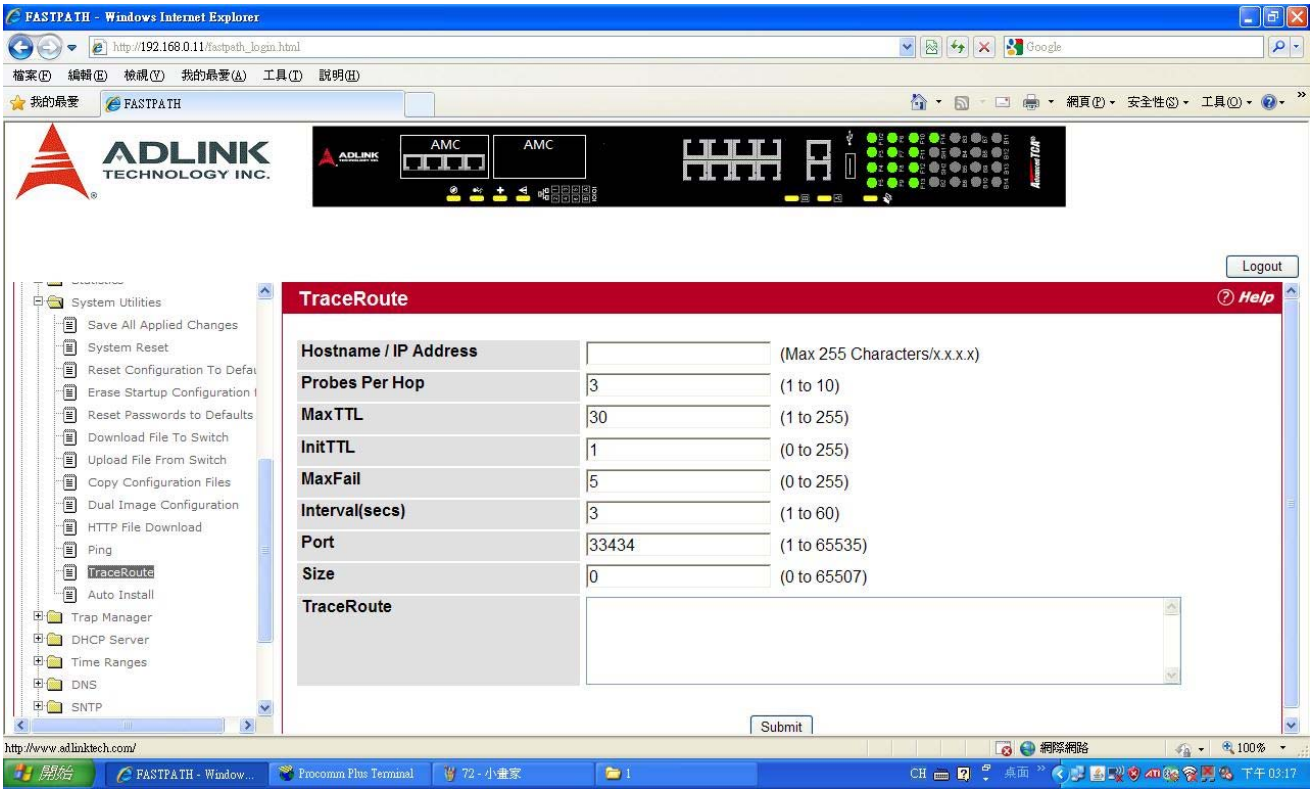
Field	Description
Hostname/IP Address	Enter the IP address or the host name of the station you want the switch to ping. The initial value is blank. This information is not retained across a power cycle.
Count	Specify the number of pings to send.
Interval	Specify the number of seconds between pings sent.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

Click **Submit** to send the ping.

TraceRoute

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

To display this page, click **System > System Utilities> TraceRoute** in the navigation tree.



Field	Description
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.

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 in on the switch.

The DHCP server that the switch communicates with must provide the following information:

• The IP address and subnet mask (option 1) to be assigned to the switch.

• The IP address of a default gateway (option 3), if needed for IP communication.

• The identification of the TFTP server from which to obtain the boot file. This is given by any of the following fields, in the priority shown (highest to lowest):

- The sname field of the DHCP reply.

- The hostname of the TFTP server (option 66). Either the TFTP address or name is specified—not both—in most network configurations. If a TFTP hostname is given, a DNS server is required to translate the name to an IP address.

- The IP address of the TFTP server (option 150).

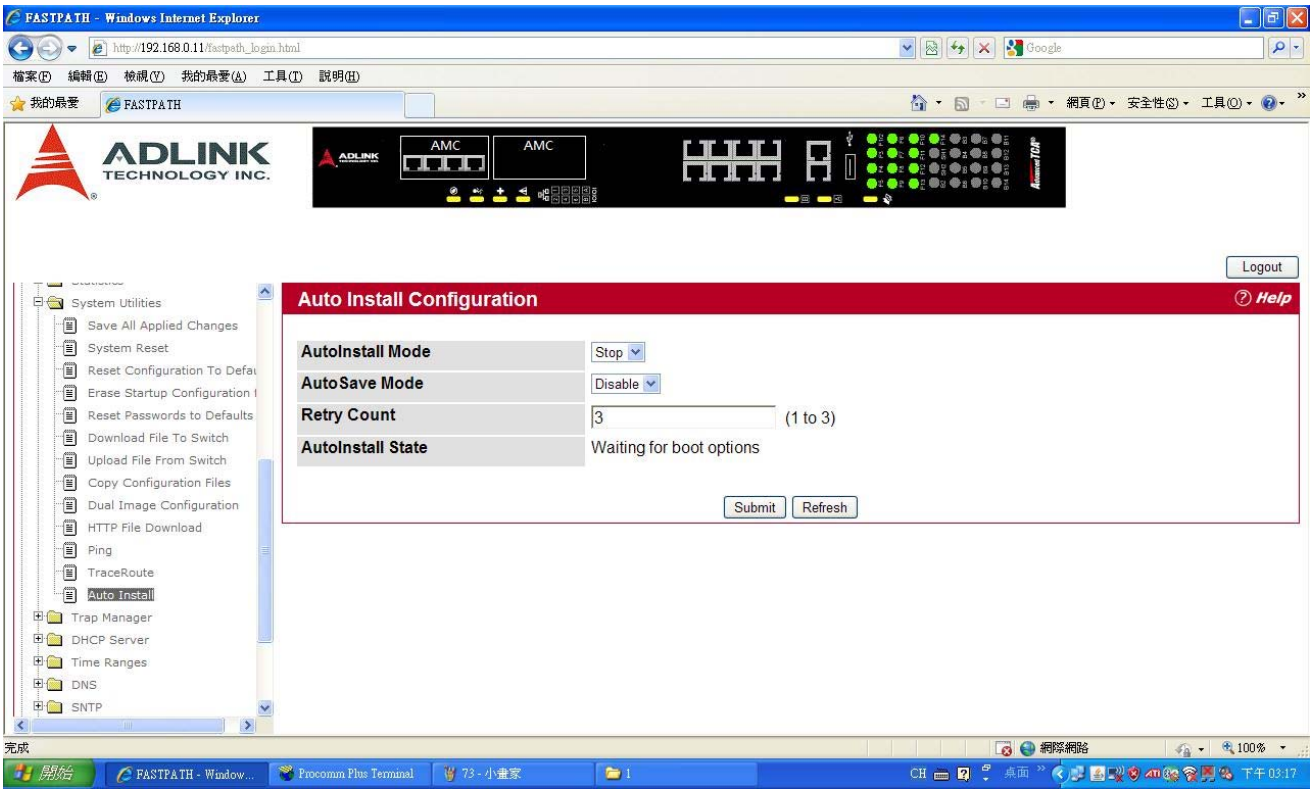
- The address of the TFTP server supplied in the siaddr field.

- The name of the configuration file (boot file or option 67) to be downloaded from the TFTP server. **The boot file name must have a file type of *.cfg.**

• The IP addresses of DNS name servers (option 6). The IP addresses of DNS name servers should be returned from the DHCP server only if the DNS server is in the same LAN as the switch performing AutoInstall. A DNS server is needed to resolve the IP address of the TFTP server if only the “sname” or option 66 values are returned to 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 the AutoInstall page, click **System > System Utilities> AutoInstall**.



Field	Description
AutoInstall Mode	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. After 3 retries, AutoInstall informs the failure to the TR-069 module, and TR-069 client tries to download the configuration file from a TFTP server through RequestDownload RPC. You can 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.

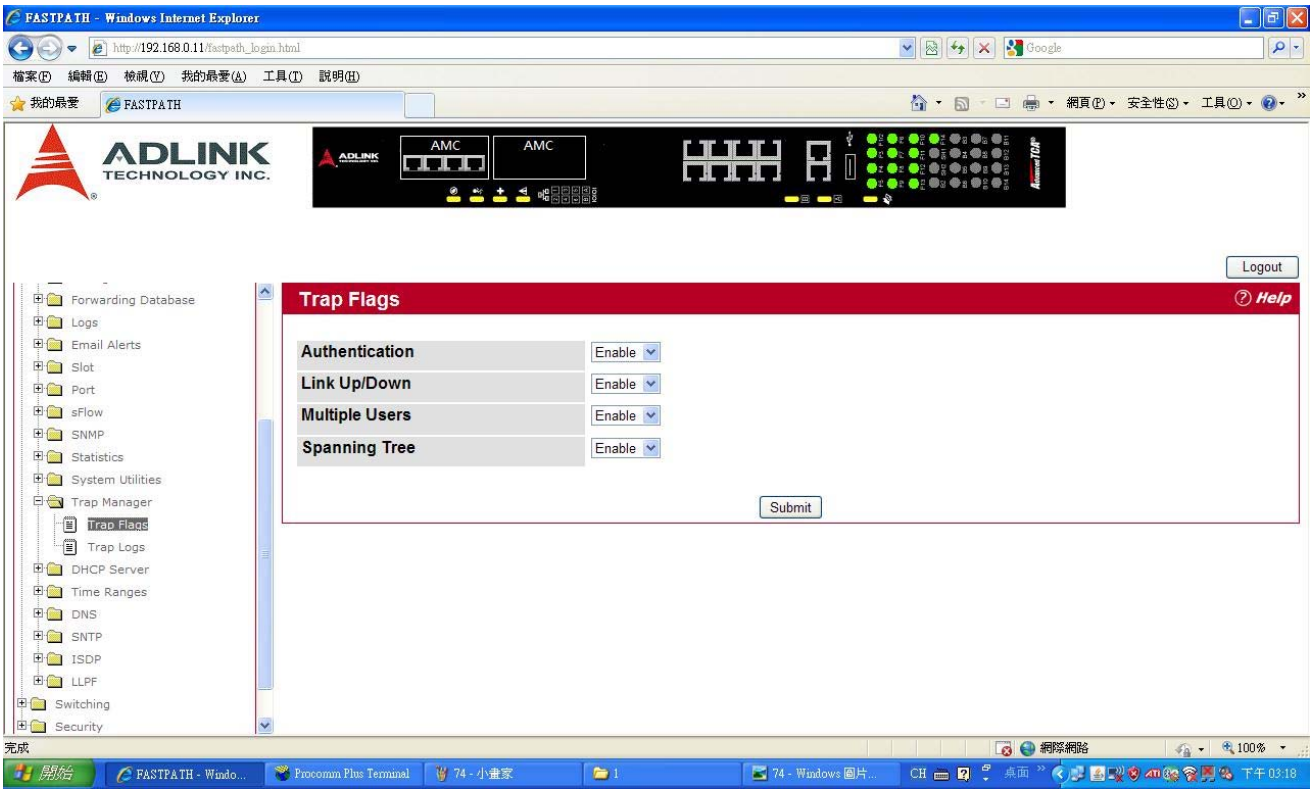
Click **Refresh** to display the most recently configured AutoInstall state from the switch.

Managing SNMP Traps

The pages in the Trap Manager folder allow you to view and configure information about SNMP traps the system generates.

Trap Flags

Use the Trap Flags page to enable or disable traps 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. To access the Trap Flags page, click **System > Trap Manager > Trap Flags** page.



The fields available on the Trap Flags page depends on the packages installed on your system. For example, if your system does not have the BGP4 package installed, the BGP Traps field is not available.

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.

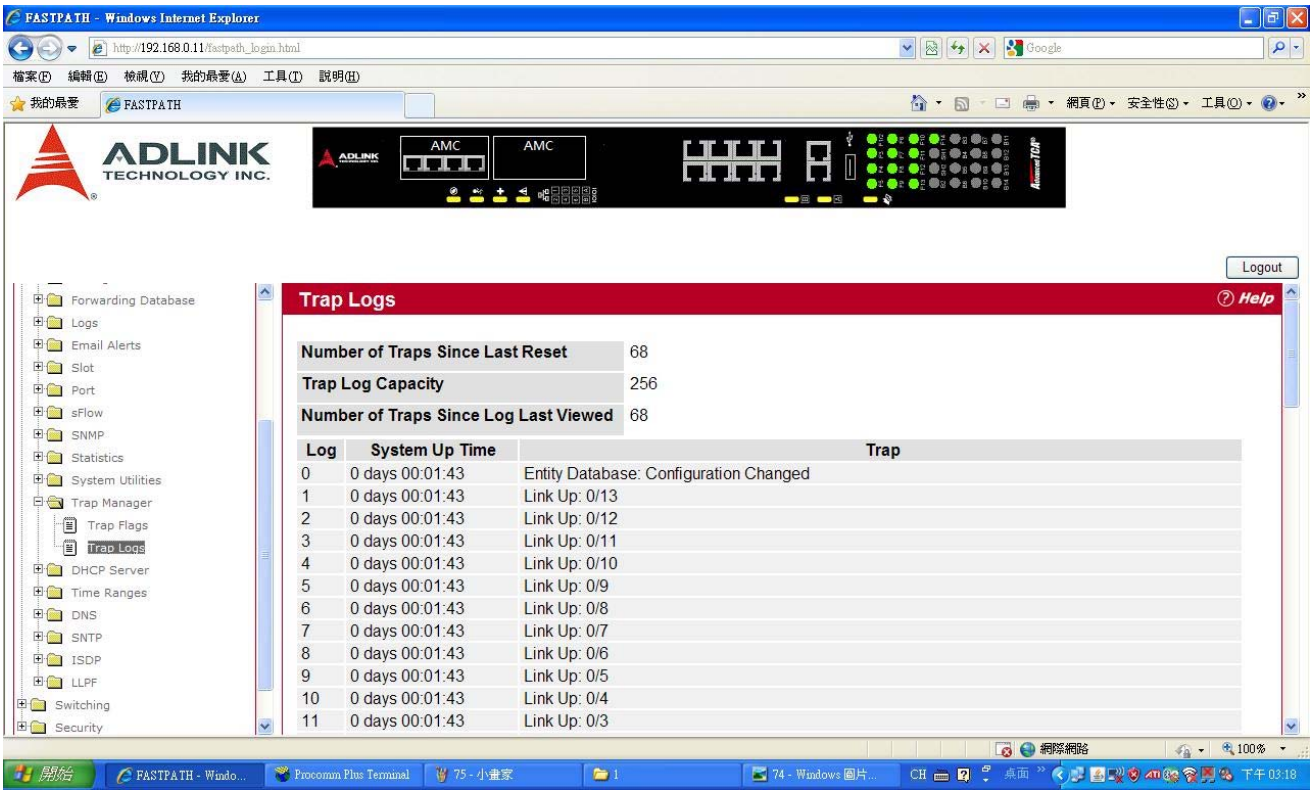
Field	Description
Multiple Users	Enable or disable activation of multiple user traps by selecting the corresponding line on the pulldown entry field. The factory default is enabled. This trap is triggered when the same user ID is logged into the switch more than once at the same time (either via telnet 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.
BGP4 Traps	Enable or disable activation of BGP traps by selecting the corresponding line on the pulldown entry field. The factory default is enabled. If your system does not support BGP, this field is not available.
DVMRP Traps	Enable or disable activation of DVMRP traps by selecting the corresponding line on the pulldown entry field. The factory default is enabled. If your system does not support Multicast, this field is not available.
OSPF Traps	Enable or disable activation of OSPF traps by selecting the corresponding line on the pulldown entry field. The factory default is enabled. This field can be configured only if the OSPF admin mode is enabled. If your system does not support OSPF routing, this field is not available.
PIM Traps	Enable or disable activation of PIM traps by selecting the corresponding line on the pulldown entry field. The factory default is enabled. If your system does not support Multicast, this field is not available.
Captive Portal	Select Enable to allow the SNMP agent on the switch to generate captive portal SNMP traps that are enabled. Select Disable to prevent 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.

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)”.

To access the Trap Log page, click **System > Trap Manager > Trap Log** in the navigation menu.



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.

Managing The DHCP Server

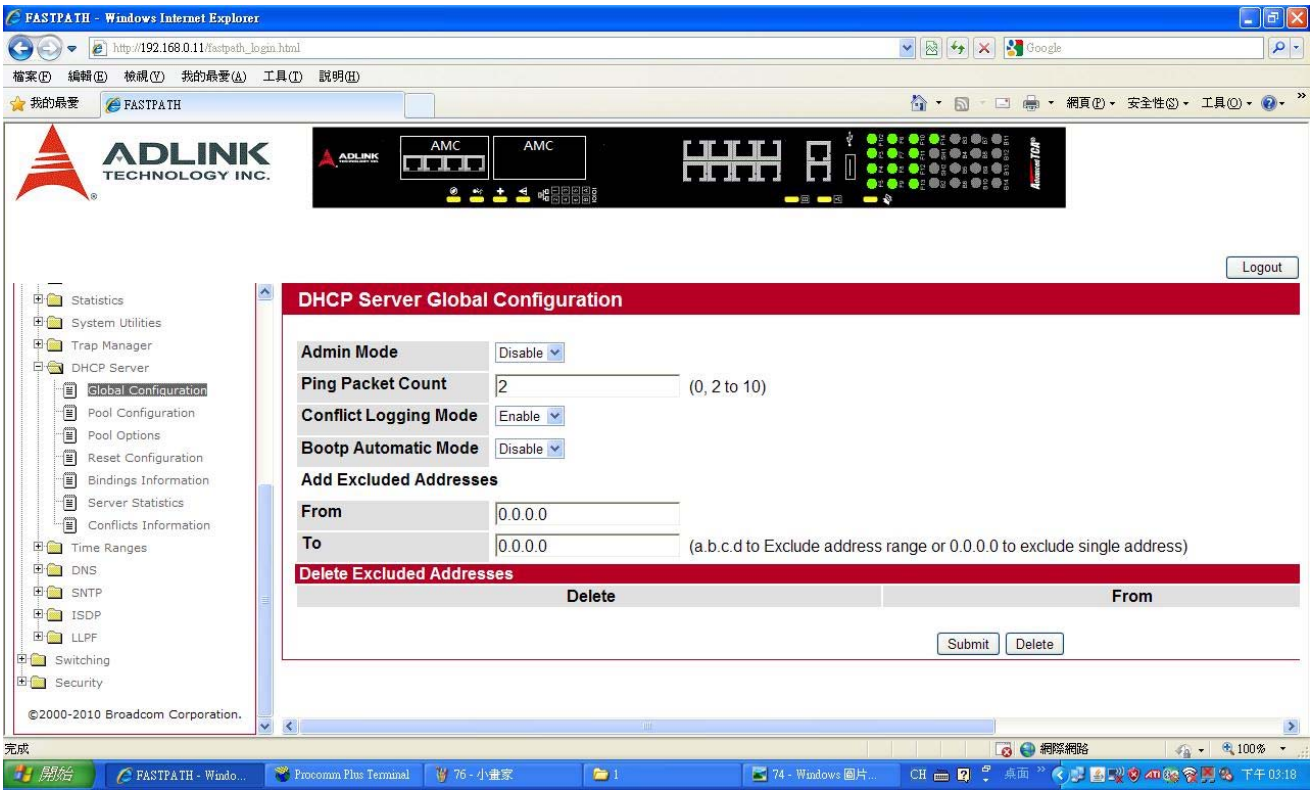
DHCP is generally used between clients (e.g., hosts) and servers (e.g., routers) for the purpose of assigning IP addresses, gateways, and other networking definitions such as DNS, NTP, and/or SIP parameters. The DHCP Server folder contains links to web pages that define and display DHCP parameters and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

- Global Configuration
- Pool Configuration
- Pool Options
- Reset Configuration
- Bindings Information
- Server Statistics
- Conflicts Information

Global Configuration

Use the Global Configuration page to configure DHCP global parameters.

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



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.
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.
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 , 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 shows. Each address or address range has a check box next to it.

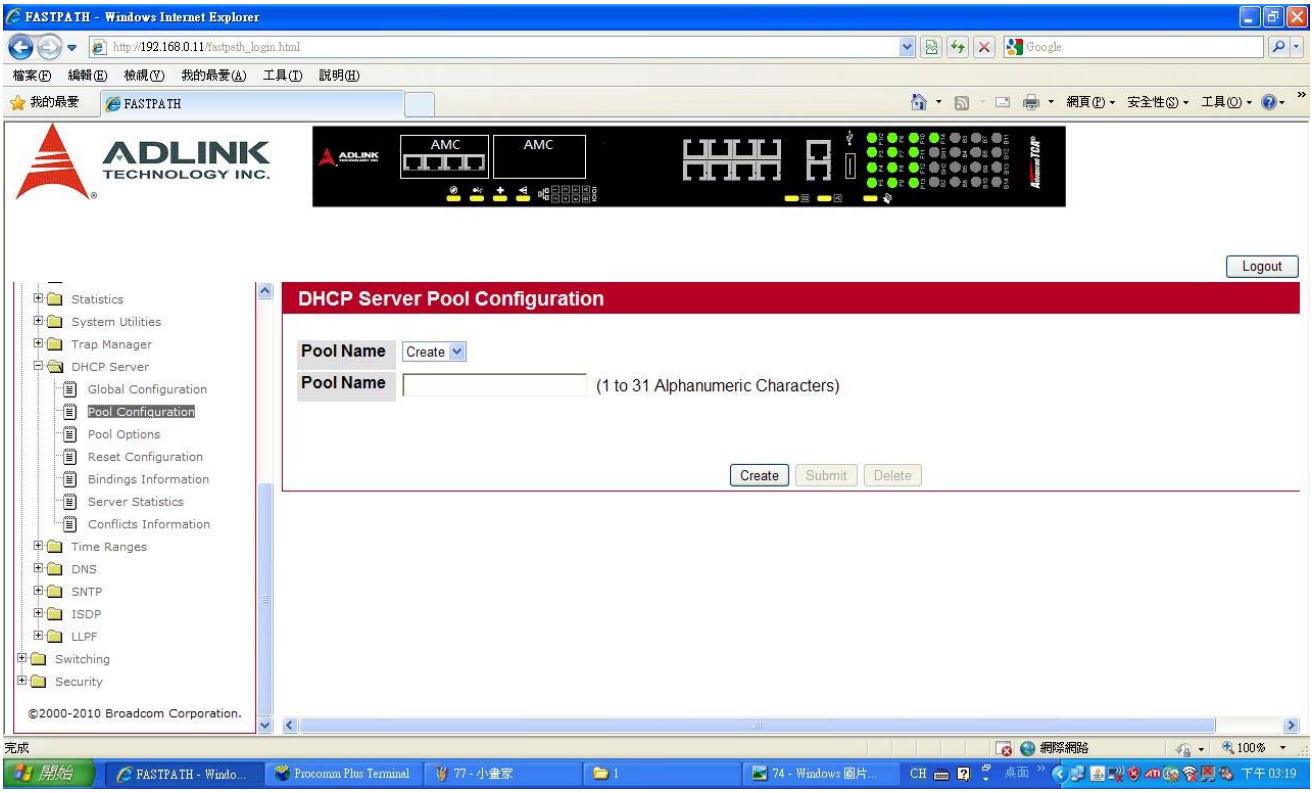
• If you change any settings or add an excluded address range, click **Submit** to apply the changes to the system. Each time you enter a value in the **From** or **To** fields, click **Submit** to add the address or address range to the excluded address list.

• 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.

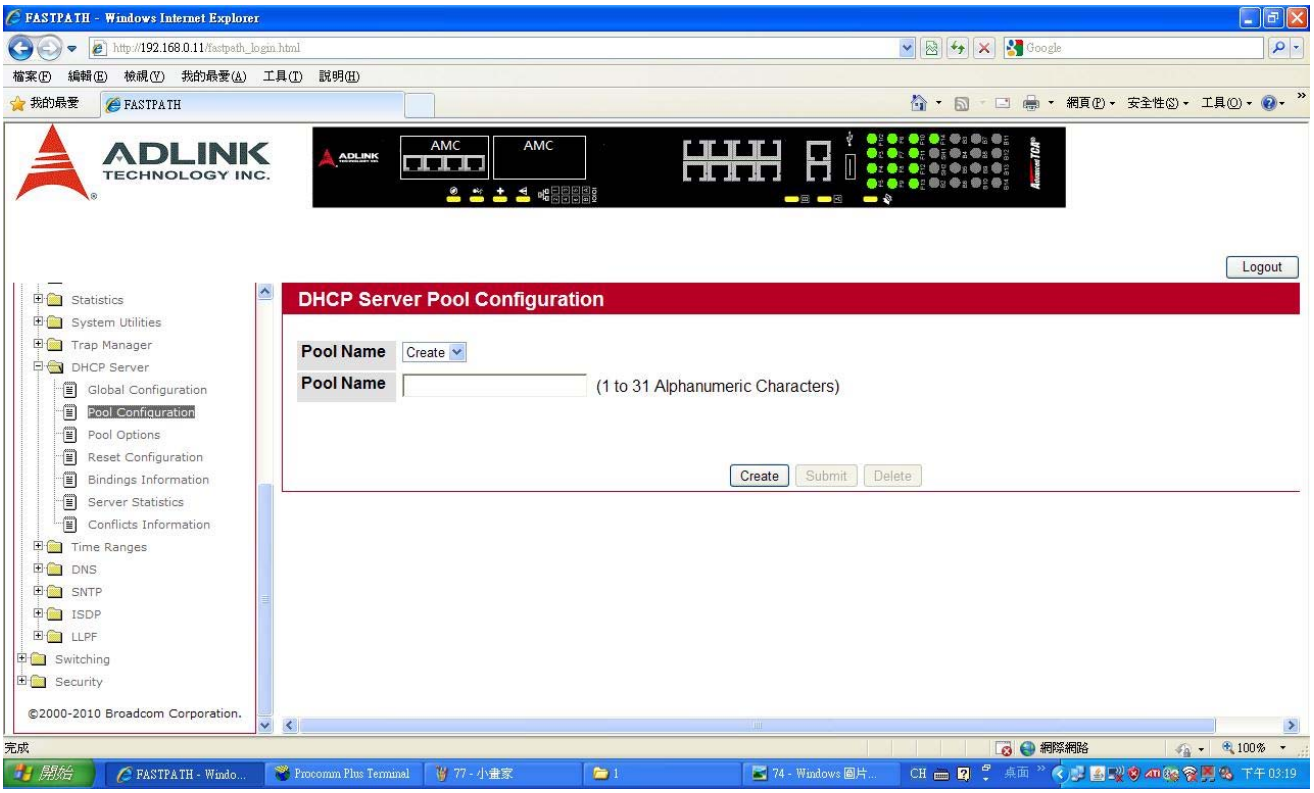
To access the Pool Configuration page, click **System > DHCP Server > Pool Configuration** in the navigation tree.



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.

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



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. • **Unallocated**: The addresses are not assigned to a client. • **Automatic**: 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**

Field	Description
	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.
Lease Time	Specifies the type of lease to assign clients: • **Infinite**: For dynamic bindings, an infinite least 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

Field	Description
	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: • **p-node Peer-to-Pee**r: 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.

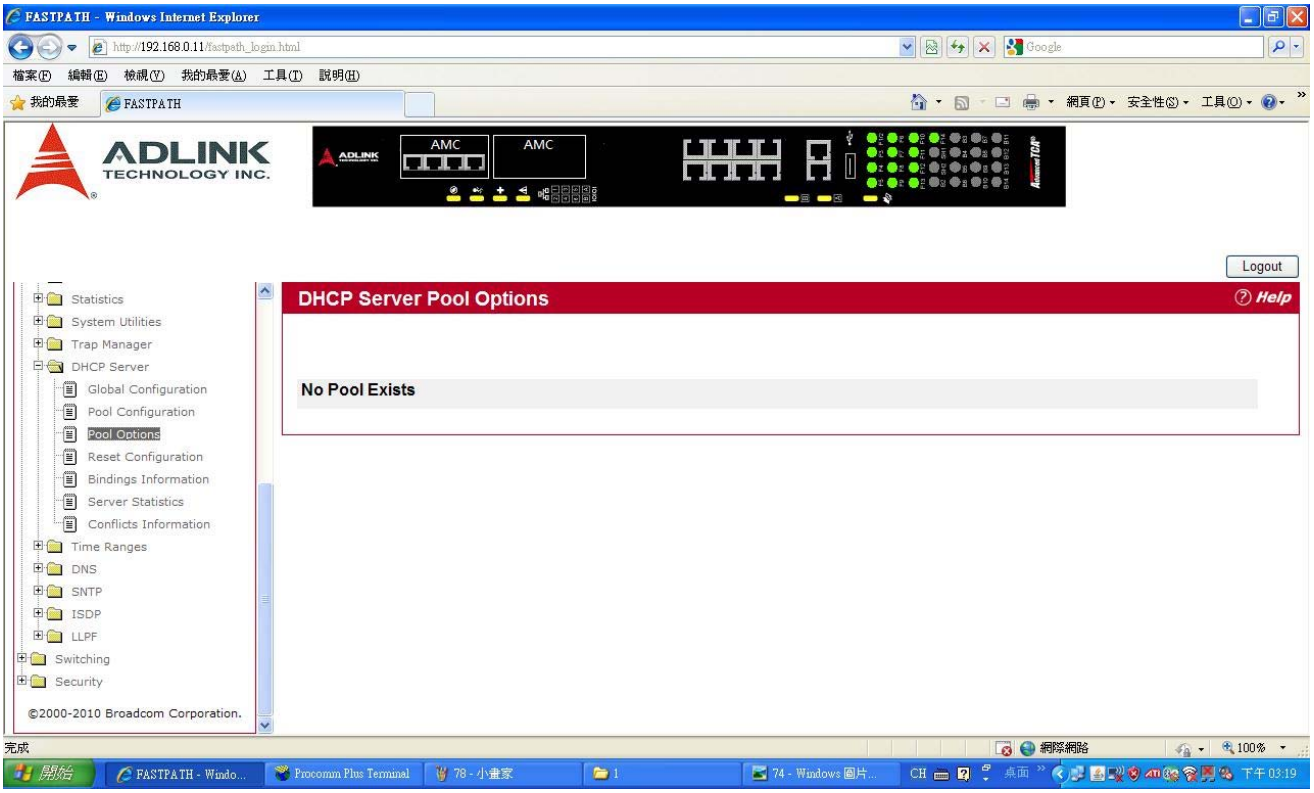
To delete a pool, select the pool from the **Pool Name** drop-down menu and click **Delete**.

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 **System > DHCP Server > Pool Options** in the navigation menu.

If no DHCP pools exist, the Pool Options page does not display the fields.



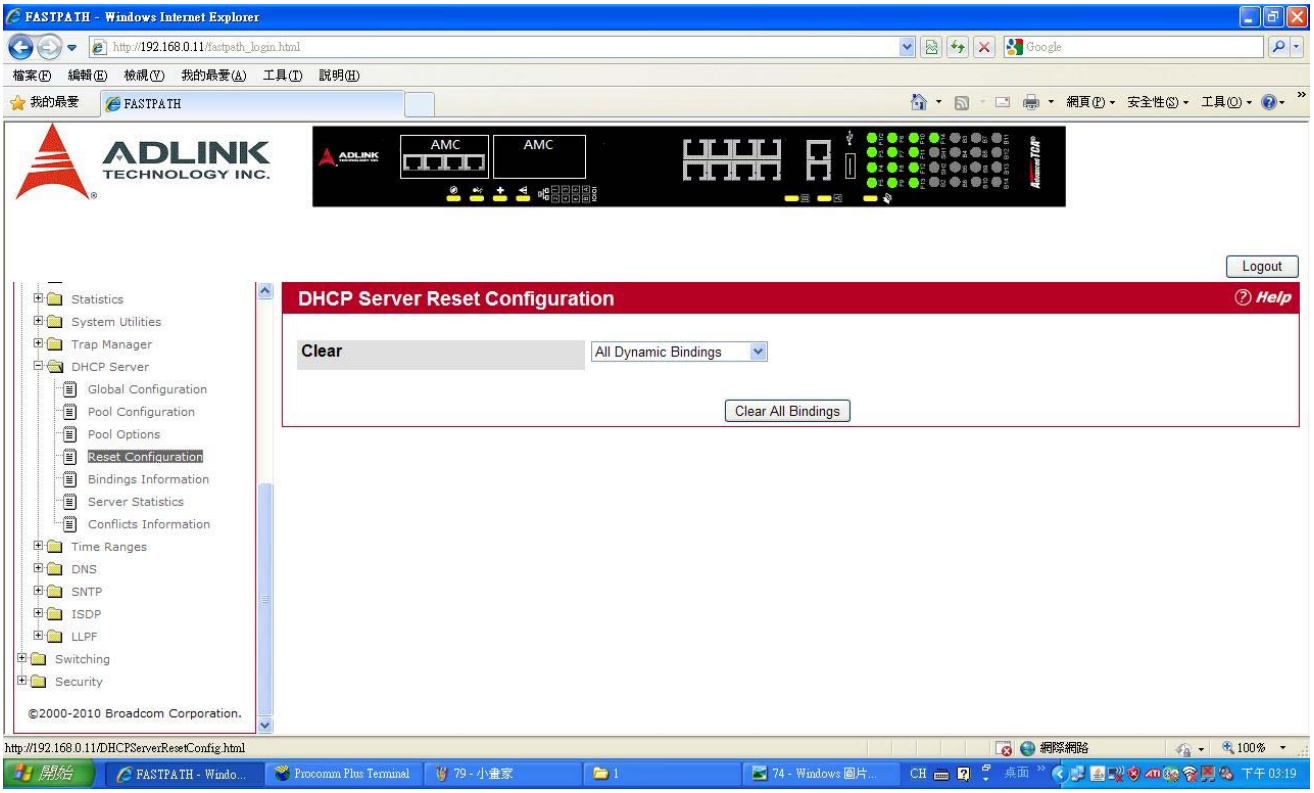
If any DHCP pools are configured on the system, the Pool Options page contains the following fields:

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: • **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.
ASCII Value	Shows the Option ASCII Value for the selected pool.
Hex Value	Shows the Option Hex Value for the selected pool.
IP Address Value	Shows the Option IP Address Value for the selected pool.
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 **System > DHCP Server > Reset Configuration** in the navigation tree.



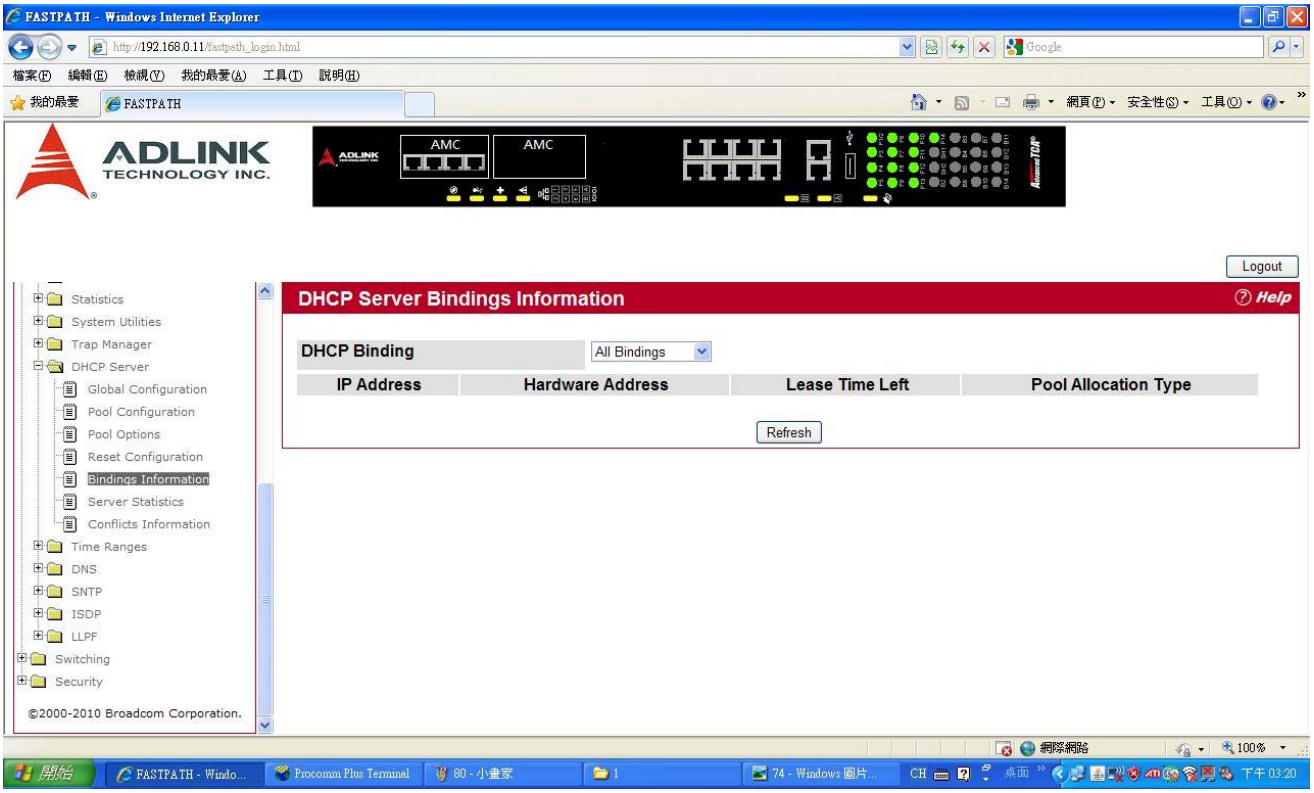
Field	Description
Clear	Specifies what to clear from the DHCP server database: • **All Dynamic Bindings**: Deletes all dynamic bindings from all address pools. • **Specific Dynamic Binding**: Deletes the specified binding. • **All Address Conflicts**: Deletes all address conflicts from the DHCP server 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.

Bindings Information

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

To access the Bindings Information page, click **System > DHCP Server > Bindings Information** in the navigation tree.



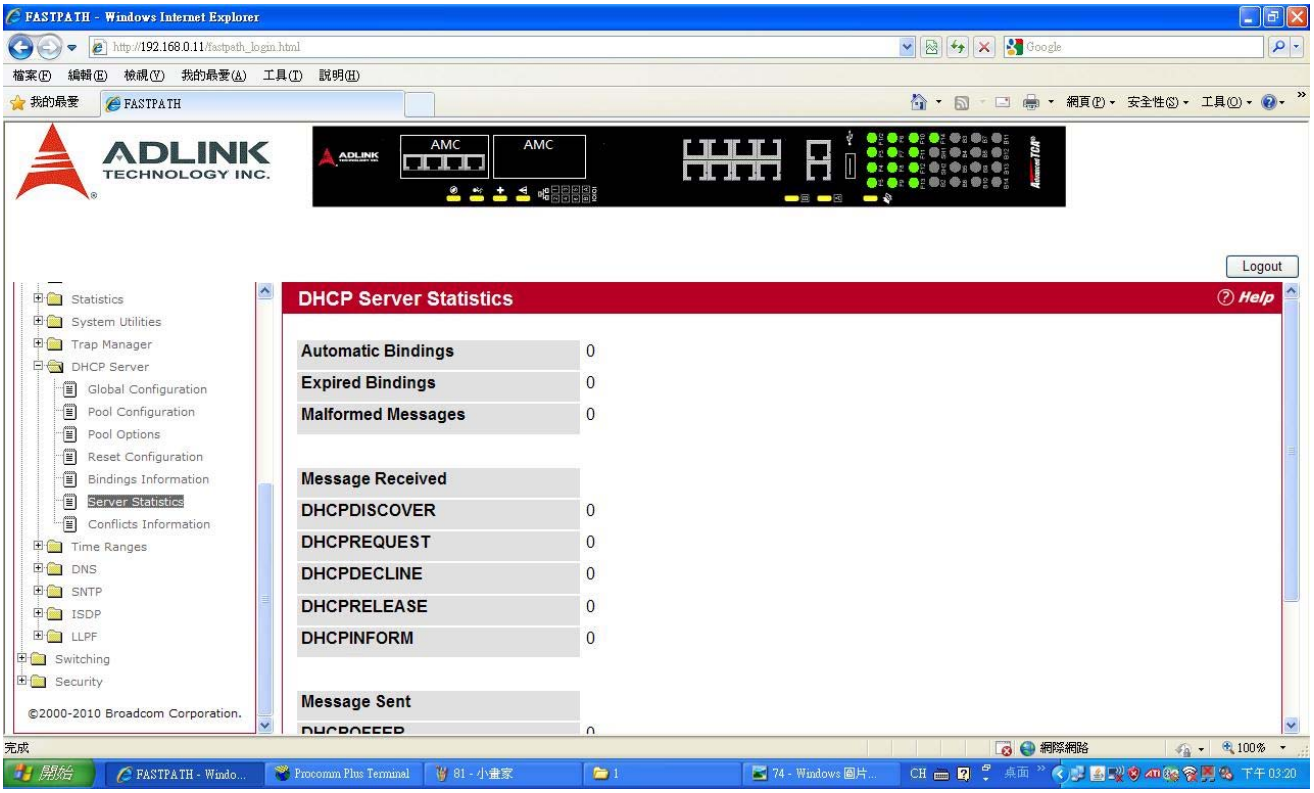
Field	Description
DHCP Binding	Select the bindings to display: • **All Bindings**: Show all bindings. • **Specific Binding**: Show a specific binding. When you select this option, the screen refreshes, and the **Binding IP Address** field appears.
Binding IP Address	Specify the IP address for which you 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	Shows the remaining time left in the lease in Days, Hours and Minutes dd:hh:mm format.
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 **System > DHCP Server > Server Statistics** in the navigation menu.



Field	Description
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.

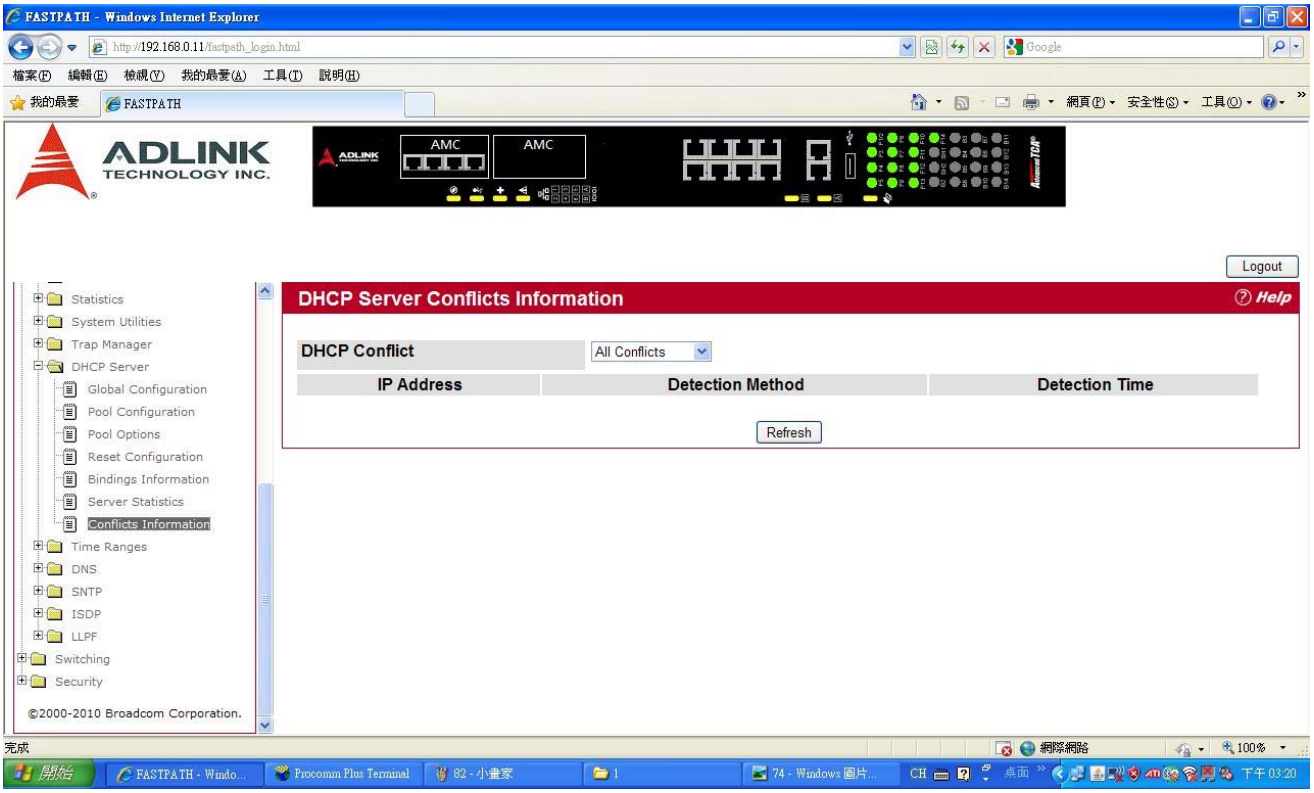
Field	Description
DHCPOFFER	Shows the number of DHCPOFFER messages sent by the DHCP server.
DHCPACK	Shows the number of DHCPACK messages sent by the DHCP server.
DHCPNAK	Shows the number of DHCPNAK messages sent by the DHCP server.

- 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 **System > DHCP Server > Conflicts Information** in the navigation tree.



Field	Description
DHCP Conflicts	Select the DHCP conflicts to display: • **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.

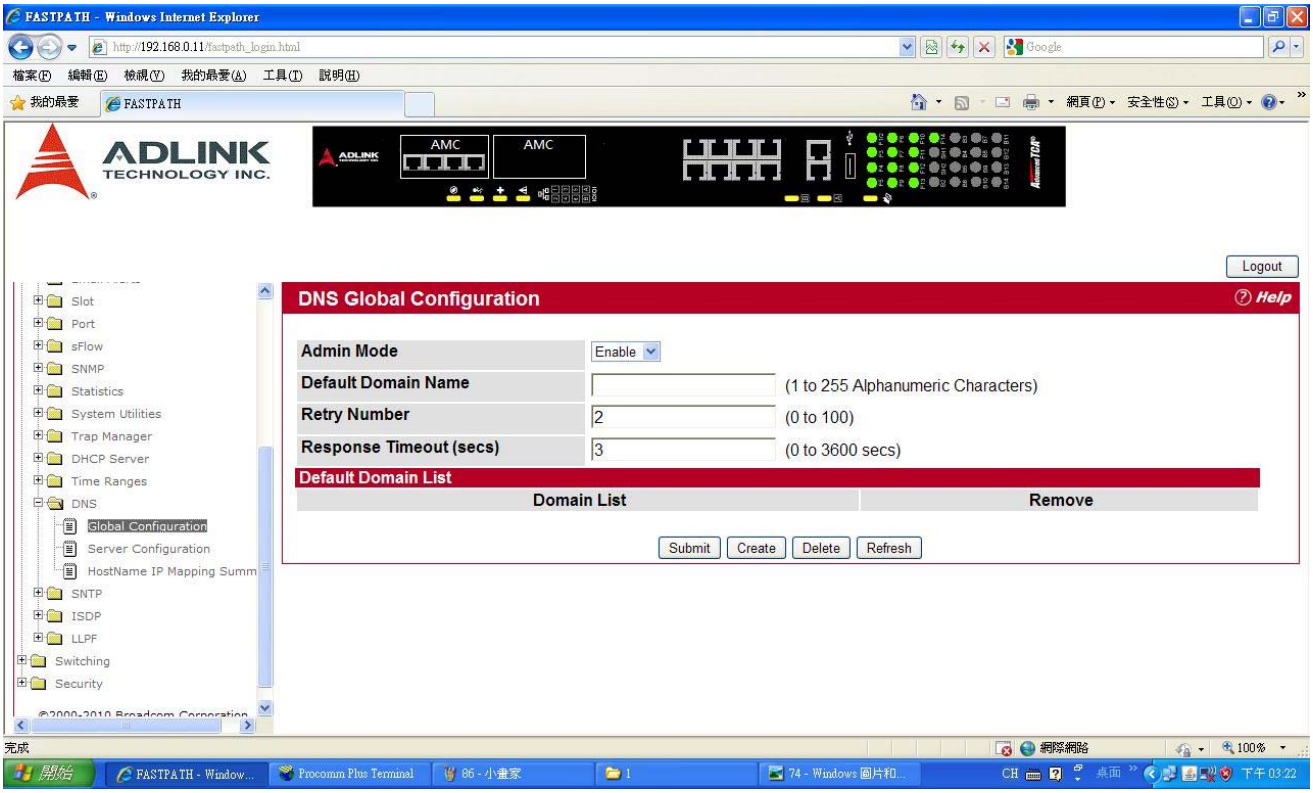
Configuring DNS

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 **System > DNS > Global Configuration**.



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.com and the user enters hotmail, then hotmail is changed to hotmail.com 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.

Field	Description
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.

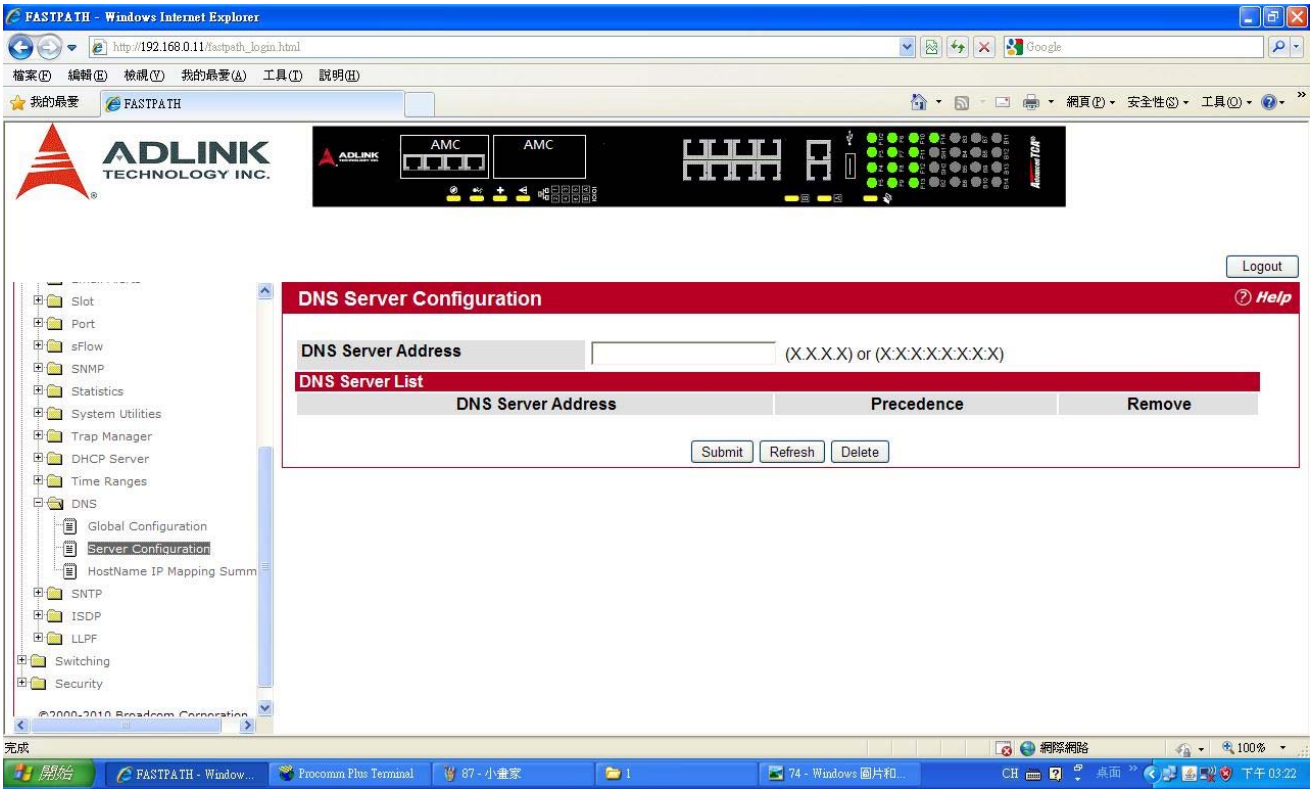
To create a new list of domain names, click **Create**. Then enter a name of the list and click submit. Repeat this step to add multiple domains to the default domain list.

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 **System > DNS > Server Configuration**.



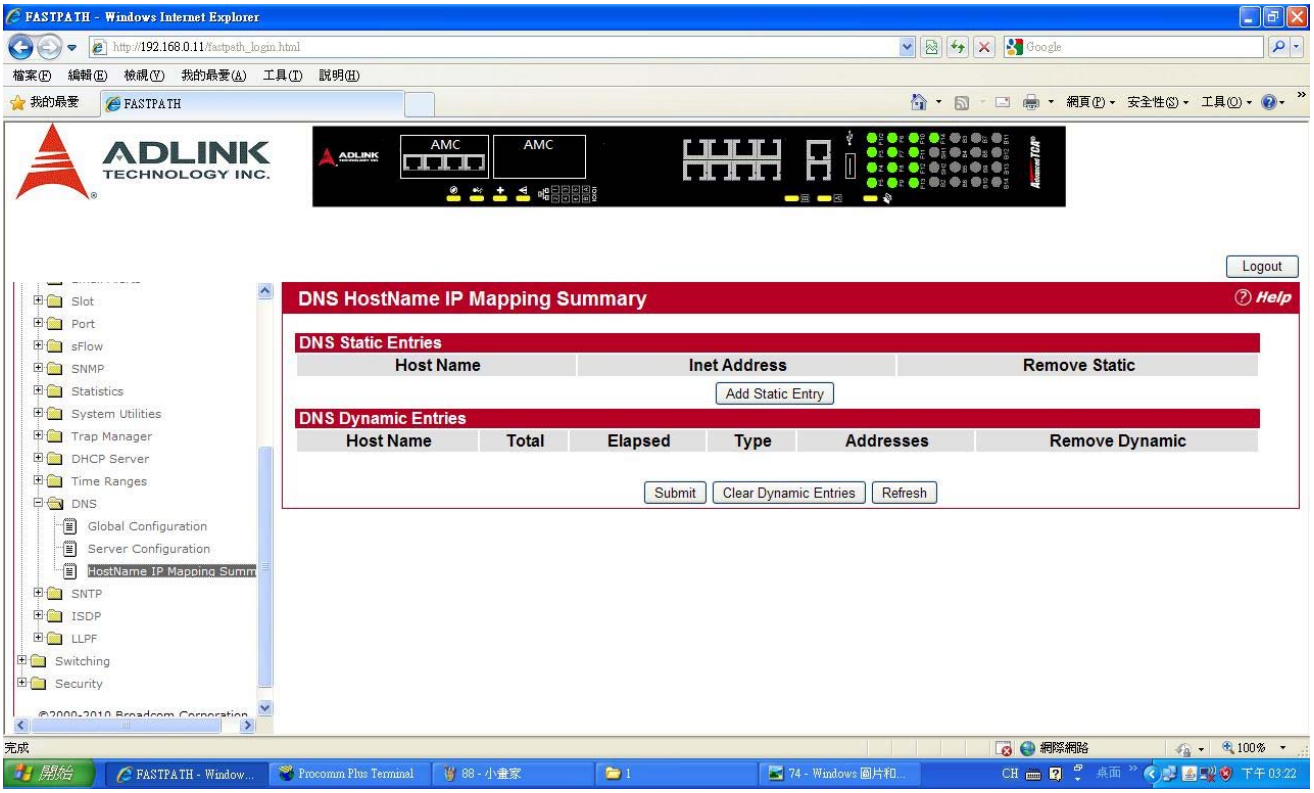
Field	Description
DNS Server Address	To add a new DNS server to the list, enter the DNS server IPv4 or IPv6 address in numeric notation.
Precedence	Shows the precedence value of the server that determines which server is contacted first; a lower number indicates has higher precedence.

- 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 **System > DNS > HostName IP Mapping Summary** in the navigation tree, then click the **Add Static Entry** button.



Field	Description
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.

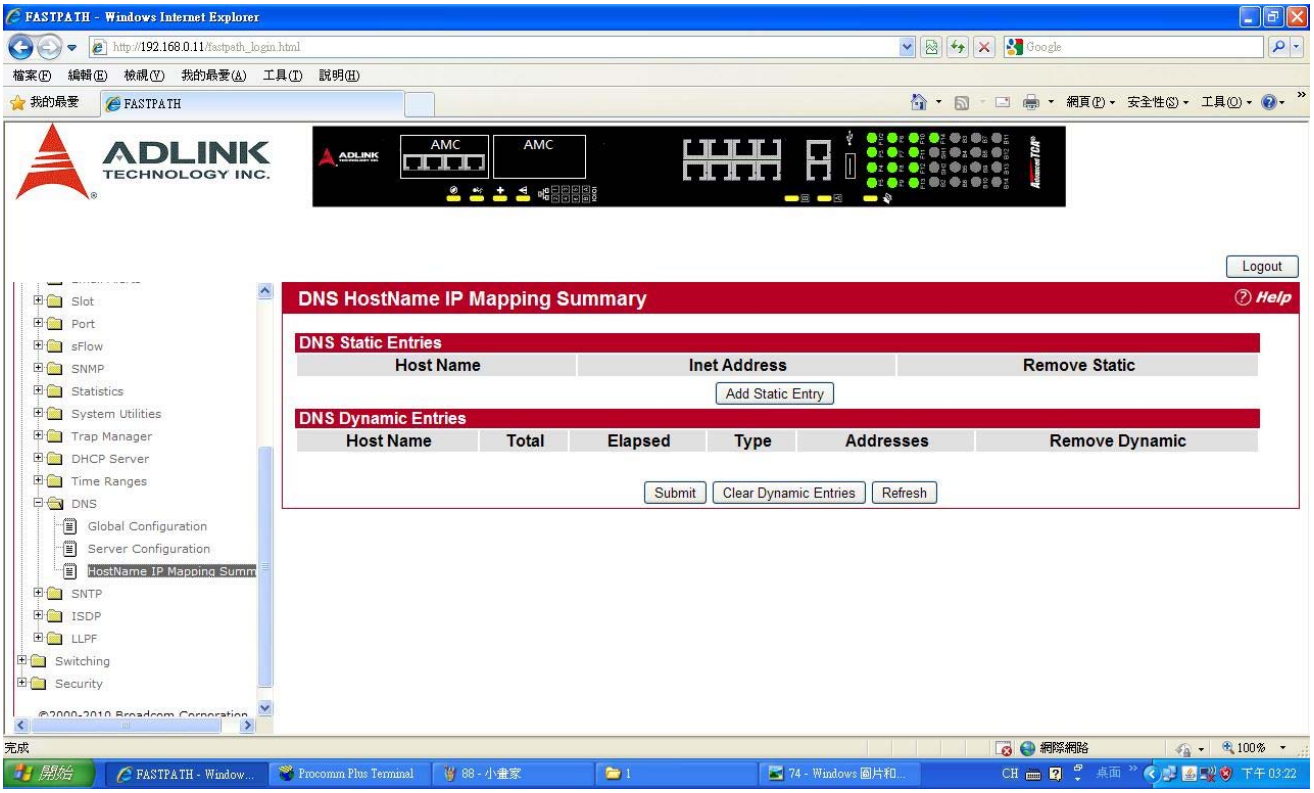
• Click **Submit** to apply the new configuration and cause the change to take effect immediately. These changes will not be retained across a power cycle unless a Save is performed.

• Click **Back** to cancel and redisplay 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 **System > DNS > Host Name IP Mapping Summary** in the navigation tree.



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.

Click **Add Static Entry** to load the Host Name IP Mapping Configuration page in order to configure the Host Name IP Mapping entries.

Field	Description
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.

Field	Description
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 **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 SNTP Settings

FASTPATH® 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. FASTPATH® software operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by Stratums. Stratums define 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 stratums:

• **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.

The SNTP folder contains links to view or configure the following features:

• SNTP Global Configuration

• SNTP Global Status

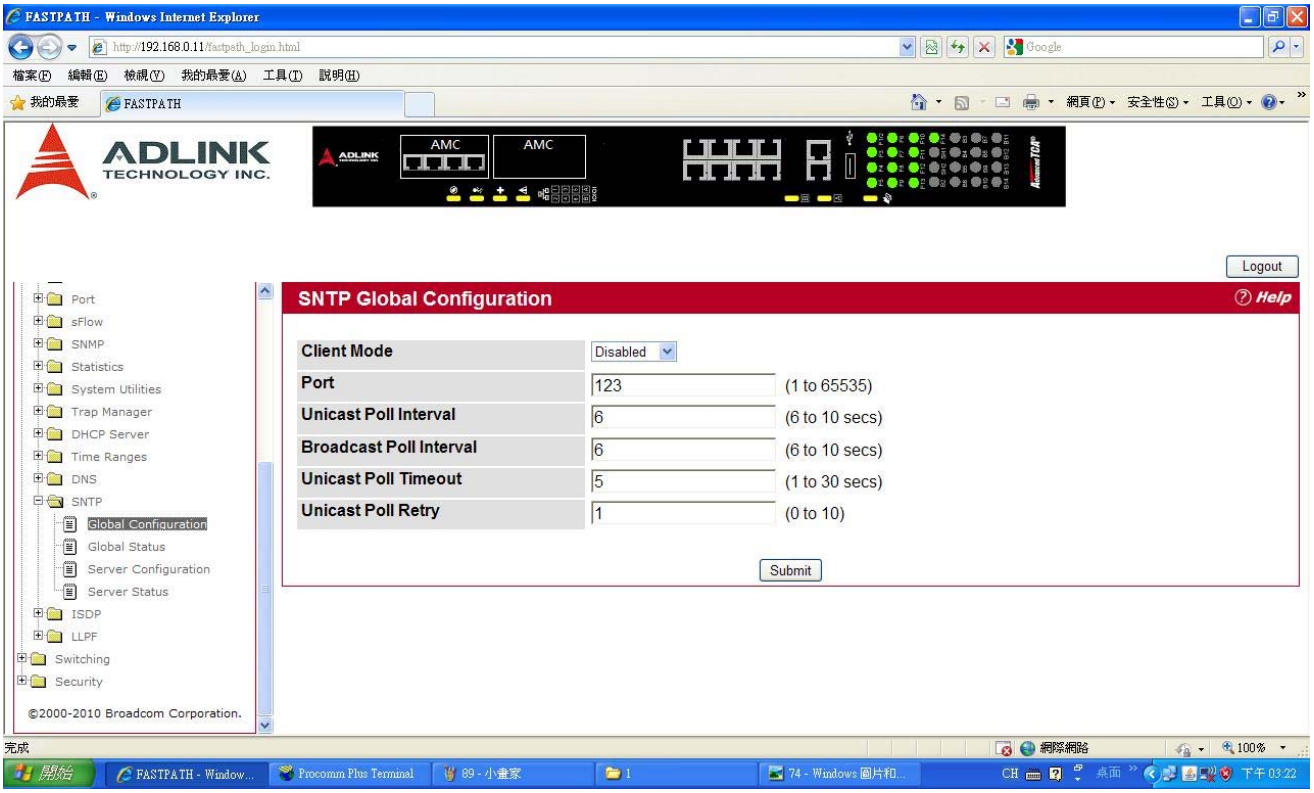
• SNTP Server Configuration

• SNTP Server Status

SNTP Global Configuration

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

To display the SNTP Global Configuration page, click **System > SNTP** > **Global Configuration** in the navigation menu.



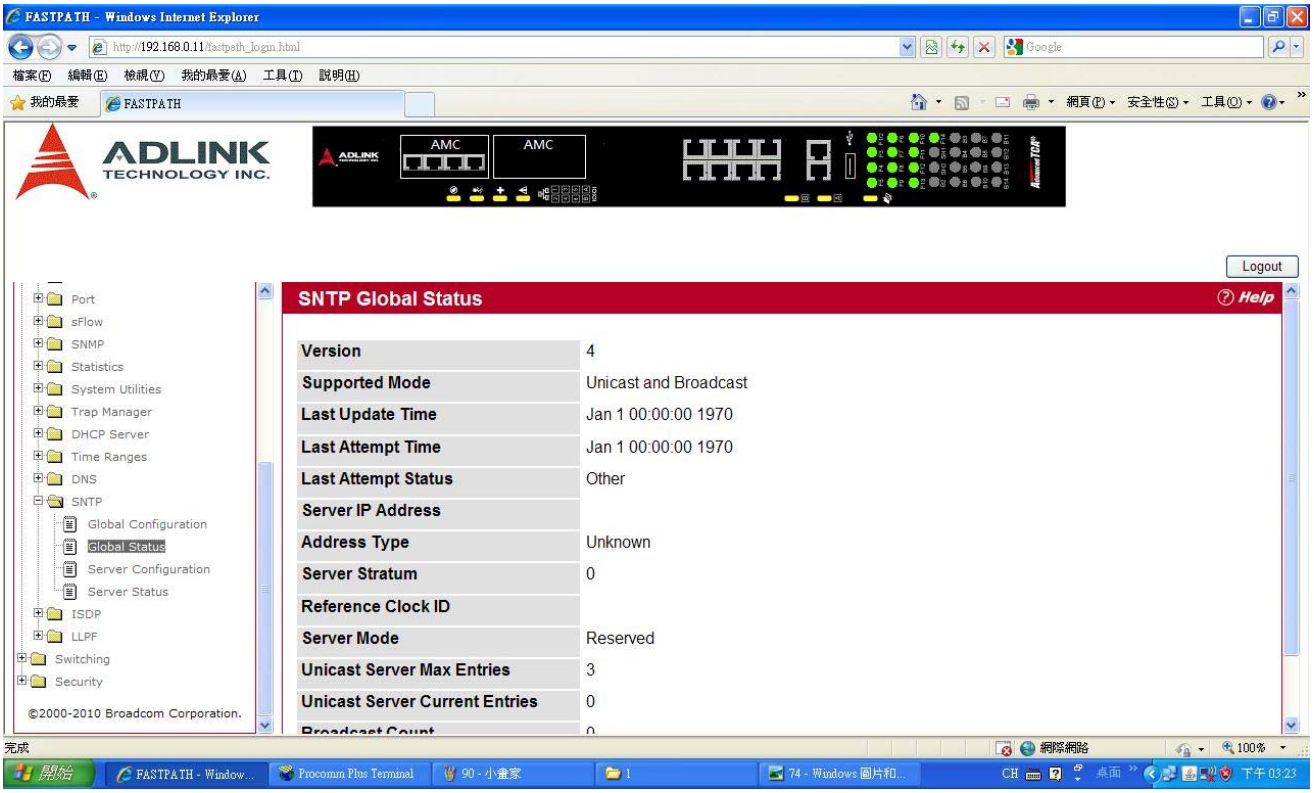
Field	Description
Client Mode	Use drop-down list specify the SNTP client mode, which is one of the following modes: • **Disable**: SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed. • **Unicast**: SNTP operates in a point to point fashion. 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.
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 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 **System > SNTP > Global Status** in the navigation menu.



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: • **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.

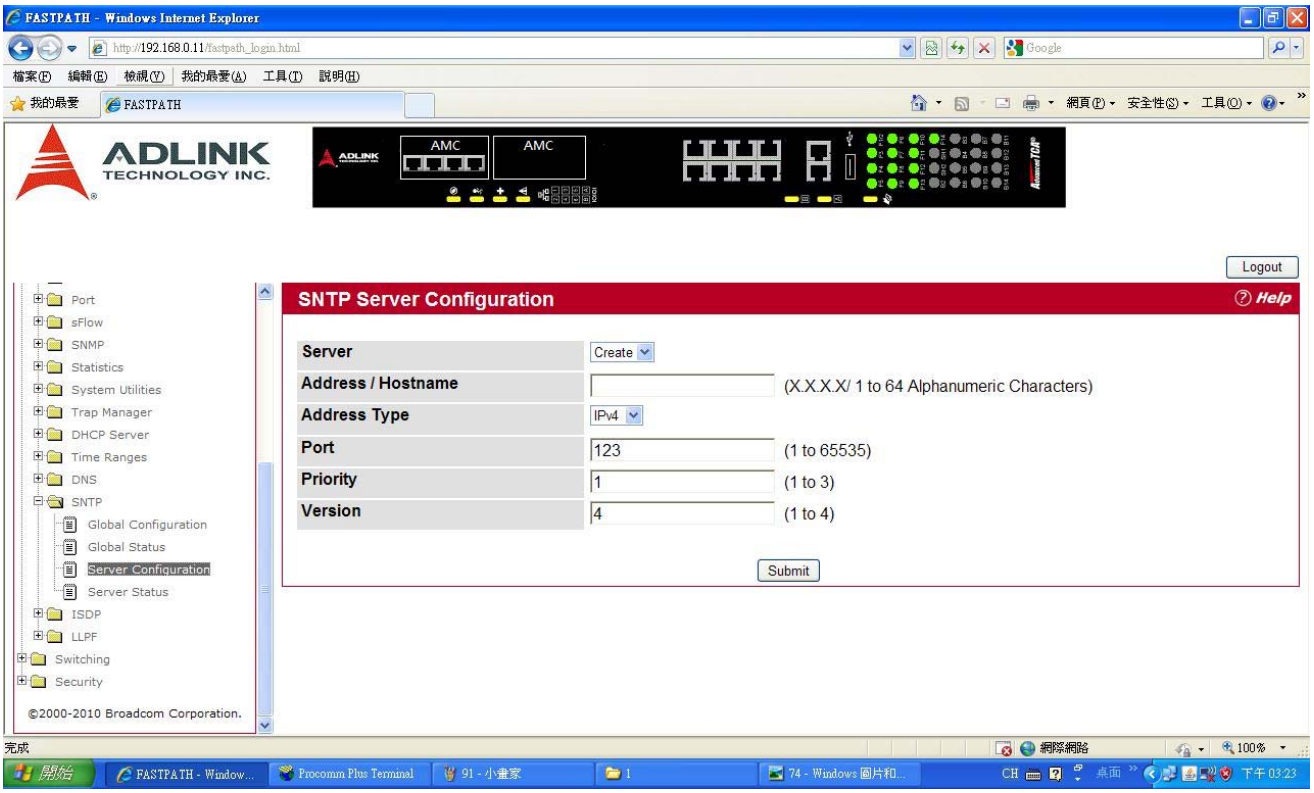
Field	Description
	• **Bad Date Encoded**: The time provided by the SNTP server is not valid. • **Version Not Supported**: The SNTP version supported by the server is not compatible with the version supported by the client. • **Server Unsynchronized**: The SNTP server is not synchronized with its peers. 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.
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.

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 **System > SNTP > Server Configuration** in the navigation tree.



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	Enter a priority from 1 to 3, with 1 being the highest priority. The router will attempt to use the highest priority server and, if it is not available, will use the next highest server.
Version	Enter the protocol version number.
Priority (1-3)	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.

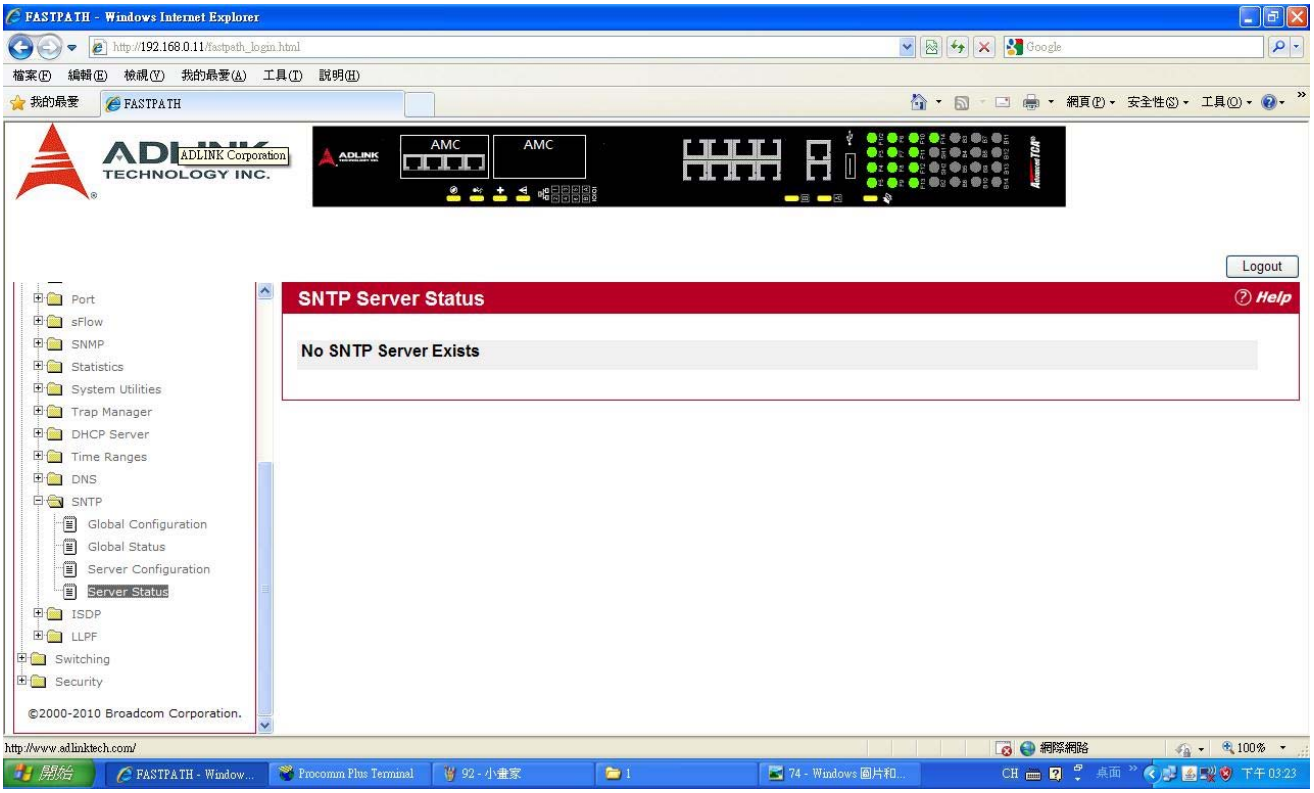
To add an SNTP server, select Create from the **Server** list, complete the remaining fields as desired, and click **Submit**. The SNTP server is added, and is now reflected in the Server list. You must perform a save to retain your changes over a power cycle.

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 **System > SNTP > Server Status** in the navigation menu.



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.
Last Attempt Status	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: • **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.

Field	Description
	• **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.

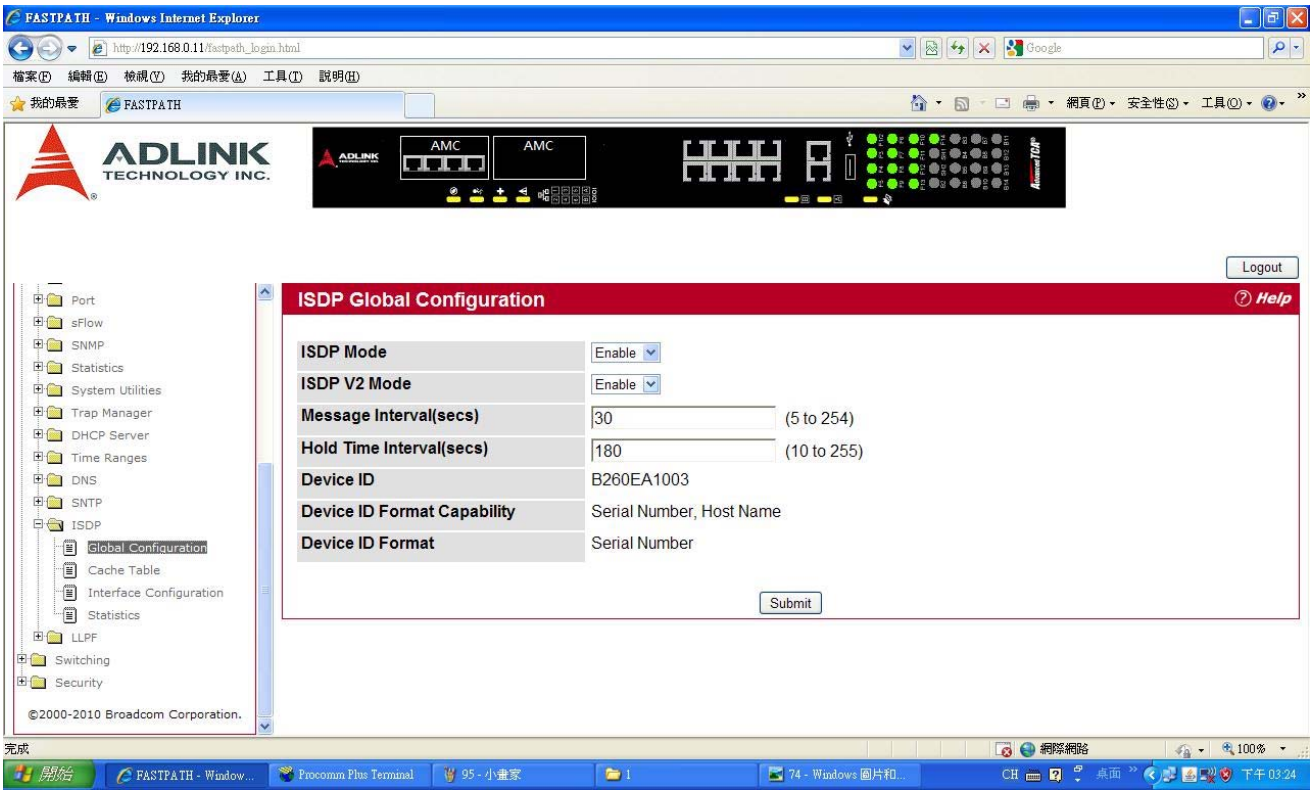
Configuring And Viewing ISDP Information

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. FASTPATH® software participates in the CDP protocol and is able to both discover and be discovered by other CDP supporting devices. The following pages are accessible from this ISDP folder:

- Global Configuration
- Cache Table
- Interface Configuration
- Statistics

Global Configuration

From the ISDP **Global Configuration** page, you can configure the ISDP settings for the switch, such as the administrative mode.



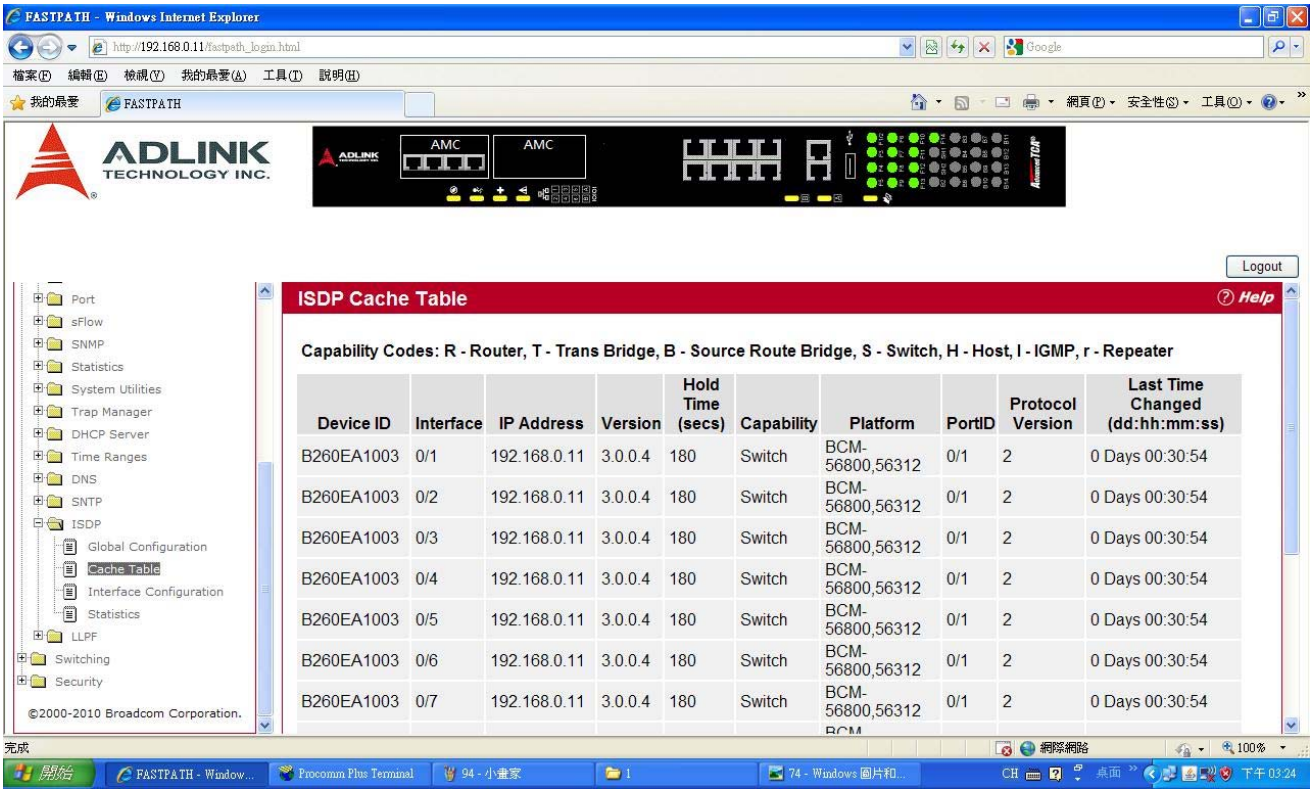
The following table describes the fields available on the ISDP **Global Configuration** page.

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.

Field	Description
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.
Device ID Format Capability	Indicates the Device ID format capability of the device. • 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	Indicates the Device ID format of the device. • 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.

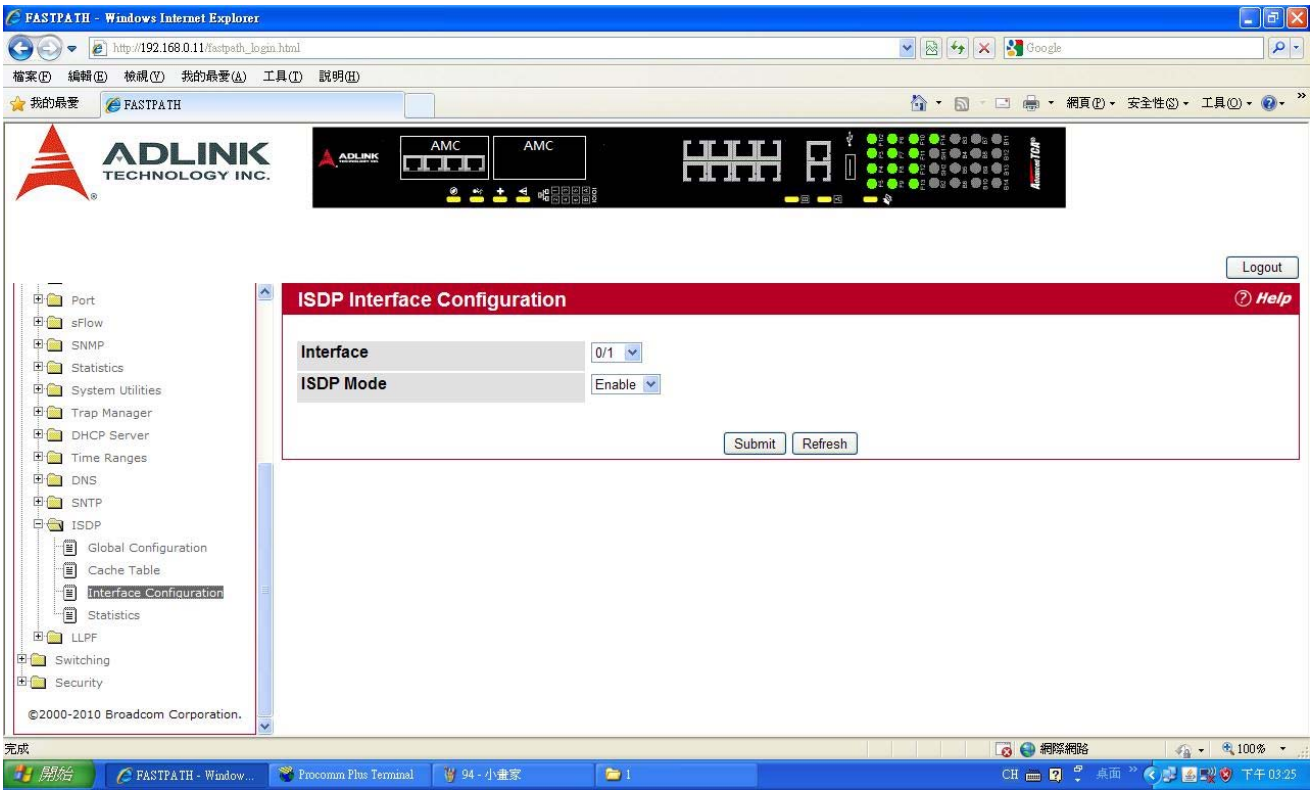


The following table describes the fields available on the ISDP **Cache Table** page.

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.
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.

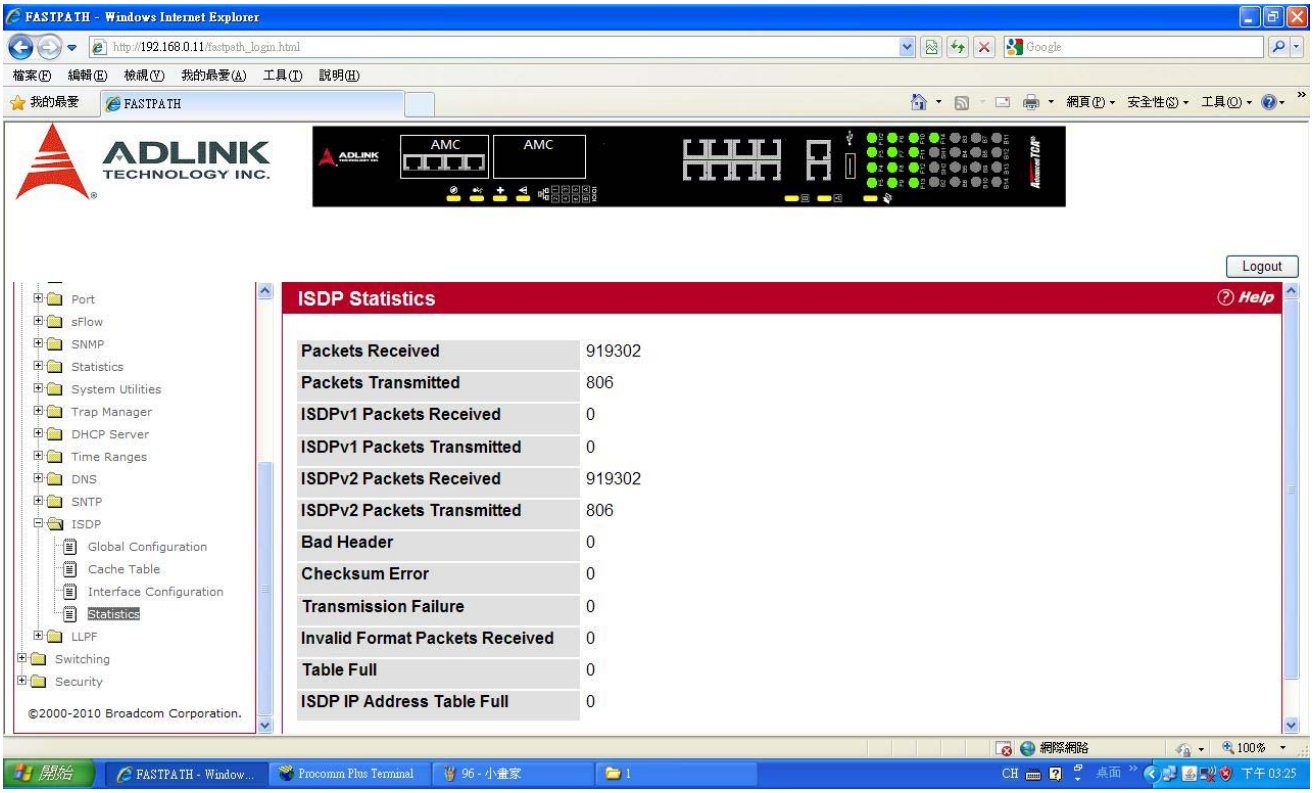


The following table describes the fields available on the ISDP **Interface Configuration** page.

Field	Description
Interface	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.



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

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.

Field	Description
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.

5.6. Configuring Switching Information

- Configuring DHCP Snooping
- Managing VLANs
- Double VLAN (DVLAN) Tunneling
- Configuring Protected Ports
- Managing IP Subnet-Based VLANs
- Managing MAC-Based VLANs
- Voice VLAN Configuration
- Creating MAC Filters
- Configuring GARP
- Configuring Dynamic ARP Inspection
- Configuring IGMP Snooping
- Configuring IGMP Snooping Queriers
- Configuring MLD Snooping
- Configuring MLD Snooping Queriers
- Creating Port Channels
- Viewing Multicast Forwarding Database Information
- Configuring Spanning Tree Protocol
- Mapping 802.1p Priority
- Configuring Port Security
- Managing LLDP

Configuring DHCP Snooping

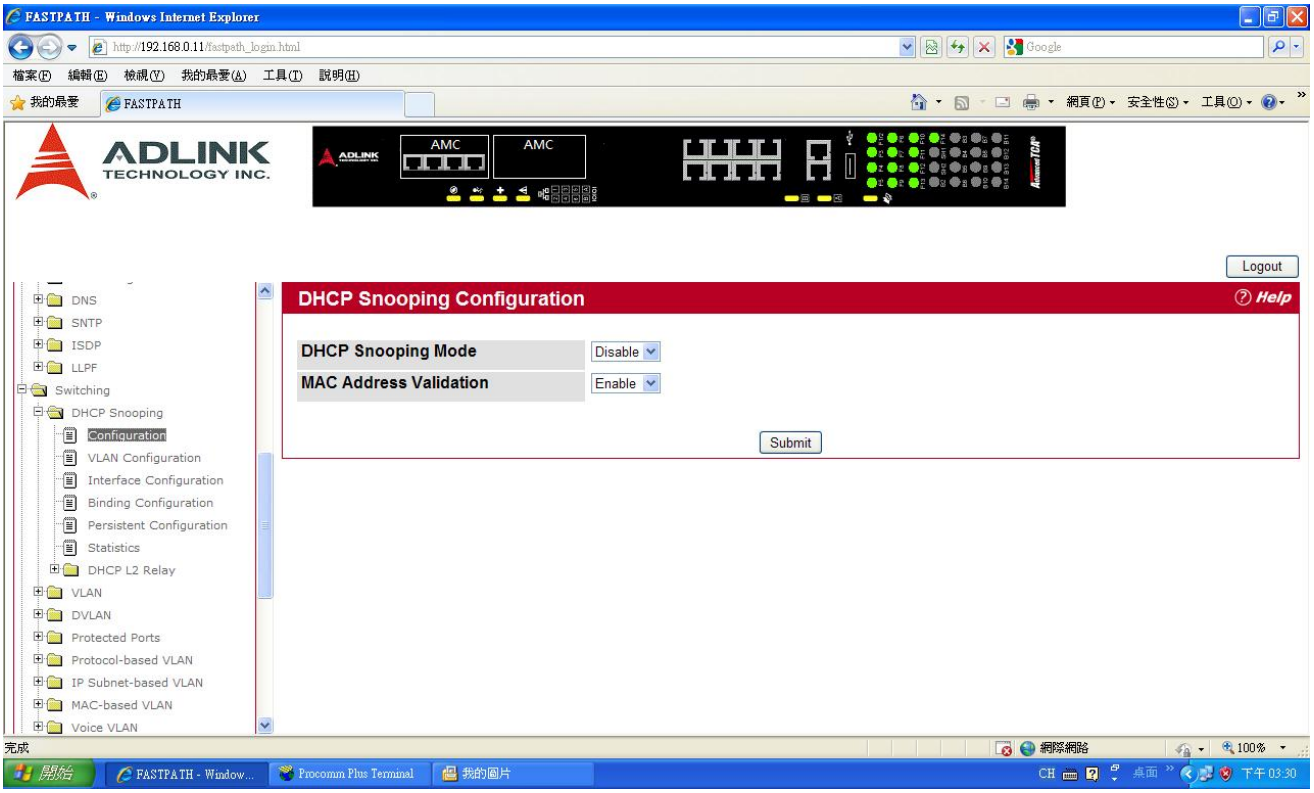
DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized. You can enable DHCP snooping globally and on specific 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 (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped if received on an untrusted port.
- DHCPRELEASE and DHCPDECLINE 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 trusted 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 Switching > DHCP Snooping > Configuration in the navigation tree.



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.

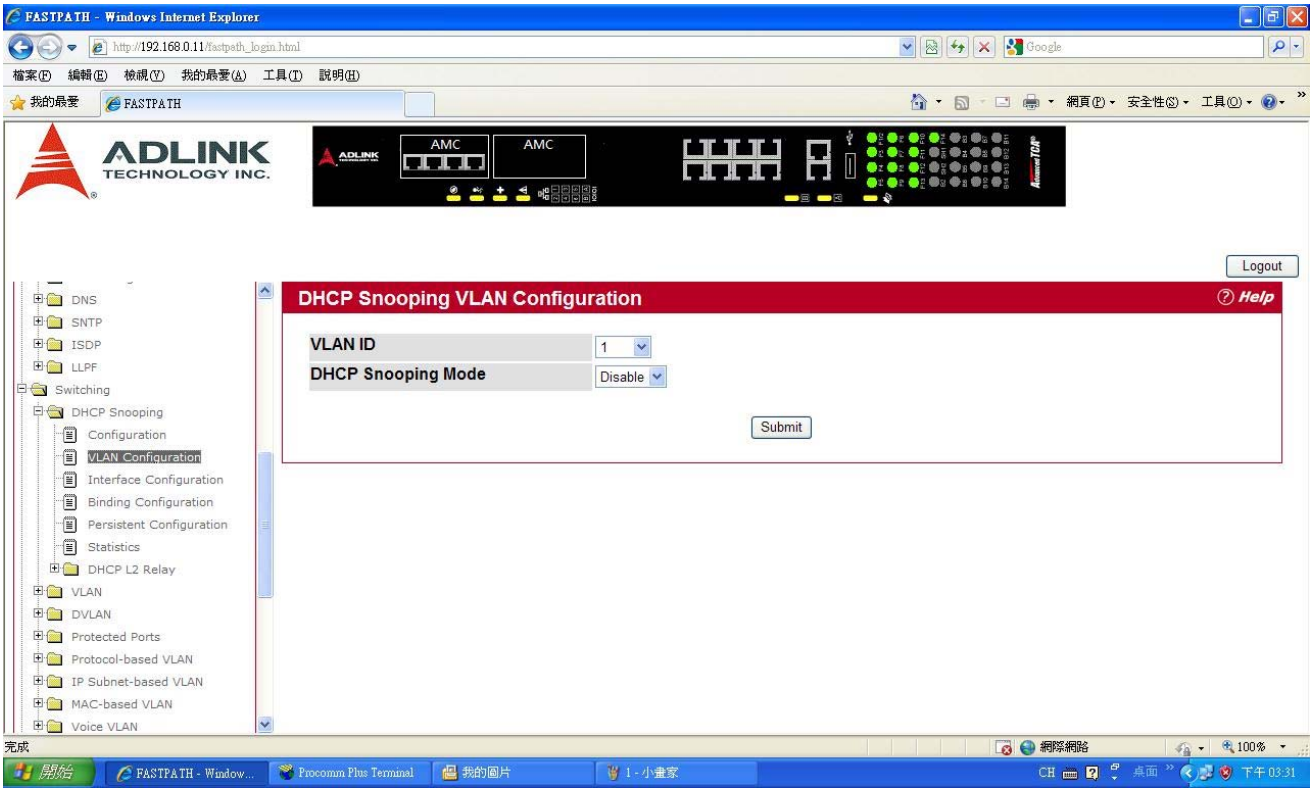
DHCP Snooping VLAN Configuration

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 Switching > DHCP Snooping > VLAN Configuration in the navigation tree.



DHCP Snooping VLAN Configuration

Field	Description
DHCP Snooping Mode	Select the VLAN for which information to be displayed or configured for the DHCP snooping application.
VLAN ID	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.

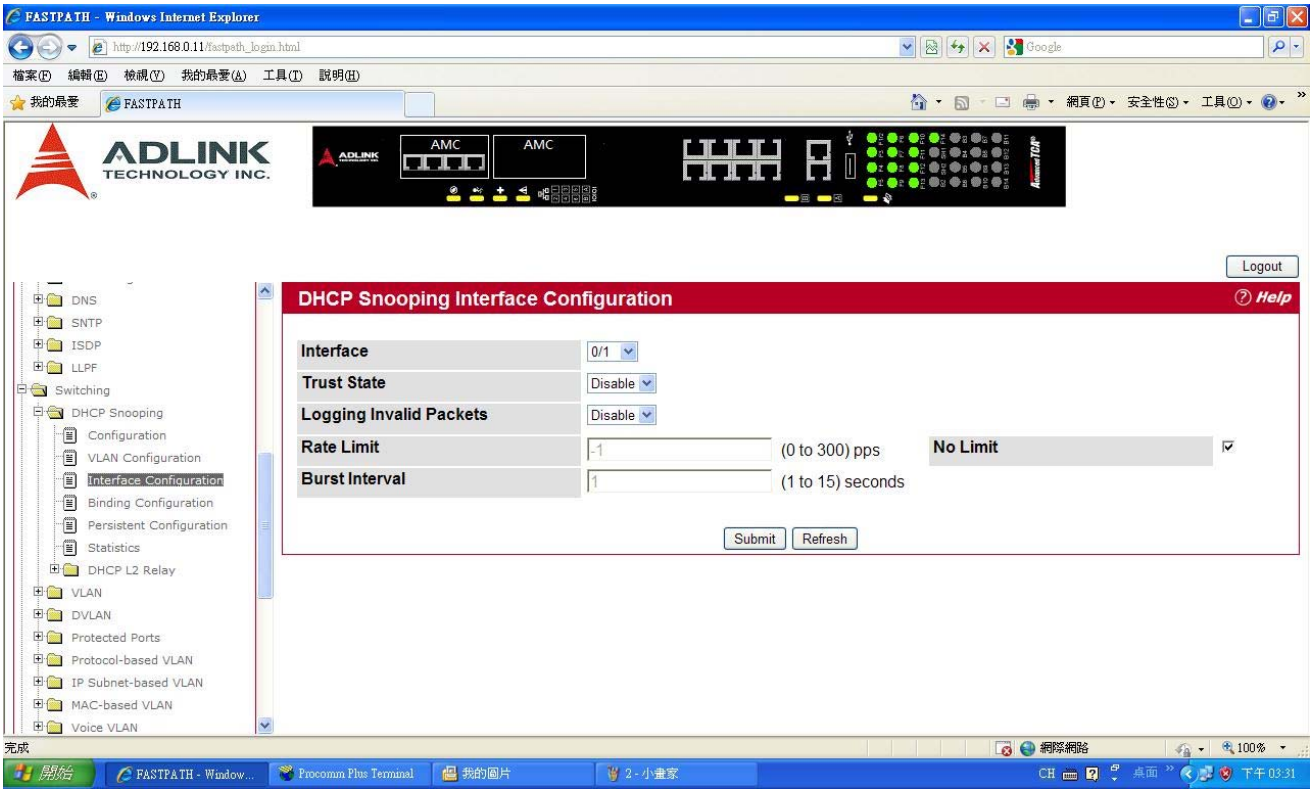
DHCP Snooping Interface Configuration

The hardware rate limits DHCP packets sent to the CPU from untrusted interfaces to 64 kbps. 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 107 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 Switching > DHCP Snooping > Interface Configuration in the navigation tree.



Field	Description
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.

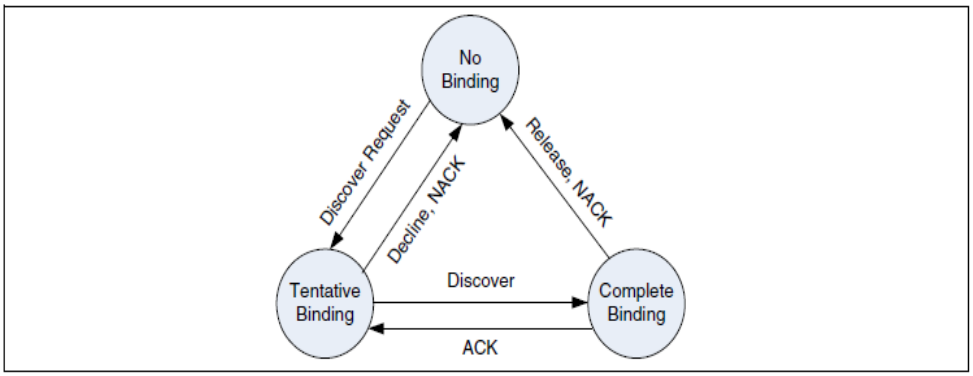
DHCP Snooping Binding Configuration

The DHCP snooping application uses DHCP messages to build and maintain the binding's database. The binding's database only includes data for clients on untrusted ports. DHCP snooping creates a tentative binding from DHCP DISCOVER and REQUEST messages. Tentative bindings tie a client to a port (the port where the DHCP client message was received). Tentative bindings are completed when DHCP snooping learns the client's IP address from a DHCP ACK message on a trusted port. DHCP snooping removes bindings in response to DECLINE, RELEASE, and NACK messages. The DHCP snooping application ignores the ACK messages as a reply to the DHCP Inform messages received on trusted ports. You can also enter static bindings into the binding database.

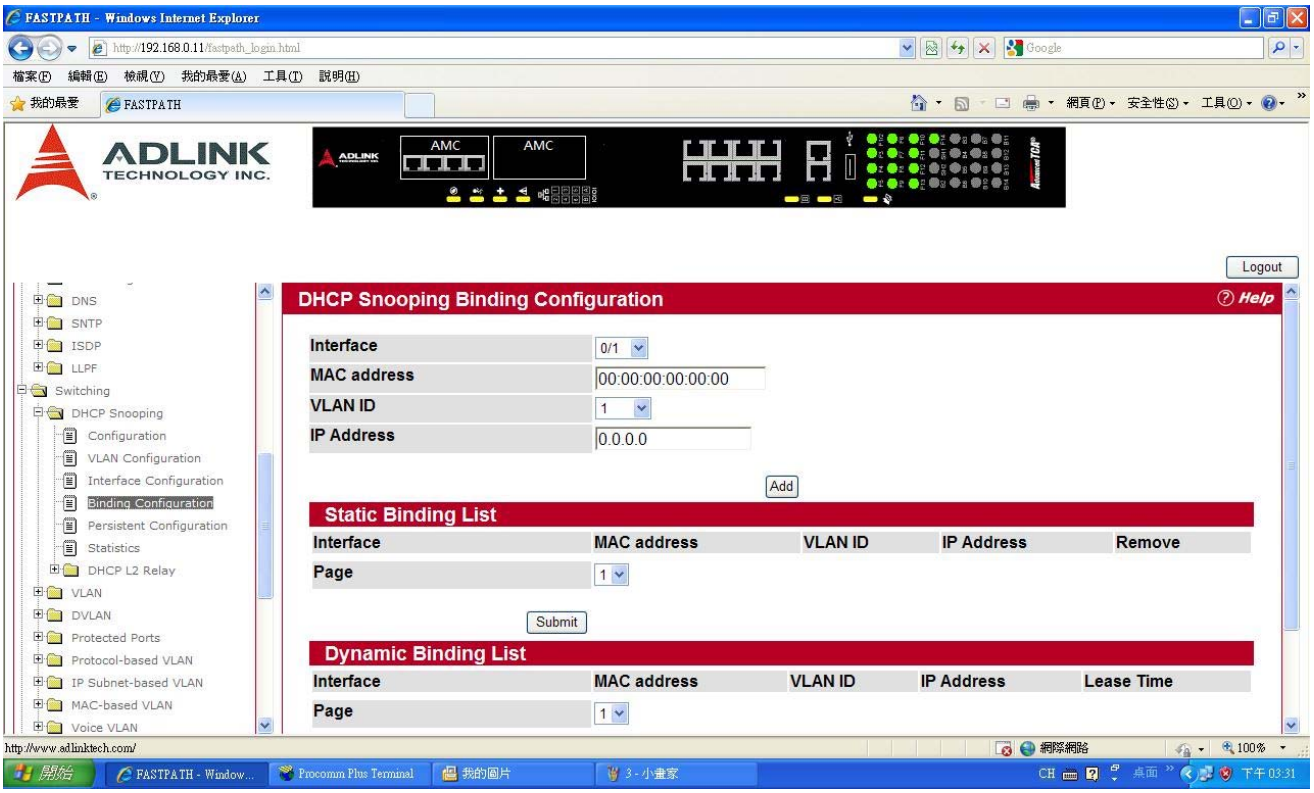
The DHCP binding database is persisted on a configured external server or locally in flash, depending on the user configuration. A row wise checksum is placed in the text file that is going to be stored in the remote configured server. On reloading, the switch reads the configured binding file to build the DHCP snooping database. When the switch starts and the calculated checksum value equals the stored checksum, the switch reads entries from the binding file and populates the binding database. A checksum failure or a connection problem to the external configured server will cause the switch to loose the bindings and will cause a host's data loss if IP Source Guard (IPSG) and/or DAI is enabled.

When a switch learns of new bindings or when it loses bindings, the switch immediately updates the entries in the database. The switch also updates the entries in the binding file. The frequency at which the file is updated is based on a configurable delay, and the updates are batched.

If the absolute lease time of the snooping database entry expires, that entry is removed. You should take care of the system time to be consistent across the reboots. Otherwise, the snooping entries will not expire properly. If a host sends a DHCP release while the switch is rebooting, when the switch receives the DHCP discovery or request, the client's binding goes to the tentative binding as shown in Figure below.



To access the DHCP Snooping Static Binding Configuration page, click Switching > DHCP Snooping > Binding Configuration in the navigation tree.



Field	Description
Interface	Select the interface to add a binding into the DHCP snooping database.
MAC Address	Specify the MAC address for the binding to be added. This is the Key to the binding database.
VLAN ID	Select the VLAN from the list for the binding rule. The range of the VLAN ID is 1 to 4093.
IP Address	Specify a valid IP address for the binding rule.

The DHCP snooping static binding list lists all the DHCP snooping static binding entries page by page. For example, Page 1 displays the first 15 available static entries. Page 2 displays the next 15 available static entries.

DHCP Snooping Static Binding List

Field	Description
Interface	Displays the interface.
MAC Address	Displays the MAC address.
VLAN ID	Displays the VLAN ID .
IP Address	Displays the IP address.
Remove	Select this to remove the particular binding entry.
Page	Lists the number of pages the static binding entries occupy. Select the Page Number from this list to display the particular Page entries.

The DHCP snooping dynamic binding list lists all the DHCP snooping dynamic binding entries page by

page. For example, Page 1 displays the first 15 available dynamic entries. Page 2 displays the next 15 available dynamic entries.

DHCP Snooping Dynamic Binding List

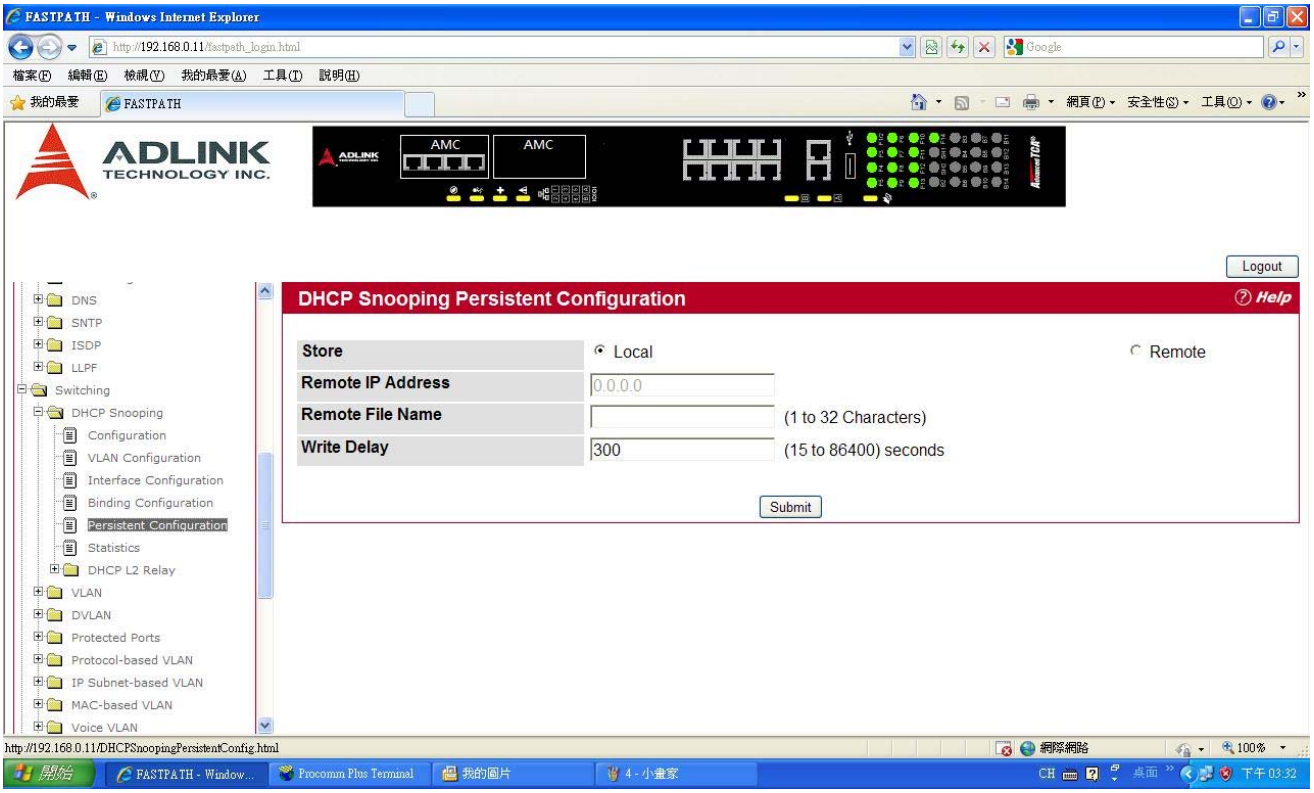
Field	Description
Interface	Displays the interface.
MAC Address	Displays the MAC address.
VLAN ID	Displays the VLAN ID.
IP Address	Displays the IP address.
Lease Time	Displays the remaining Lease time for the dynamic entries.
Page	Lists the number of pages the static binding entries occupy. Select the Page Number

- Click Add to add a DHCP snooping binding entry into the database.
- 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 Clear All to delete all DHCP snooping binding entries.
- Click Refresh to refresh the page with the most current data from the switch.

DHCP Snooping Persistent Configuration

Use the DHCP Snooping Persistent Configuration page to configure the persistent location of the DHCP snooping database. This location can be local or remote on a given IP machine.

To access the DHCP Snooping Persistent Configuration page, click Switching > DHCP Snooping > Persistent Configuration in the navigation tree.



DHCP Snooping Persistent Configuration

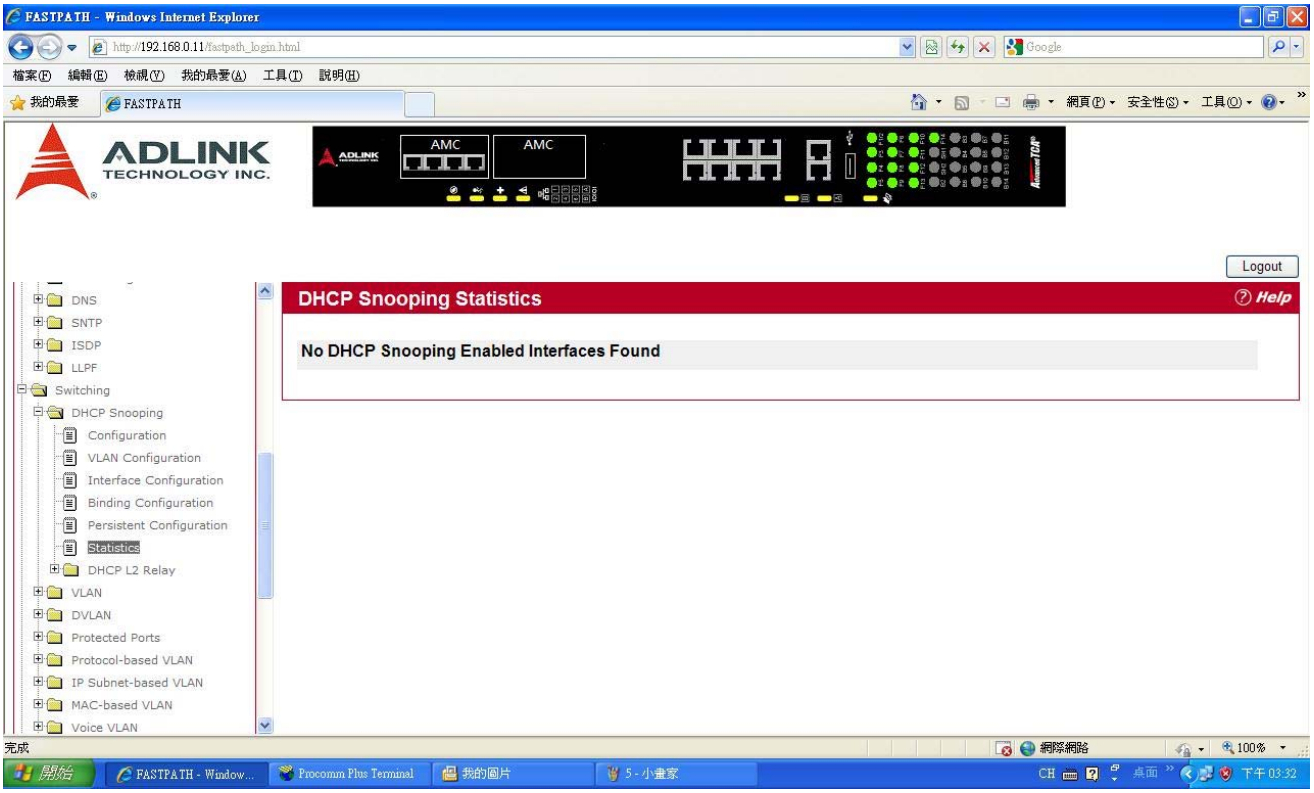
Field	Description
Store Locally	• Local: Select the Local check box to store the DHCP binding database in the flash memory on the switch • Remote: Check the Remote check box to store the DHCP binding database on a remote server.
Remote IP Address	Enter the Remote IP address on which the snooping database will be stored when the Remote check box is selected.
Remote File Name	Enter the Remote filename to store the database when the Remote check box is selected.
Write Delay	Enter the maximum write time to write the database into local or remote. The write delay range is 15 to 86400 seconds.

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 Statistics

The DHCP Snooping Statistics page displays DHCP snooping interface statistics.

To access the DHCP Snooping Statistics page, click Switching > DHCP Snooping > Statistics in the navigation tree.



Field	Description
Interface	Select the untrusted and snooping-enabled interface for which statistics are to be displayed.
MAC Verify Failures	The number of packets that were dropped by DHCP snooping because there is no matching DHCP snooping binding entry found.
Client Ifc Mismatch	The number of DHCP messages that are dropped based on the source MAC address and client hardware address verification.
DHCP Server Msgs Received	The number of server messages that are dropped on an untrusted port.

Click the Clear Stats to clear all interface statistics.

Configuring DHCP L2 Relay

When a DHCP client and server are in the same IP subnet, they can directly connect to exchange IP address requests and replies. However, having a DHCP server on each subnet can be expensive in and is often impractical. Alternatively, network infrastructure devices can be used to relay packets between a DHCP client and server on different subnets. Such a device, a Layer 3 Relay agent, is generally a router that has IP interfaces on both the client and server subnets and can route between them. However, in Layer 2 switched networks, there may be one or more infrastructure devices (for example, a switch) between the client and the L3 Relay agent/DHCP server. In this instance, some of the client device information required by the L3 Relay agent may not be visible to it. In this case, an L2 Relay agent can be used to add the information that the L3 Relay Agent and DHCP server need to perform their roles in address and configuration and assignment.

Before it relays DHCP requests from clients, the switch can add a Circuit ID and a Remote ID. These provide information about the circuit and port number connected to the client. This information is added as suboptions in the DHCP Option 82 packets (see sections 3.1 and 3.2 of RFC3046). The switch removes this option from packets that it relays from L3 Relay agents/DHCP servers to clients.

These sub-options may be used by the DHCP server to affect how it treats the client, and also may be used by the relay agent to limit broadcast replies to the specific circuit or attachment point of the client.

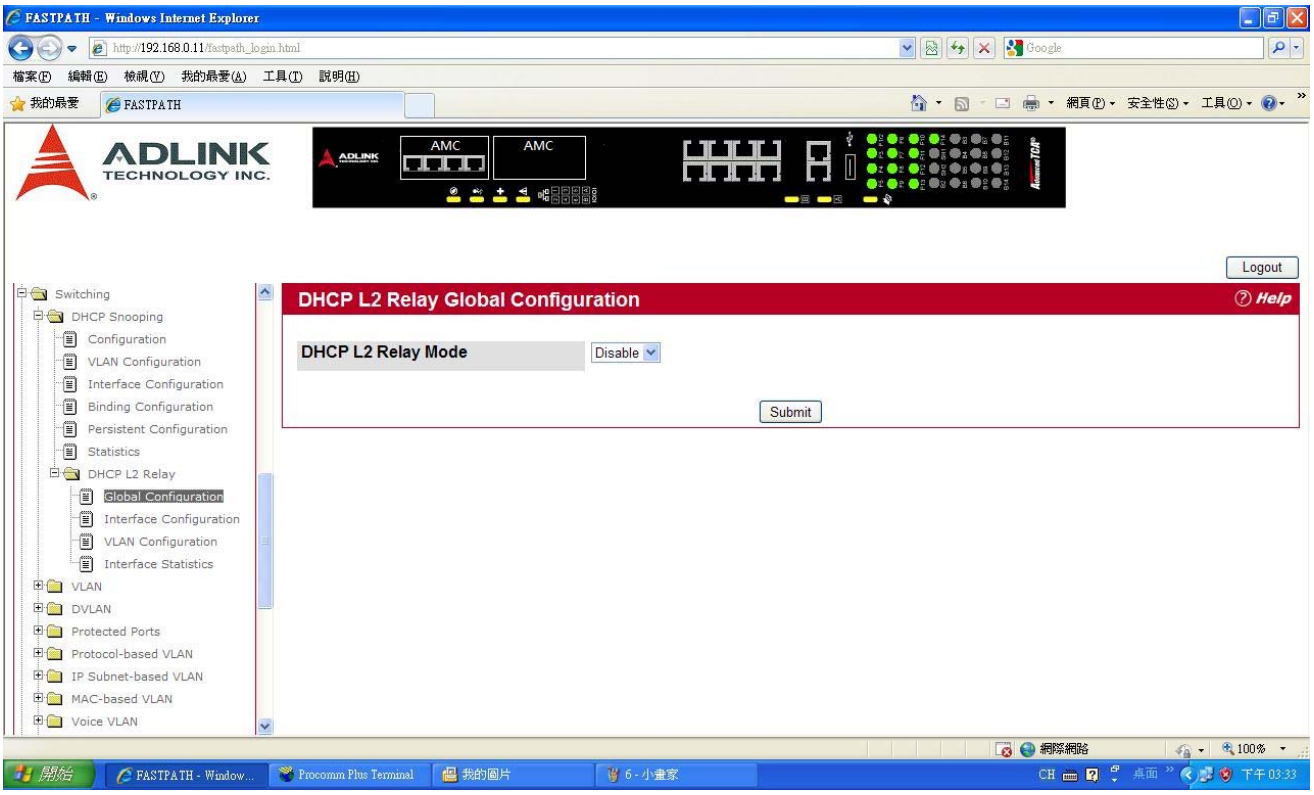
The Switching > DHCP Snooping > DHCP L2 Relay folder provides access to the following pages:

- DHCP L2 Relay Global Configuration
- DHCP L2 Relay Interface Configuration
- DHCP L2 Relay VLAN Configuration
- DHCP L2 Relay Interface Statistics

DHCP L2 Relay Global Configuration

Use this page to enable or disable the switch to act as a DHCP L2 relay agent. This functionality must also be enabled on each port you want this service to operate on (see “DHCP L2 Relay Interface Configuration”). The switch can also be configured to relay requests only when the VLAN of the requesting client corresponds to a service provider’s VLAN ID that has been enabled with the L2 DHCP relay functionality (see “DHCHP L2 Relay VLAN Configuration”).

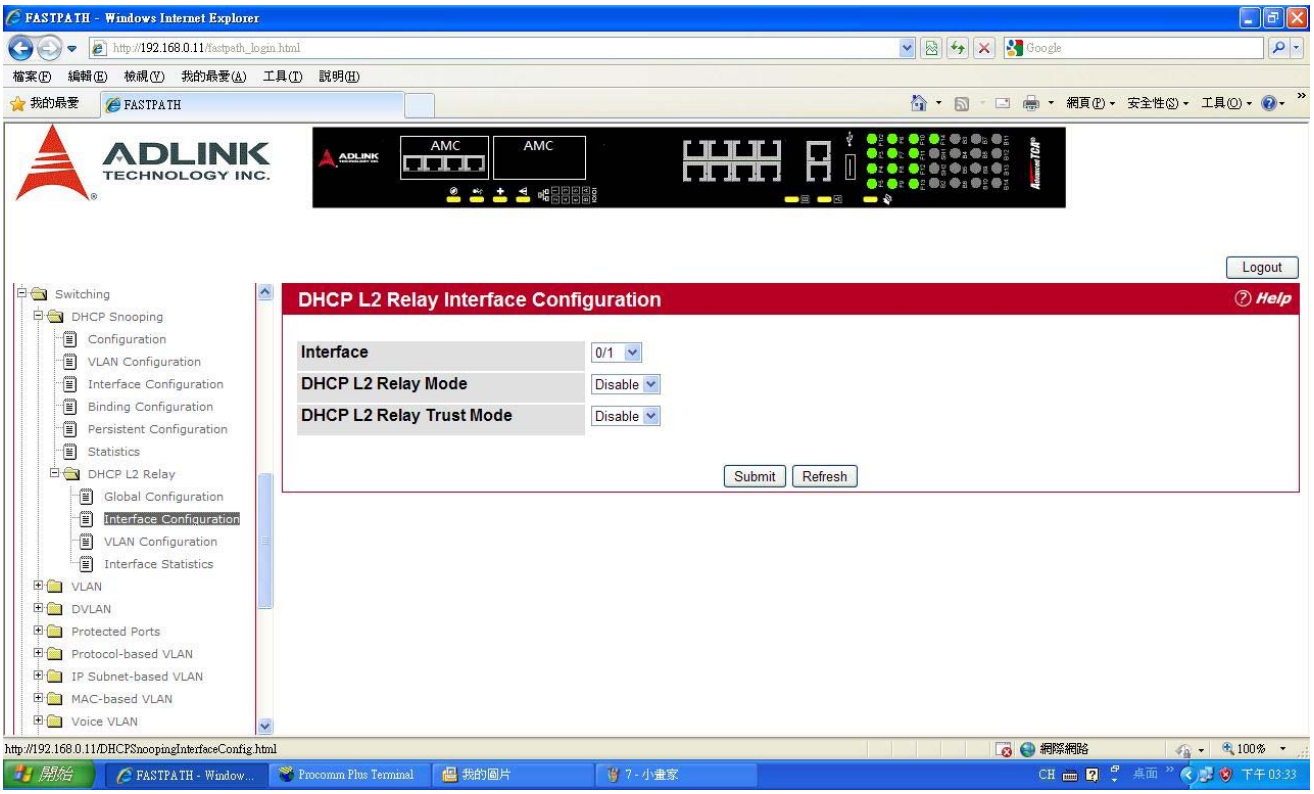
To access this page, click Switching > DHCP Snooping > DHCP L2 Relay > Global Configuration.



If you enable or disable this feature, click Submit to apply the changes to system.

DHCP L2 Relay Interface Configuration

Use this page to enable L2 DHCP relay on individual ports. Note that L2 DHCP relay must also be enabled globally on the switch. To access this page, click Switching > DHCP Snooping > DHCP L2 Relay > Interface Configuration.



DHCP L2 Relay Interface Configuration

Field	Description
Interface	Select the slot/port to configure this feature on.
DHCP L2 Relay Mode	Enable or disable L2 Relay mode on the selected interface.
DHCP L2 Relay Trust Mode	Enable or disable L2 Relay Trust Mode on the selected interface. Trusted interfaces usually connect to other agents or servers participating in the DHCP interaction (e.g. other L2 or L3 Relay Agents or Servers). When enabled in Trust Mode, the interface always expects to receive DHCP packets that include Option 82 information. If Option 82 information is not included, these packets are discarded. Untrusted interfaces are generally connected to clients. DHCP packets arriving on an untrusted interface are never expected to carry Option 82 and are discarded if they do.

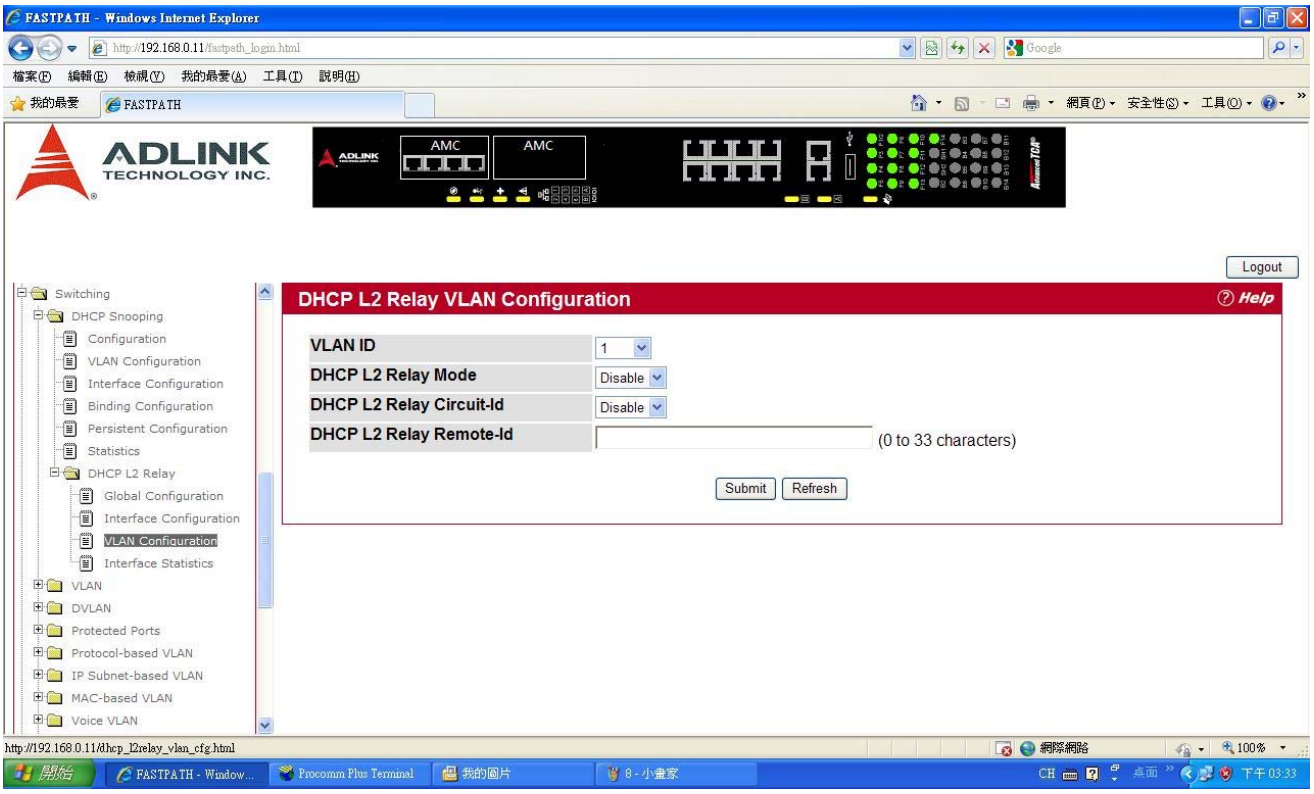
If you change any settings on this page, click Submit to apply the changes to system.

DHCP L2 Relay VLAN Configuration

You can enable L2 DHCP relay on a particular VLAN. The VLAN is identified by a service VLAN ID (S-VID), which a service provider uses to identify a customer's traffic while traversing the provider network to multiple remote sites. The switch uses the VLAN membership of the switch port client (the customer VLAN ID, or C-VID) to perform a lookup a corresponding S-VID.

If the S-VID is enabled for DHCP L2 Relay, the packet can be forwarded. If the C-VID does not correspond to an S-VID that is enabled for DHCP L2 relay, the switch will not relay the DHCP request packet.

To access this page, click Switching > DHCP Snooping > DHCP L2 Relay > VLAN Configuration.



DHCP L2 Relay VLAN Configuration

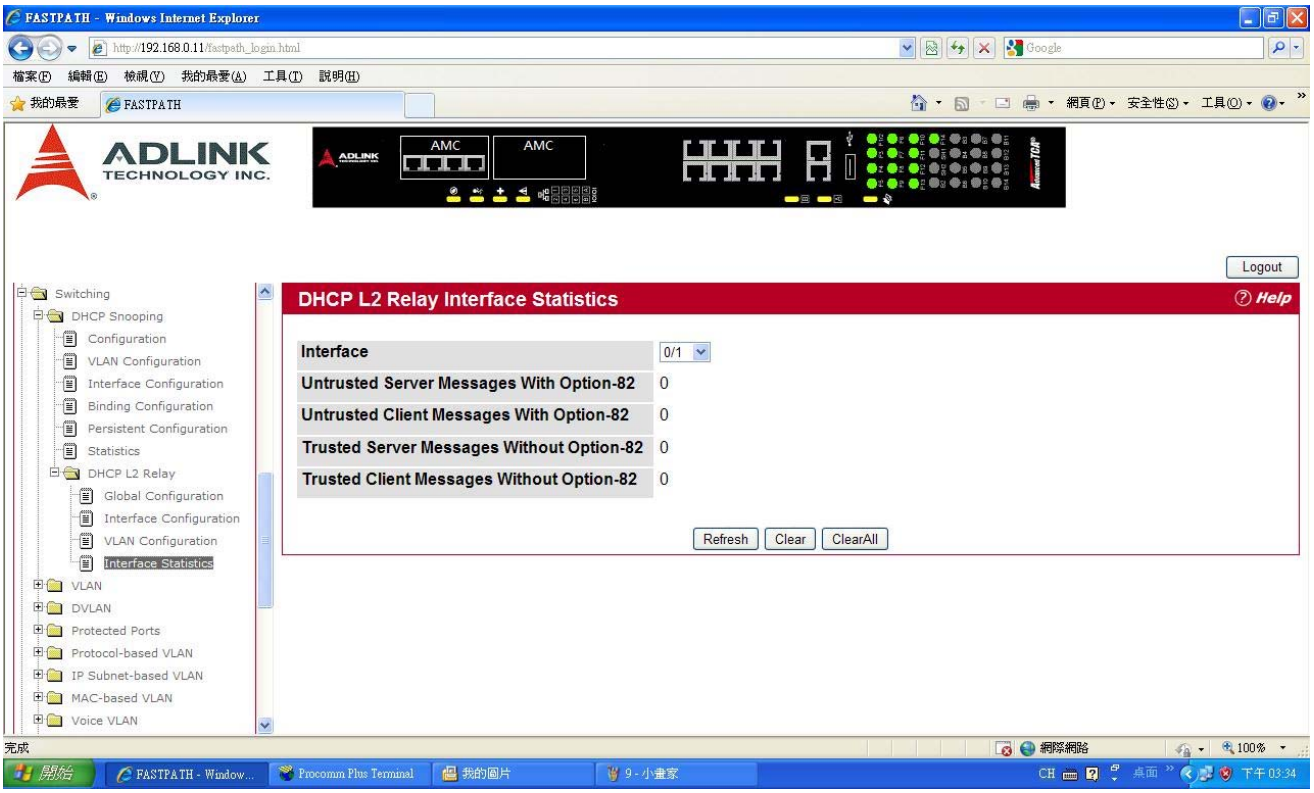
Field	Description
VLAN ID	Select a VLAN ID from the list for configuration. This is an S-VID (as indicated by the service provider) that identifies a VLAN that is authorized to relay DHCP packets through the provider network.
DHCP L2 Relay Mode	Enable or disable the selected VLAN for DHCP L2 relay services.
DHCP L2 Relay Circuit-Id	When enabled, if a client sends a DHCP request to the switch and the client is in a VLAN that corresponds to the selected S-VID, the switch adds the client's interface number to the Circuit ID sub-option of Option 82 in the DHCP request packet. This enables the switch to reduce the broadcast domain to which the

Field	Description
	server replies are switched when the broadcast bit is set for DHCP packets. When this bit is set, the server is required to echo the Option-82 in replies. Since the circuit-id field contains the client interface number, the L2 relay agent can forward the response to the requesting interface only, rather to all ports in the VLAN).
DHCP L2 Relay Remote-Id	When a string is entered here, if a client sends a DHCP request to the switch and the client is in a VLAN that corresponds to the selected S-VID, the switch adds the string to the Remote-ID sub-option of Option 82 in the DHCP request packet. This sub-option can be used by the server for parameter assignment. The content of this option is vendor-specific.

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

DHCP L2 Relay Interface Statistics

Use this page to display statistics on L2 DHCP Relay requests received on a selected port. To access this page, click Switching > DHCP Snooping > DHCP L2 Relay > Interface Statistics.



DHCP L2 Relay Interface Statistics

Field	Description
Interface	Select the slot/port to configure this feature on.
Untrusted Server Msgs With Option—82	If the selected interface is configured in untrusted mode, this field shows the number of messages received on the interface from a DHCP server that contained Option 82 data.These messages are dropped.
Untrusted Client Msgs With Option—82	If the selected interface is configured in untrusted mode, this field shows the number of messages received on the interface from a DHCP client that contained Option 82 data.These messages are dropped.
Trusted Server Msgs Without Option—82	If the selected interface is configured in trusted mode, this field shows the number of messages received on the interface from a DHCP server that did not contain Option 82 data. These messages are dropped.
Trusted Client Msgs Without Option—82	If the selected interface is configured in trusted mode, this field shows the number of messages received on the interface from a DHCP client that did not contain Option 82 data. These messages are dropped.

Click Refresh to redisplay the page with the latest information from the switch.

Click Clear to set statistics for this port to their initial values.

Click Clear All to set statistics for all ports to their initial values.

5.7 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.

The VLAN folder contains links to the following features:

- VLAN Configuration
- VLAN Status
- VLAN Port Configuration
- VLAN Port Summary
- Reset VLAN Configuration

VLAN Configuration

Use the VLAN Configuration page to define VLAN groups stored in the VLAN membership table. Your switch supports up to 4093 VLANs. VLAN 1 is the default VLAN of which all ports are members.

To display the VLAN Configuration page, click Switching > VLAN > Configuration in the navigation tree.



VLAN Configuration Fields

Field	Description
VLAN ID List	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/Range	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 4093).
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.”

Field	Description
Interface	Indicates which port is associated with the fields on this line. For platforms with the stacking package, the field is Interface.
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: • 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.
Tagging	Select the tagging behavior for this port in this VLAN. The factory default is “Untagged.” The possible values are: • 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 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 Switching > VLAN > Status in the navigation tree.



VLAN Status Fields

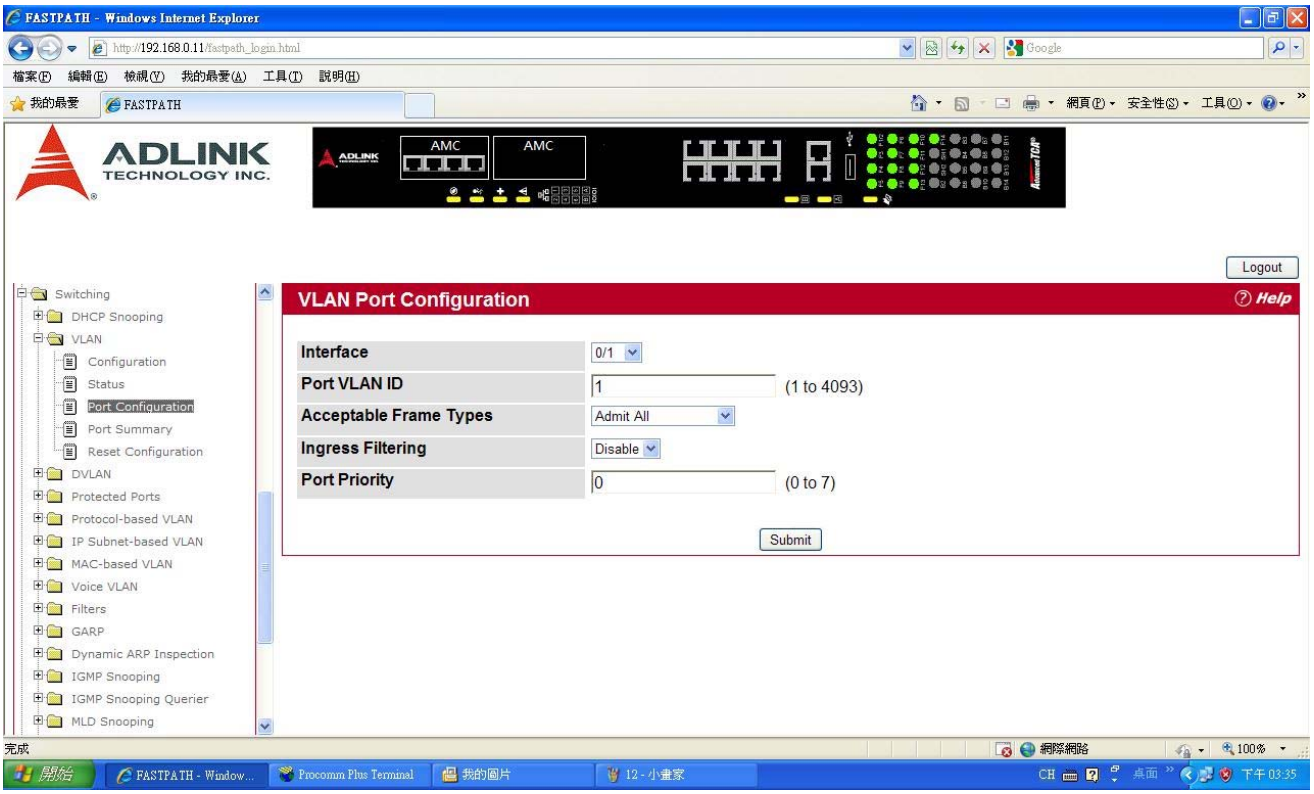
Field	Description
VLAN ID	The VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	The name of the VLAN. VLAN ID 1 is always named Default.
VLAN Type	The VLAN type, which can be one of the following: • Default: (VLAN ID = 1) -- always present • Static: A VLAN you have configured • 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 Switching > VLAN > Port Configuration in the navigation tree.



VLAN Port Configuration 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. For systems with the stacking package installed, the field is Interface.
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. • 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.

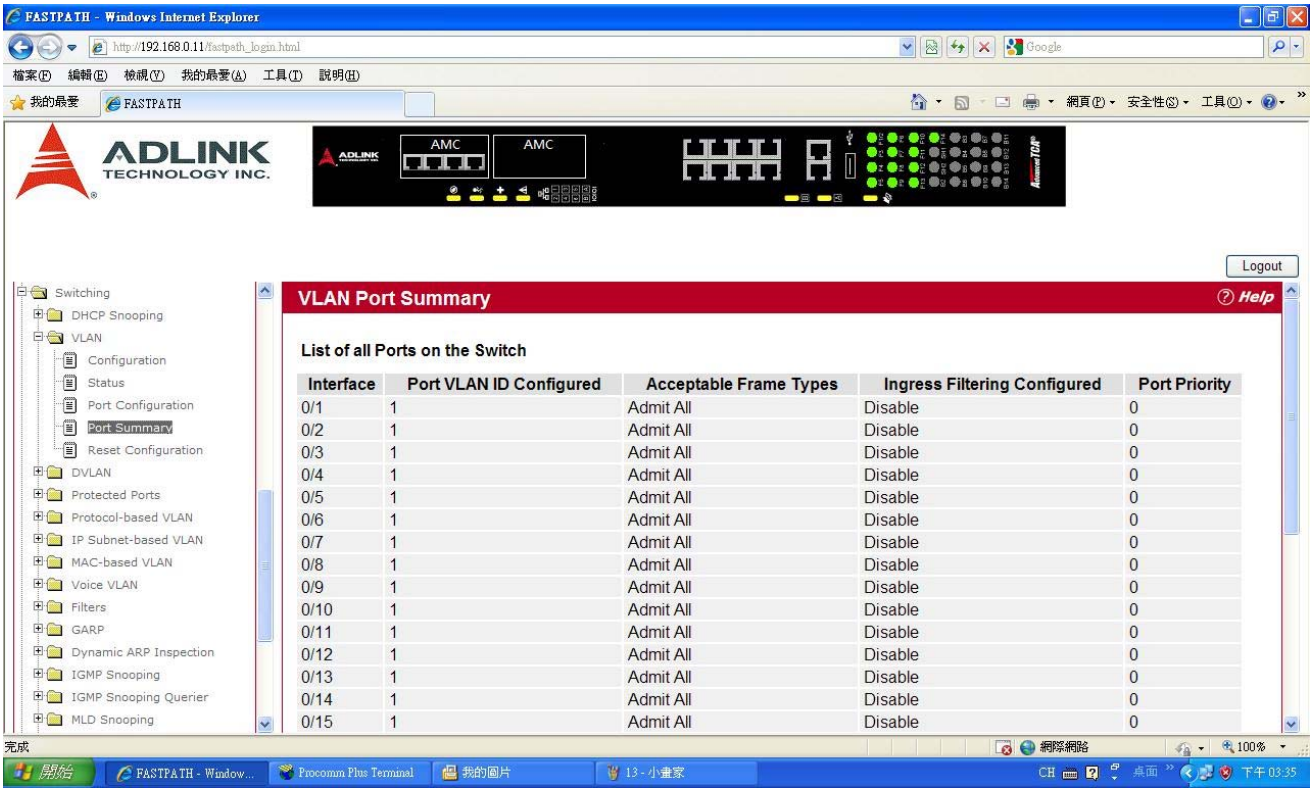
Field	Description
Ingress Filtering	Specify how you want the port to handle tagged frames: • Enable: A tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. • Disable: All tagged frames will be accepted. The factory default is disable.
Port Priority	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 Switching > VLAN > Port Summary in the navigation menu.



Interface	Port VLAN ID Configured	Acceptable Frame Types	Ingress Filtering Configured	Port Priority
0/1	1	Admit All	Disable	0
0/2	1	Admit All	Disable	0
0/3	1	Admit All	Disable	0
0/4	1	Admit All	Disable	0
0/5	1	Admit All	Disable	0
0/6	1	Admit All	Disable	0
0/7	1	Admit All	Disable	0
0/8	1	Admit All	Disable	0
0/9	1	Admit All	Disable	0
0/10	1	Admit All	Disable	0
0/11	1	Admit All	Disable	0
0/12	1	Admit All	Disable	0
0/13	1	Admit All	Disable	0
0/14	1	Admit All	Disable	0
0/15	1	Admit All	Disable	0

VLAN Port Summary Fields

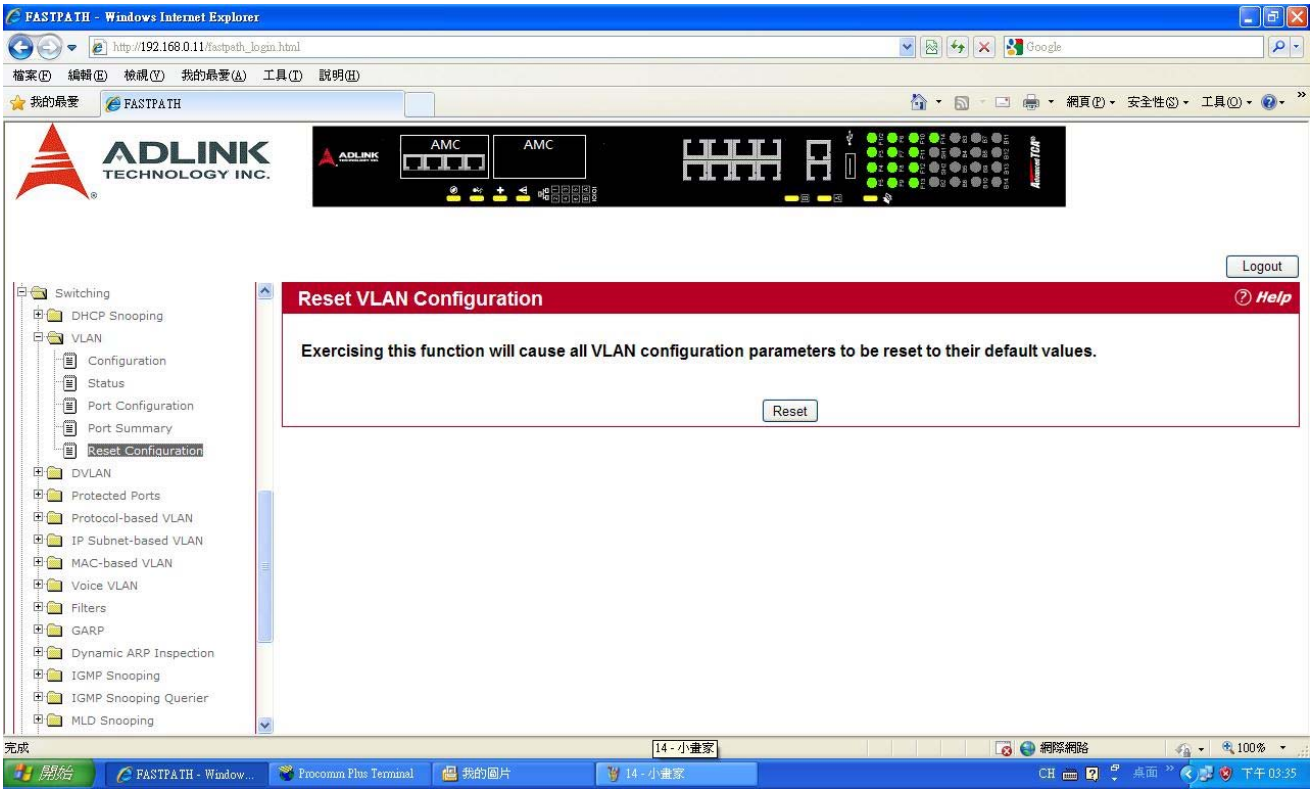
Field	Description
Interface	Identifies the physical interface associated with the rest of the data in the row.
Port VLAN ID Configured	Identifies the VLAN ID assigned to untagged or priority-tagged frames received on this port. The factory default is 1.
Port VLAN ID Current	Displays the actual VLAN ID 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, the two may differ.
Acceptable Frame Types	Indicates how the port handles untagged and priority tagged frames. • 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. • 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.

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 Switching > VLAN > Reset Configuration in the navigation tree.



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.

5.8 Double VLAN (DVLAN) Tunneling

DVLAN 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 DVLAN Tunneling enabled, every frame that is transmitted from an interface has a new VLAN tag (S-tag) attached while every packet that is received from an interface has a VLAN tag (S-tag) removed (if one or more tags are present).

DVLAN also supports up to 4 Tag Protocol Identifier (TPID) values per switch and the ability to map these values to ports. This allows you to configure the same or different TPIDs for different ports.

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

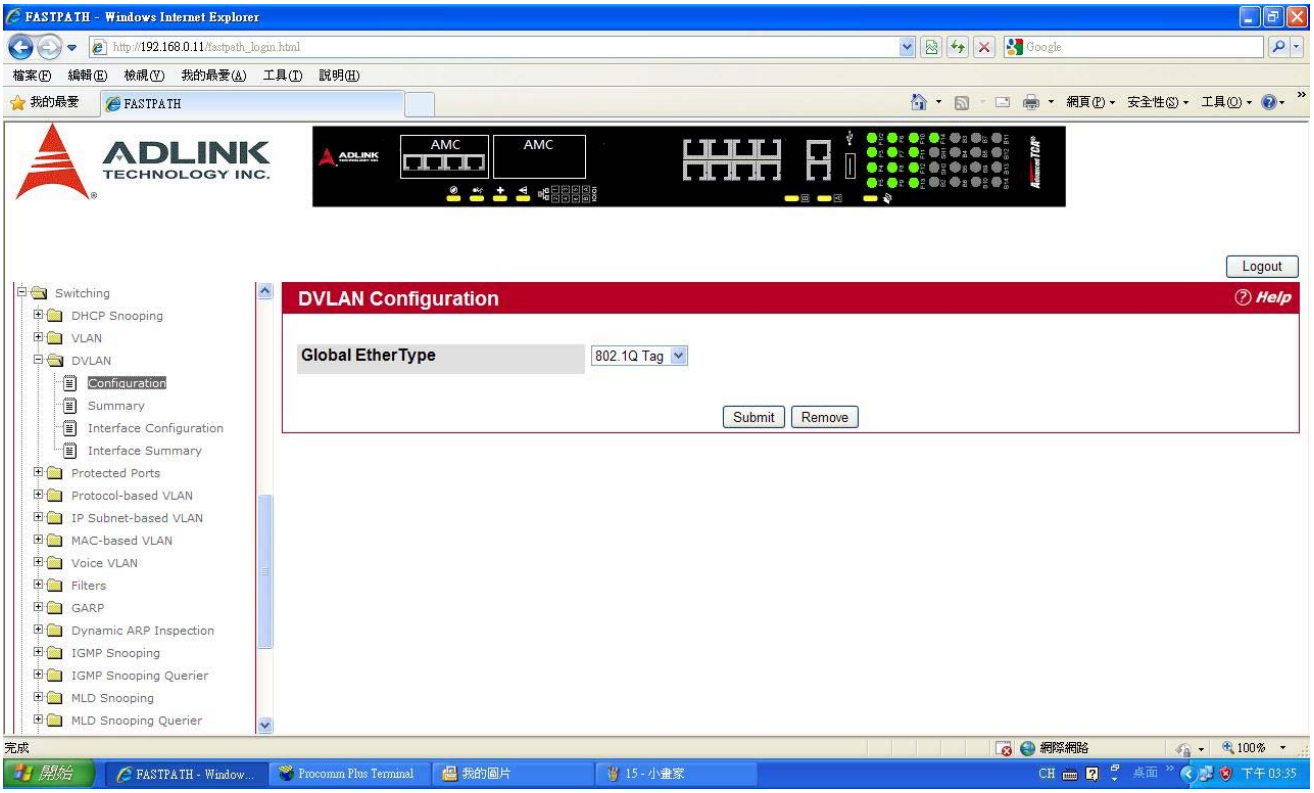
The DVLAN folder contains links to the following features:

- DVLAN Config
- DVLAN Summary
- DVLAN Interface Config
- DVLAN Interface Summary

DVLAN Config

The DVLAN Config page allows you to configure the TPID with an associated Global Ethertype for all ports on the system.

To access the DVLAN Config page, click Switching > DVLAN > Config in the navigation tree.



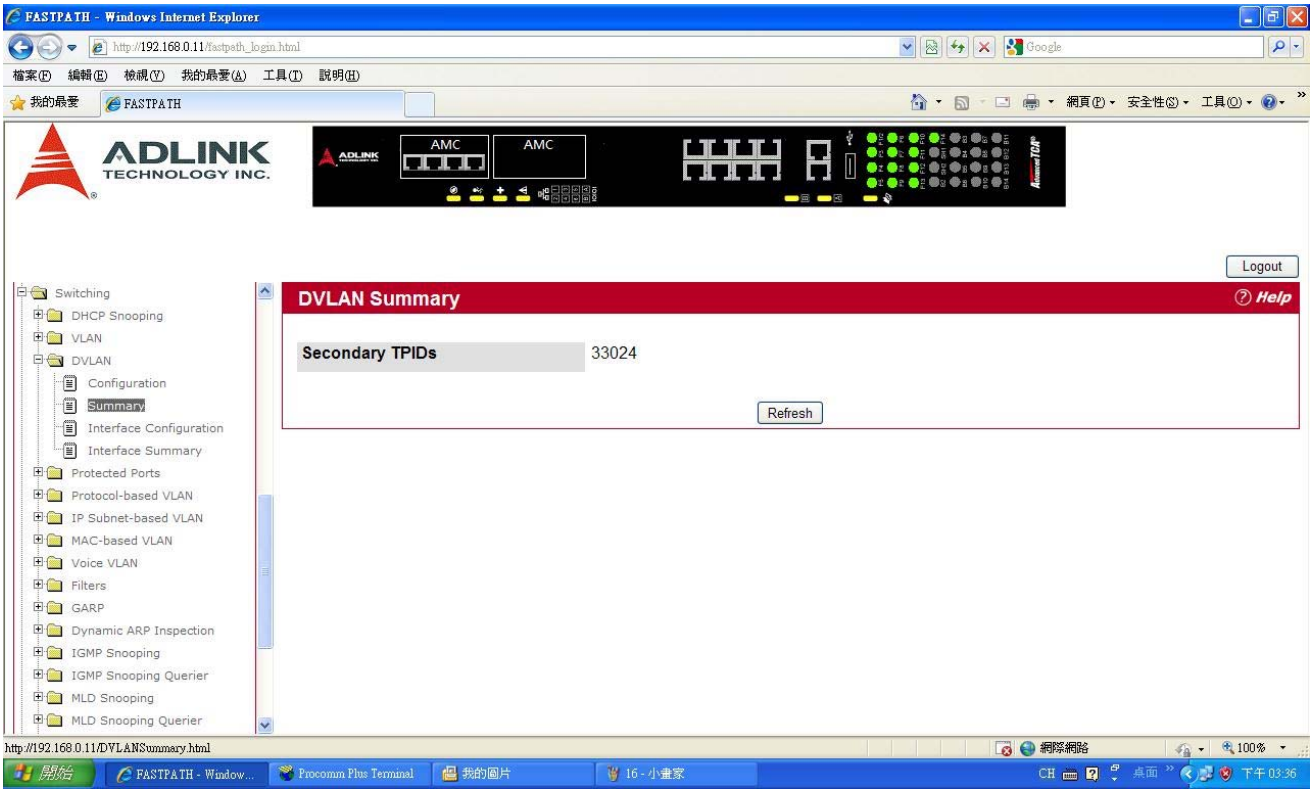
Field	Description
Global EtherType	Specifies one of the following global EtherType options: •802.1Q Tag - Commonly used tag representing 0x8100 •vMAN Tag - Commonly used tag representing 0x88A8 •Custom Tag - Configure the tag for EtherType by providing a custom value in any range from 0 to 65535. The two-byte hex EtherType is used as the first 16 bits of the DVLAN tag.

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

DVLAN Summary

The DVLAN Summary page allows you to view the Global and Default TPIDs configured for all ports on the system.

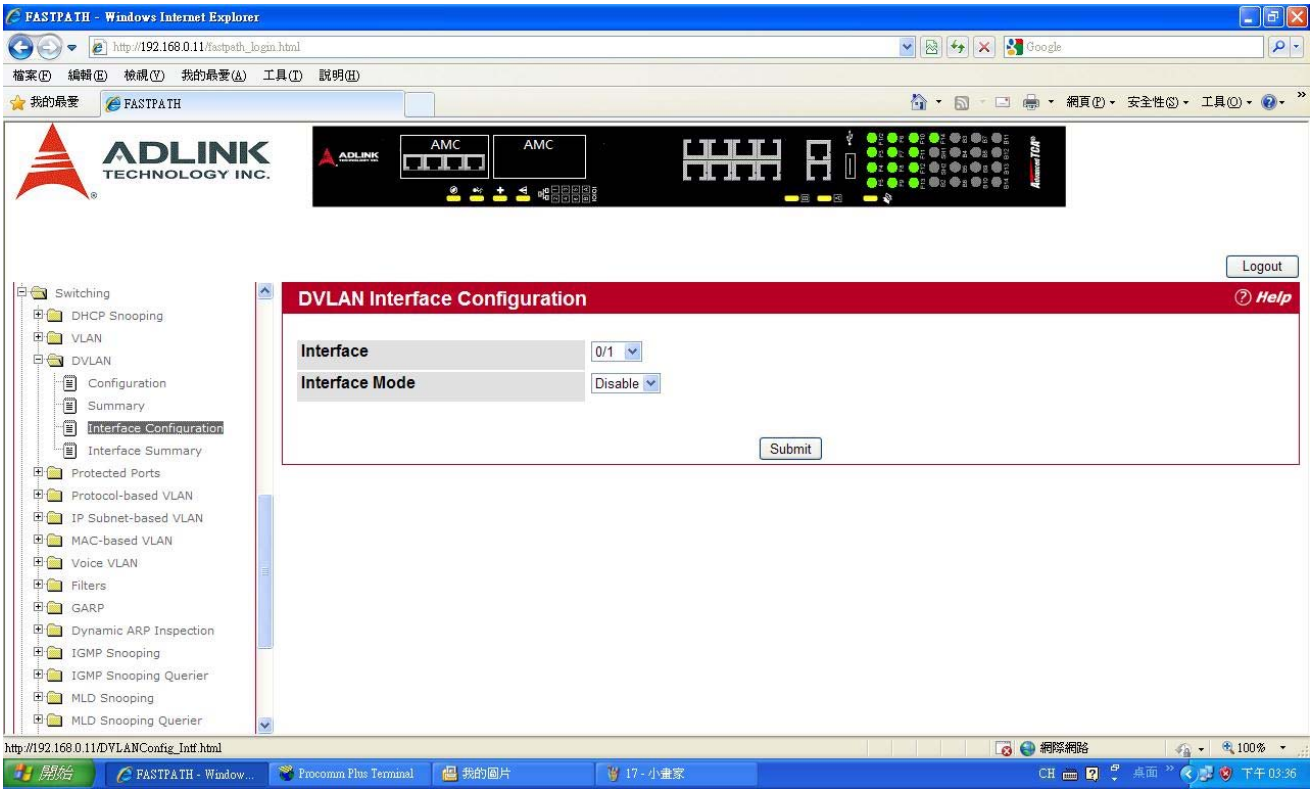
To access the DVLAN Summary page, click Switching > DVLAN > Summary in the navigation tree.



DVLAN Interface Config

The DVLAN Interface Config page allows you to view and configure the DVLAN interface configuration status for all ports on the system.

To access the DVLAN Interface Config page, click Switching > DVLAN > Interface Config in the navigation tree.



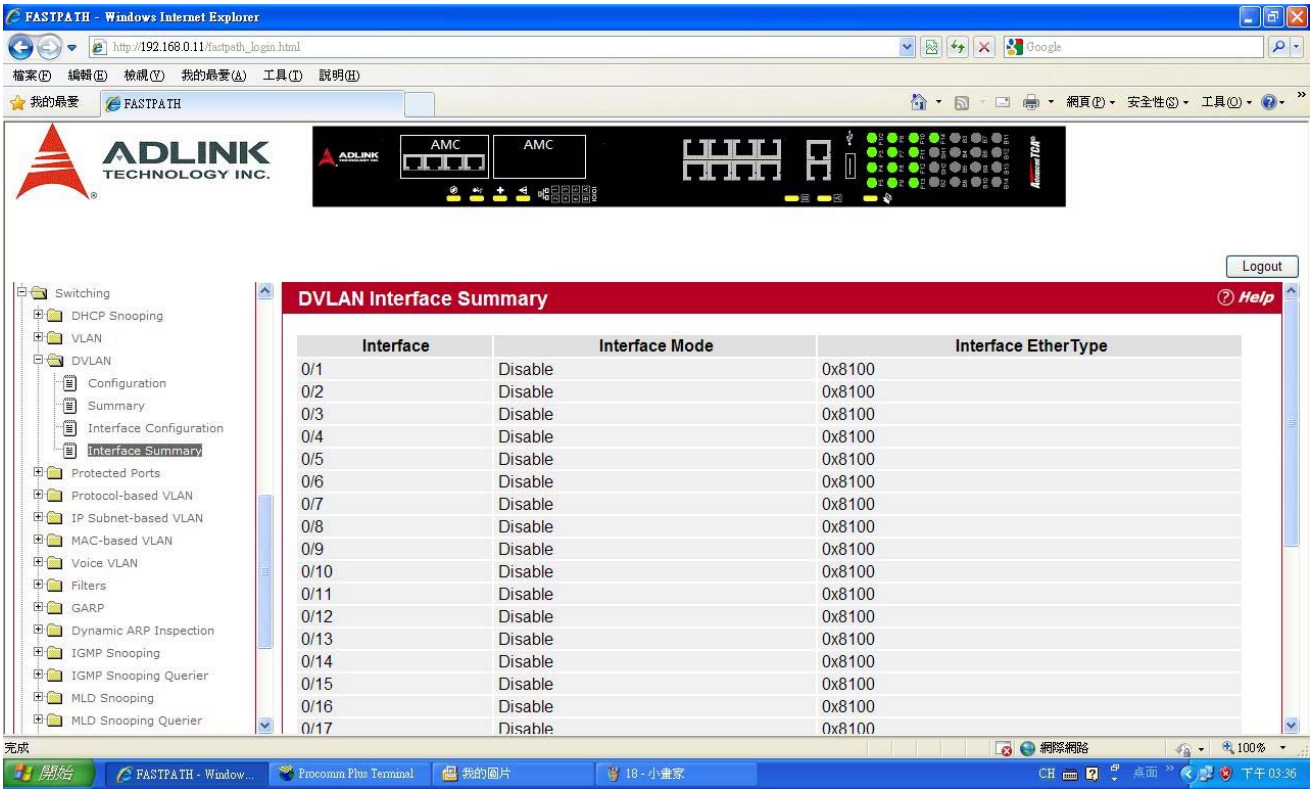
Field	Description
Interface	Select the physical interface for which you want to display or configure data. Select All to set the parameters for all ports to same values.
Interface Mode	This specifies the administrative mode for DVLAN Tagging: • Enable: DVLAN Tagging is enabled for the specified port (or All ports). • Disable: DVLAN Tagging is disabled for the specified port (or All ports), which is the default value.

Click Refresh to redisplay the most current information from the router.

DVLAN Interface Summary

The DVLAN Interface Summary page displays the DVLAN interface configuration status for all ports on the system.

To access the DVLAN Interface Summary page, click Switching > DVLAN > Interface Summary in the navigation tree.



See “DVLAN Interface Config” for a description of these fields.

Click Refresh to redisplay the most current information from the router.

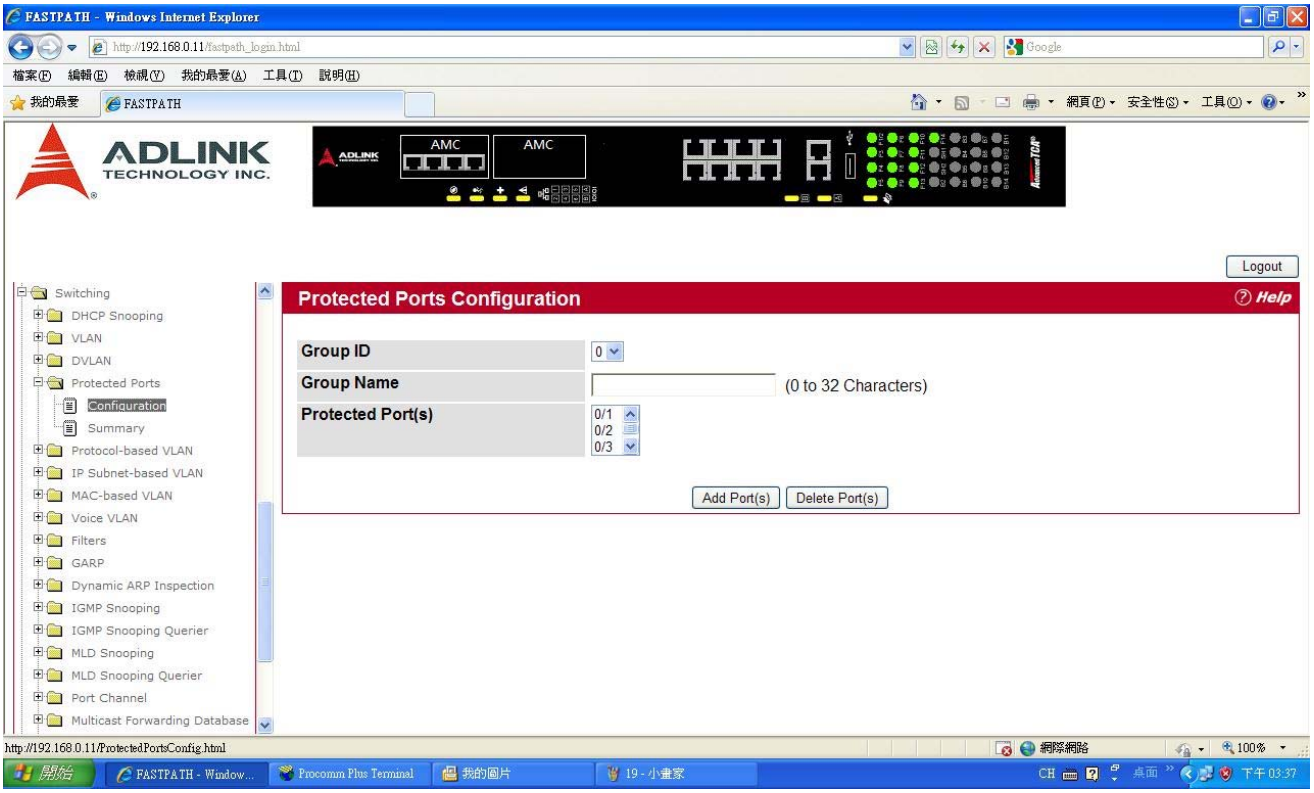
Configuring Protected Ports

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 Switching > Protected Ports > Configuration in the navigation tree.



Field	Description
Group ID	The protected ports can be combined into a logical group. Traffic can flow between protected ports belonging to different groups
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 characters long
Protected Port(s)	Specifies the Slot and Port (non-stacking) or Unit parameters are defined.

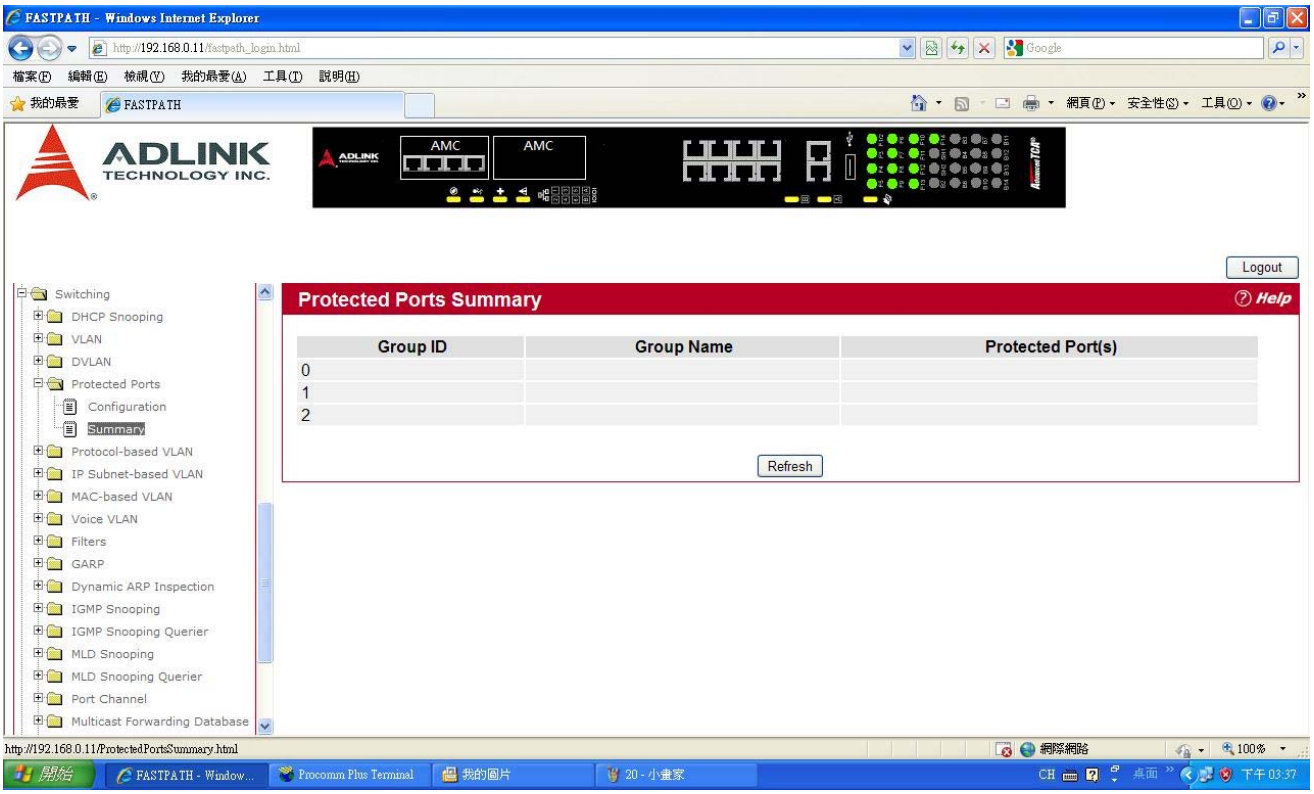
Assigning Ports to a Group

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 Switching > Protected Ports > Summary in the navigation tree.



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 and Port (non-stacking) or Unit, Slot, and Port (stacking) that are members of the protected ports group.

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

5.9 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.

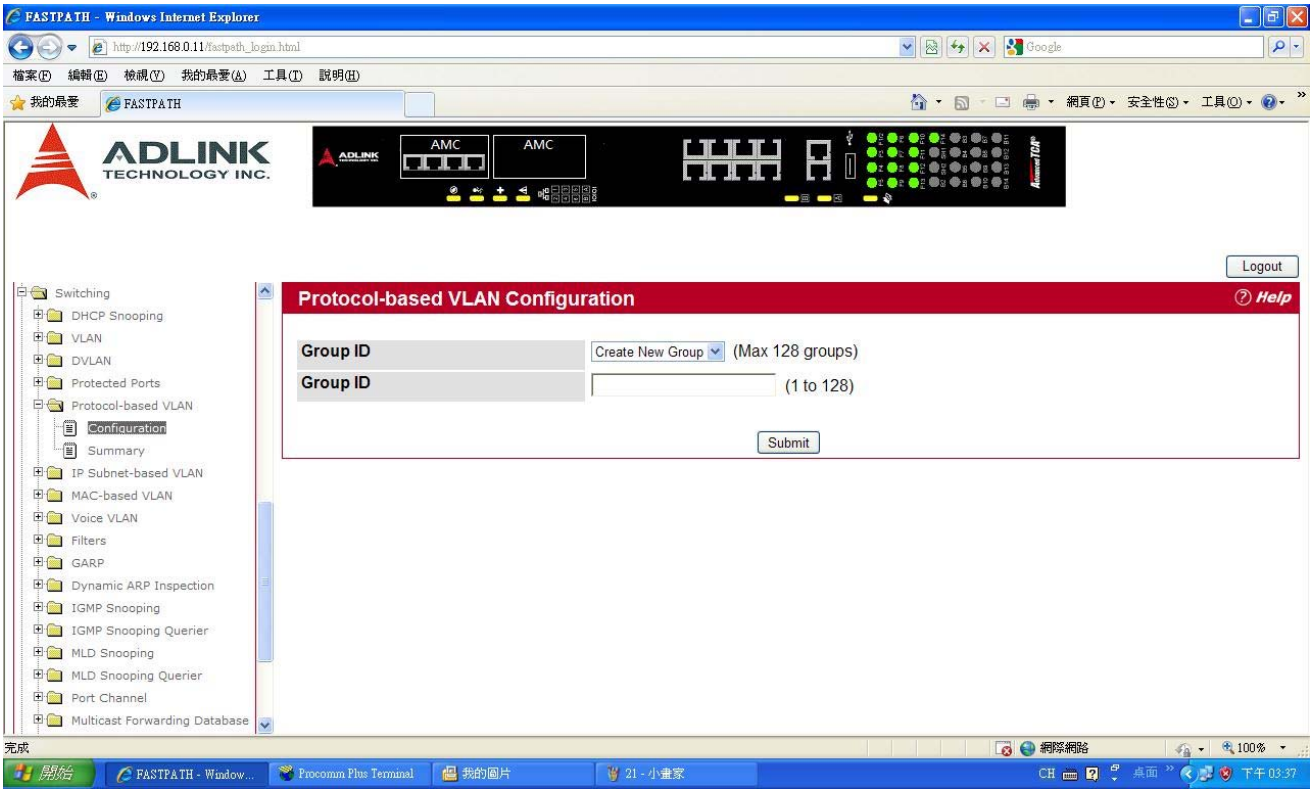
If you assign a port to a protocol-based VLAN for a specific protocol, untagged frames received on that port for that protocol will be assigned the protocol-based VLAN ID. Untagged frames received on the port for other protocols will be assigned the Port VLAN ID (PVID), which is either the default PVID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

Configuration

Use the Protocol-based VLAN Configuration page to configure which protocols go to which VLANs, and 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 (the range is platform-dependent), and can include multiple ports.

To display the Protocol-Based VLAN Configuration page, click Switching > VLAN > Protocol-based VLAN > Configuration in the navigation tree.



Field	Description
Group	Use the drop-down menu to create or modify a protocol group. You can create up to 128 groups.
Group Name	When creating a group, 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.
Group ID	Shows the number that identifies the group you create. Group IDs are automatically assigned when you create a group.
Protocols	Select one or more protocols to associate with this group. CTRL + click to select multiple protocols. • IP: IP is a network layer protocol that provides a connectionless service for the delivery of data. • ARP: Address Resolution Protocol (ARP) is a low-level protocol that

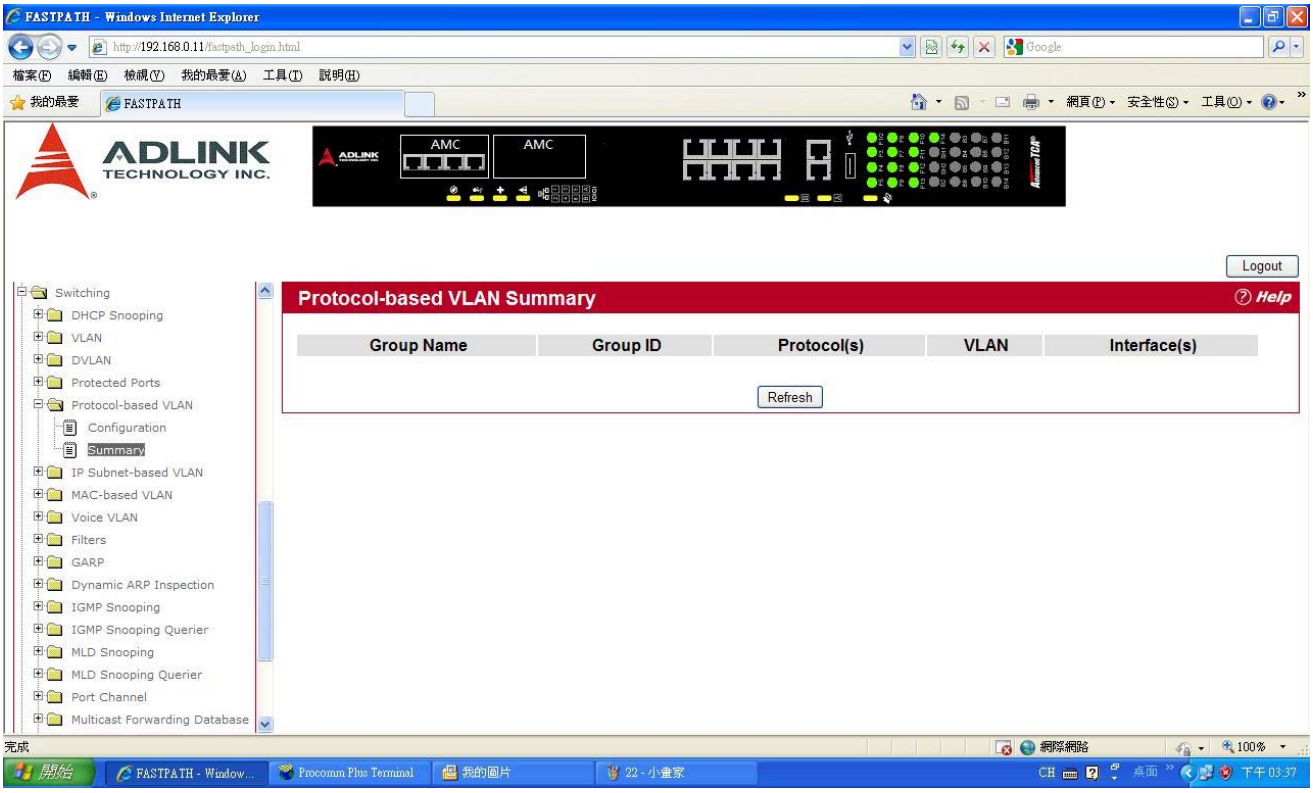
Field	Description
	dynamically maps network layer addresses to physical medium access control (MAC) addresses • IPX: The Internetwork Packet Exchange (IPX) is a connectionless datagram Network-layer protocol that forwards data over a network.
VLAN ID	Specifies the VLAN ID associated with this group. The range is 1-4093.
Interface	Selects the interface(s) to add or remove from this group. CTRL + click to select multiple protocols. On platforms that support stacking, the field is Interface

- To create or modify a protocol-based VLAN group, edit the fields, and click Submit.
- To delete an existing protocol-based VLAN group, select the group from the Group ID field, and 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 Switching > Protocol-based VLAN > Summary in the navigation tree.



Field	Description
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 protocols to associate with this group, which can be one or more of the following: • IP: IP is a network layer protocol that provides a connectionless service for the delivery of data. • ARP: Address Resolution Protocol (ARP) is a low-level protocol that dynamically maps network layer addresses to physical medium access control (MAC) addresses • IPX: The Internetwork Packet Exchange (IPX) is a connectionless datagram Network- layer protocol that forwards data over a network.
VLAN	Specifies the VLAN ID associated with this group.
Interface	Shows the interfaces participating in this group. On platforms that support stacking, the field is named Interface.

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

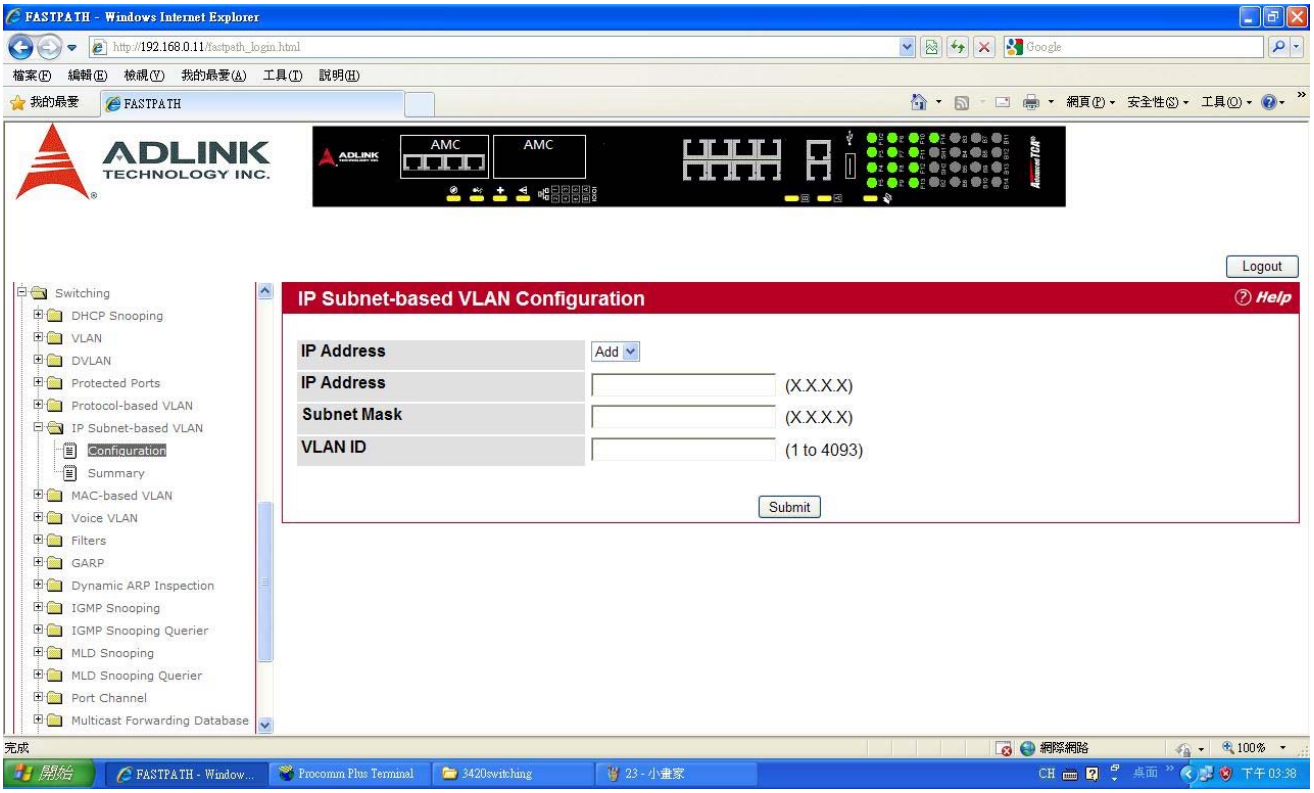
5.10 Managing IP Subnet-Based VLANS

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, 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.

Configuration

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 Switching > IP Subnet-based VLAN > Configuration in the navigation menu.



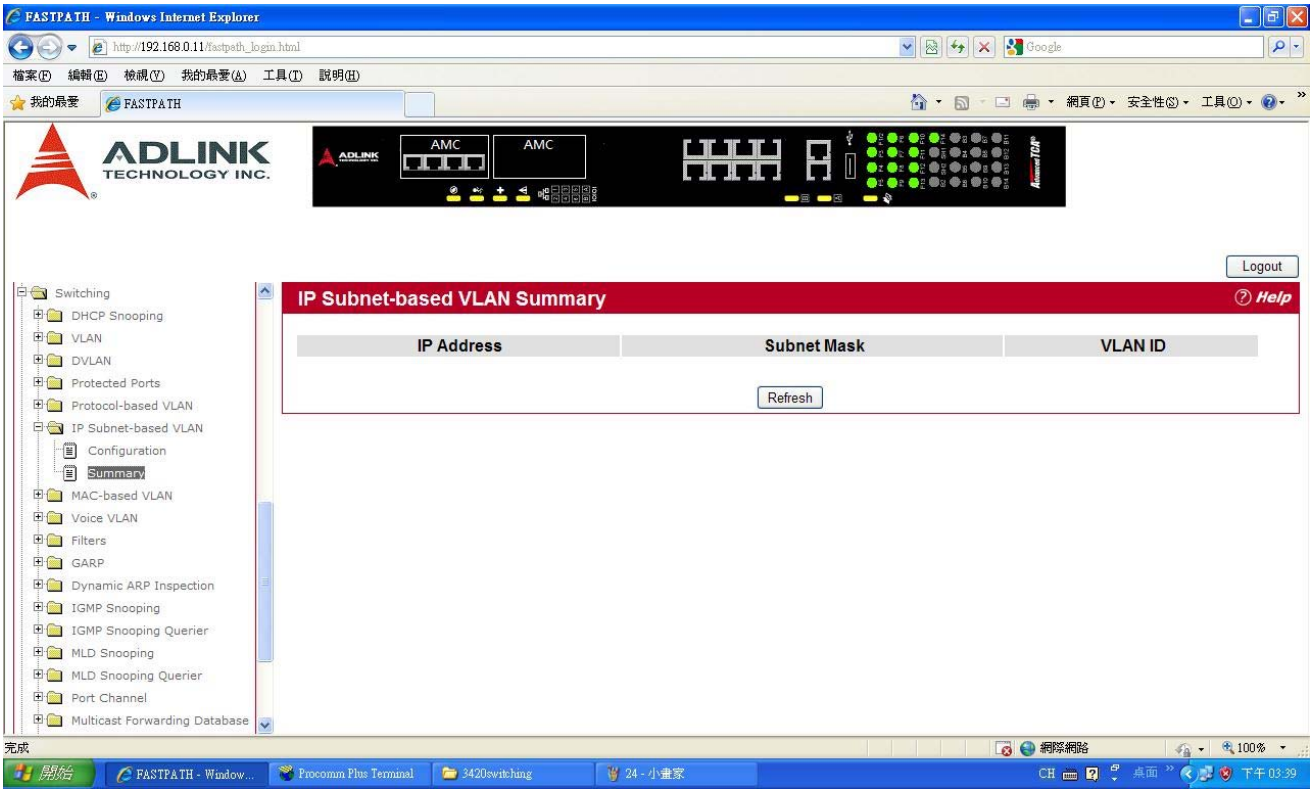
Field	Description
IP Address	Select the IP address of the IP
IP Address	Specifies packet source IP address. This field is configurable only when you create a new IP Subnet
Subnet Mask	Specifies packet source IP subnet mask address.This field is configurable only when you create a new IP Subnet
VLAN ID	Specifies the VLAN to which the IP address is assigned. The valid range is 1

- 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 click Delete.

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 Switching > IP Subnet-based VLAN Summary in the navigation tree.



IP Subnet-based VLAN Summary Fields

Field	Description
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.

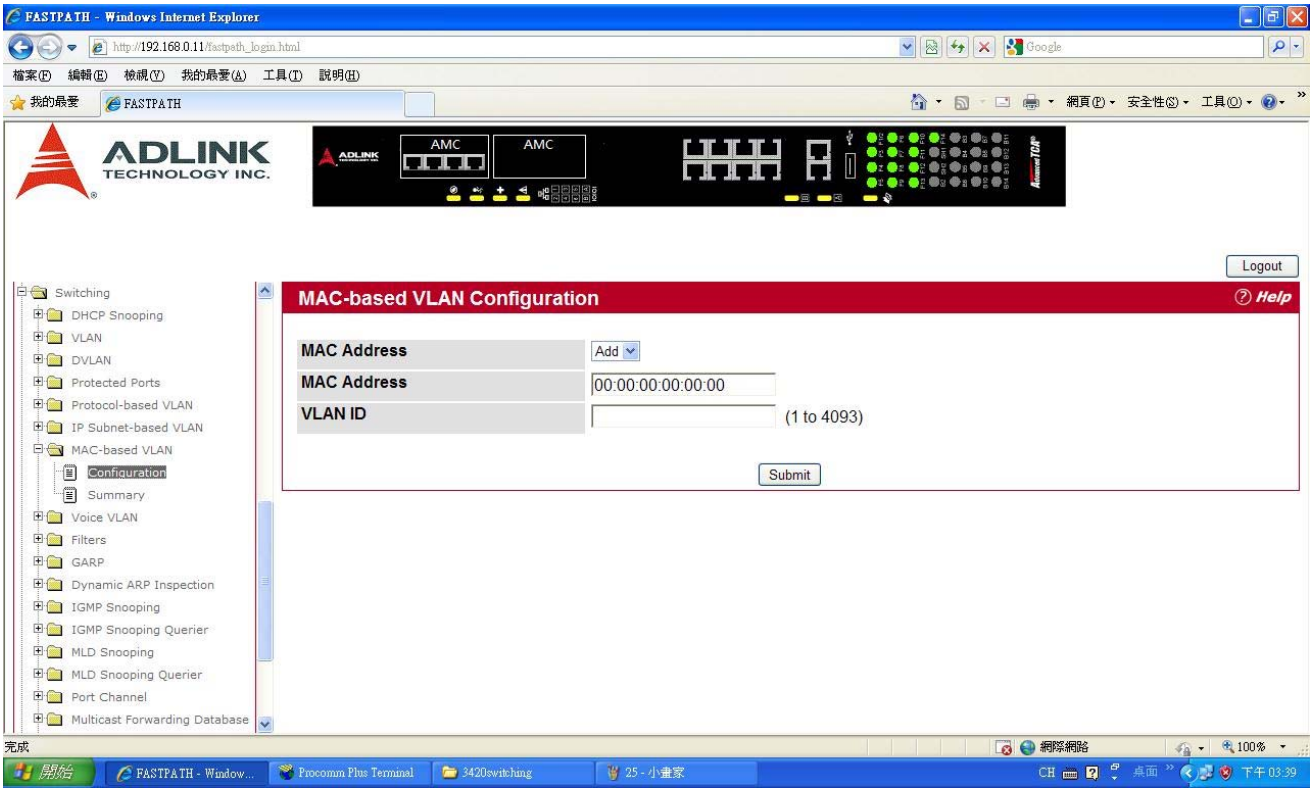
Click Refresh to reload the page and display the most current information.

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, 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 Switching > MAC-based VLAN > Configuration in the navigation menu.



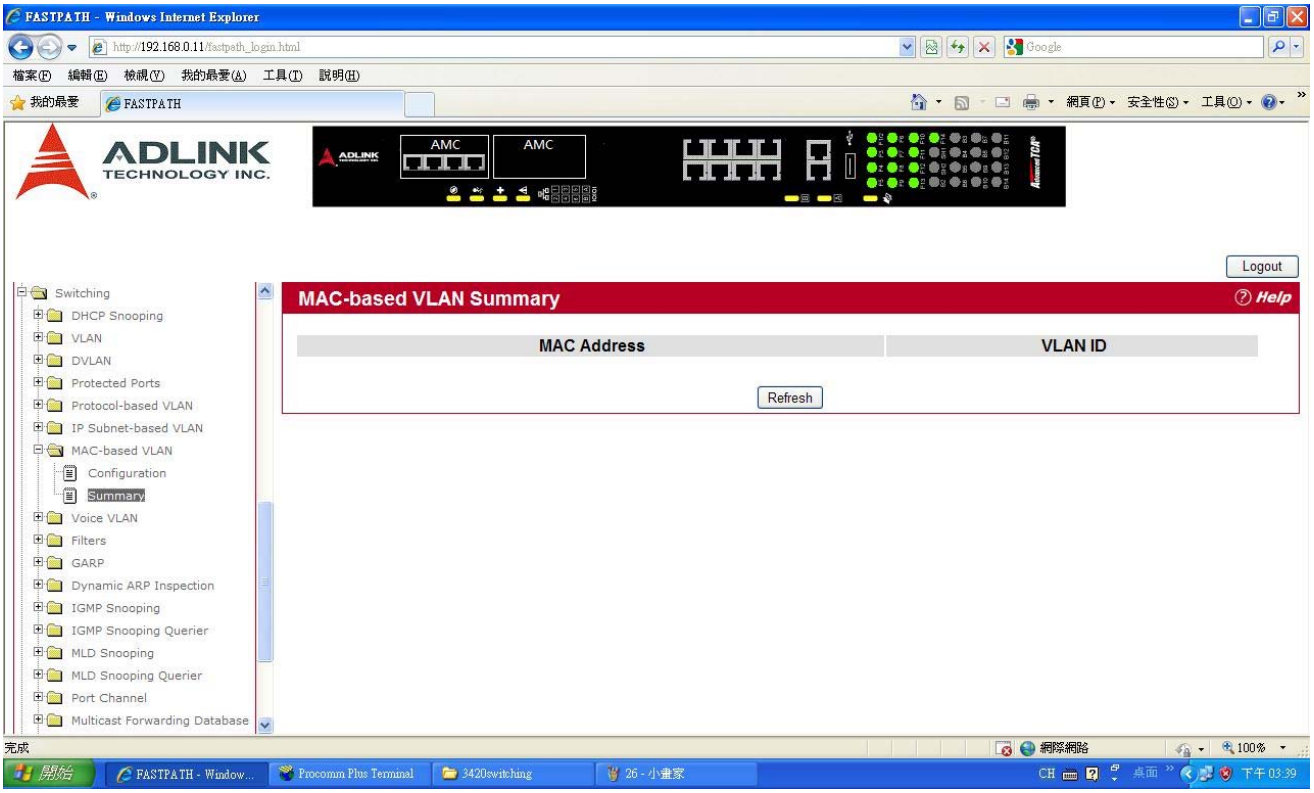
Field	Description
MAC Address	Specifies the source MAC address to map to a VLAN.
VLAN ID	Specifies the VLAN to which the source MAC address is to be bound.

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 Switching > MAC-based VLAN > Summary in the navigation menu.



Field	Description
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.

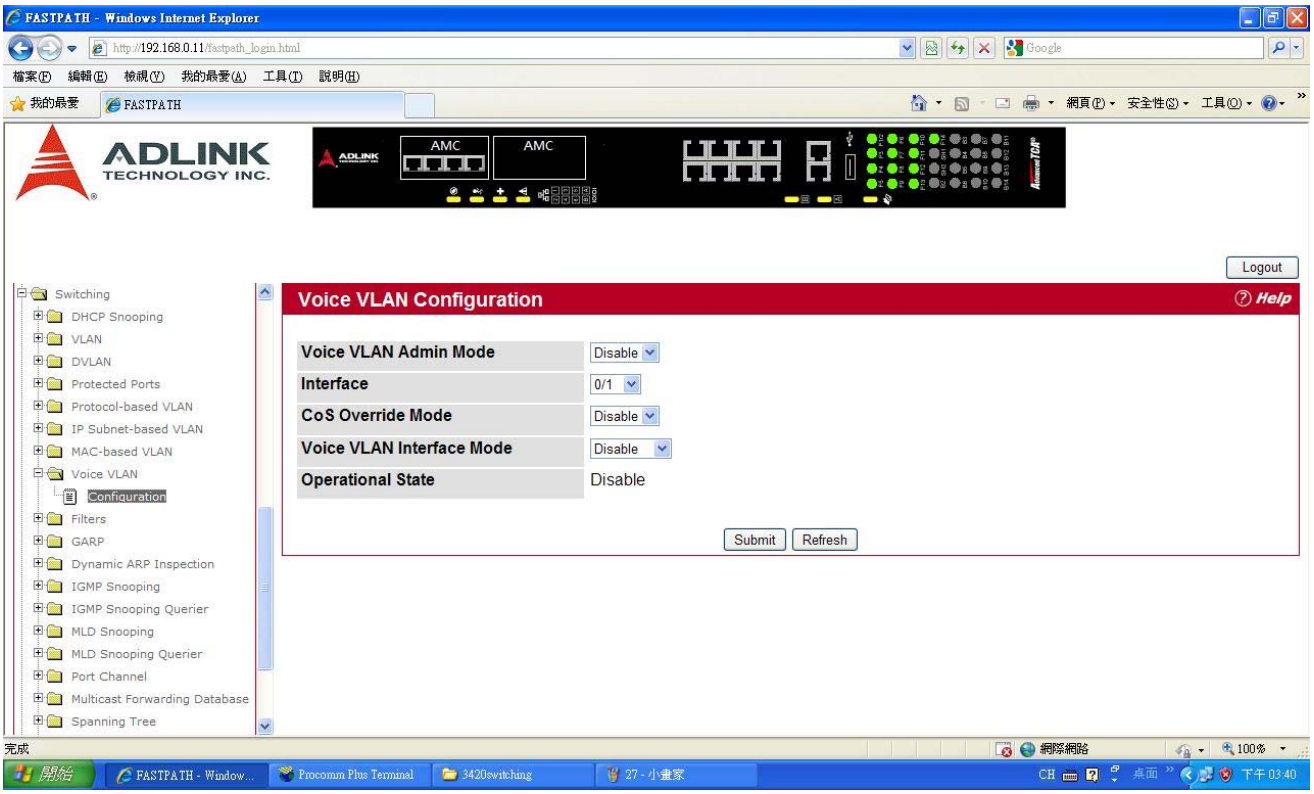
Voice VLAN Configuration

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 System > Voice VLAN > Voice VLAN Configuration.



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 stack unit, slot, and port to configure this service on.
Voice VLAN Interface	Select one of the following interface modes:

Mode	• 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, the service will not be operational. • None: The voice VLAN service is disabled on this interface; however, unlike Disable mode, the CoS override feature is still operational on the port. • 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 VLAN ID. This feature may not be supported by all hardware configurations. • Untagged:
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.
Operational State	Indicates whether the voice VLAN is operational.

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

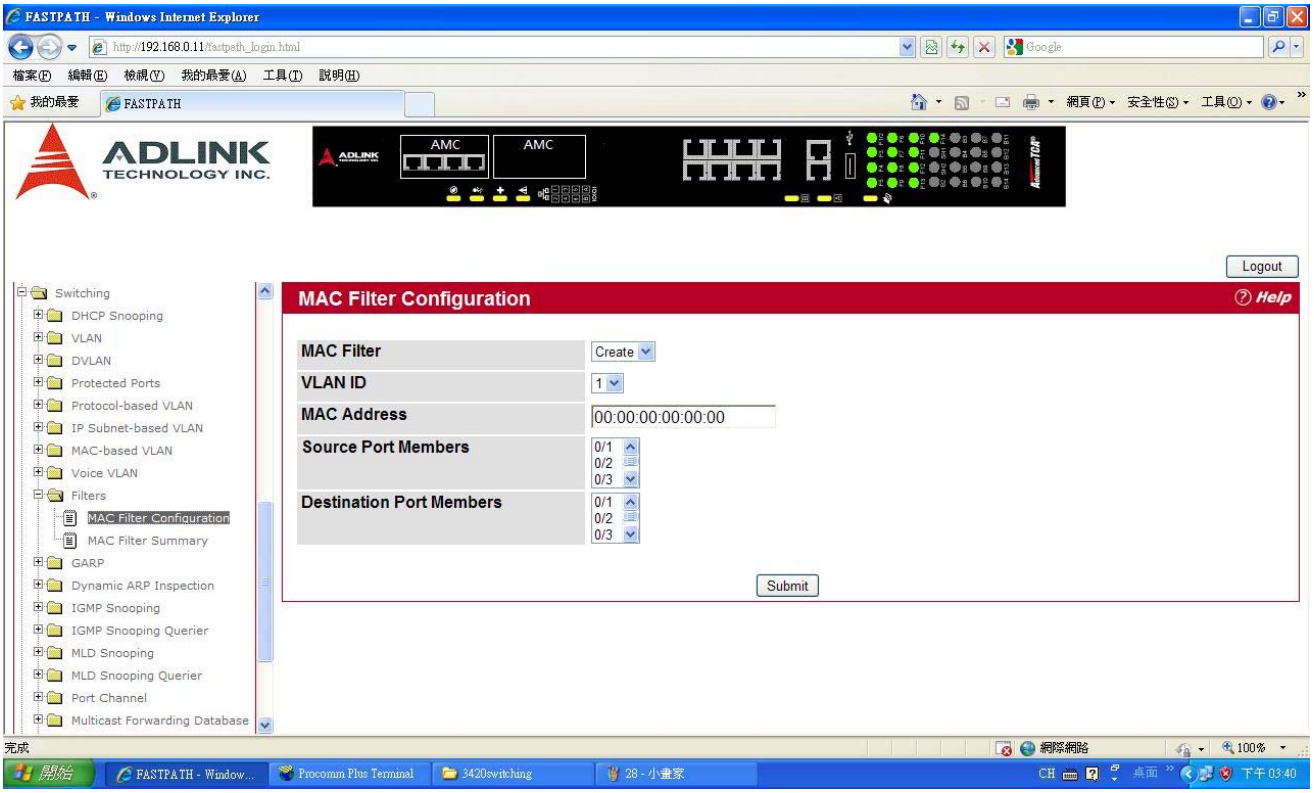
Click Refresh to display the latest information from the router.

Creating MAC Filters

Static MAC filtering allows you to associate a MAC address with a VLAN and set of source ports and destination ports. (The availability of source and destination port filters is subject to platform restrictions). 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.

MAC Filter Configuration

Use the MAC Filter Configuration page to associate a MAC address with a VLAN and one or more source and/or destination ports
To access the MAC Filter Configuration page, click Switching > Filters > Configuration in the navigation tree.



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: •00:00:00:00:00:00

Field	Description
	•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 Mask	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 Mask	Select the ports you want to include in the outbound filter. A packet, once admitted, is sent to all the ports in this list.

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

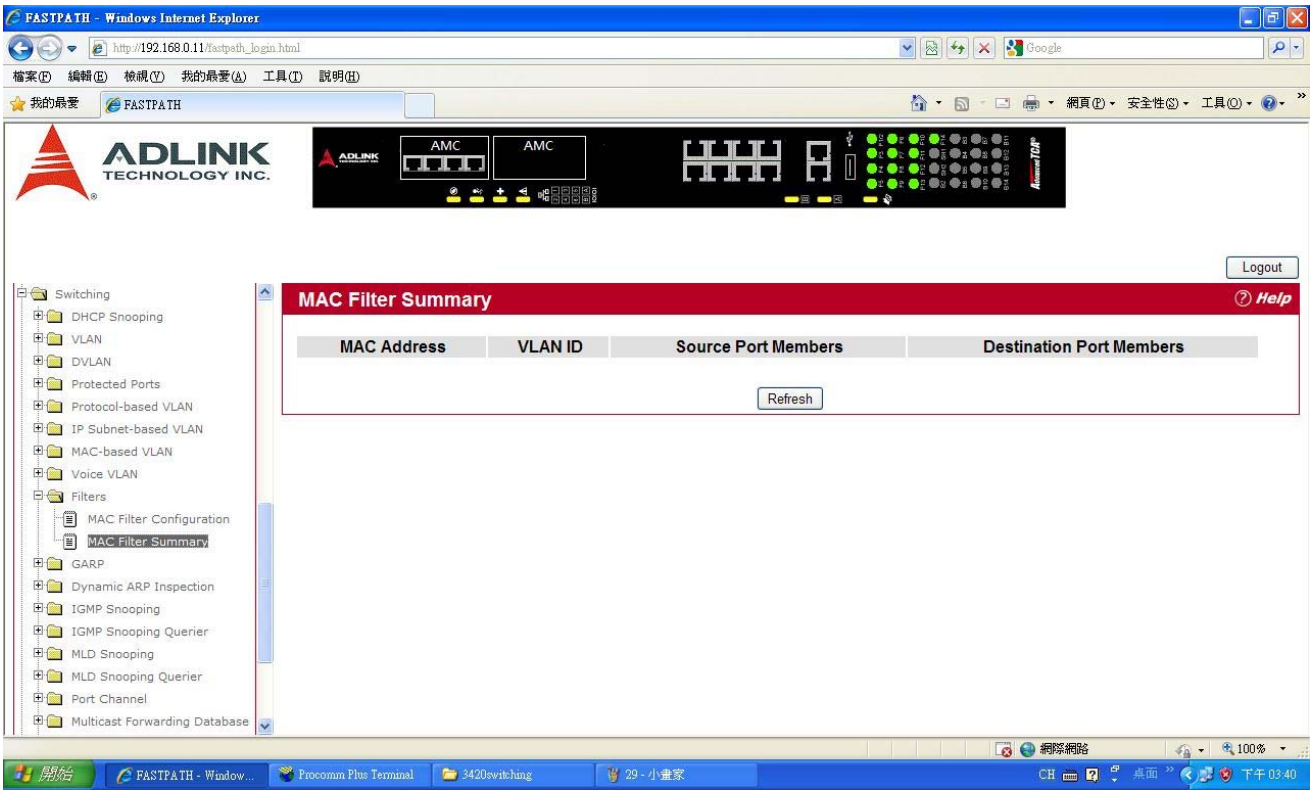
To change the port mask(s) for an existing filter, select the entry from the MAC Filter field, and click (or CTRL + click) the port(s) to include in the filter. Only those ports that are highlighted when you click Submit are included in the filter.
To change the MAC address or VLAN associated with a 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 Switching > Filters > Summary in the navigation tree.



Field	Description
MAC Address	Shows the MAC address of the filter.
VLAN ID	Shows the VLAN ID used with the MAC address to fully identify packets you want filtered.
Source Port Members	Lists the ports included in the inbound filter. If a packet with the MAC address and VLAN ID displayed is received on a port that is not in the list, it will be dropped.
Destination Port Members	Lists the ports included in the outbound filter. A packet, once admitted, is sent to all ports in the list.

5.11 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 GVRP.

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 Extended Filtering Services.

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 Switching > GARP > Status in the navigation tree.



GARP Status Fields

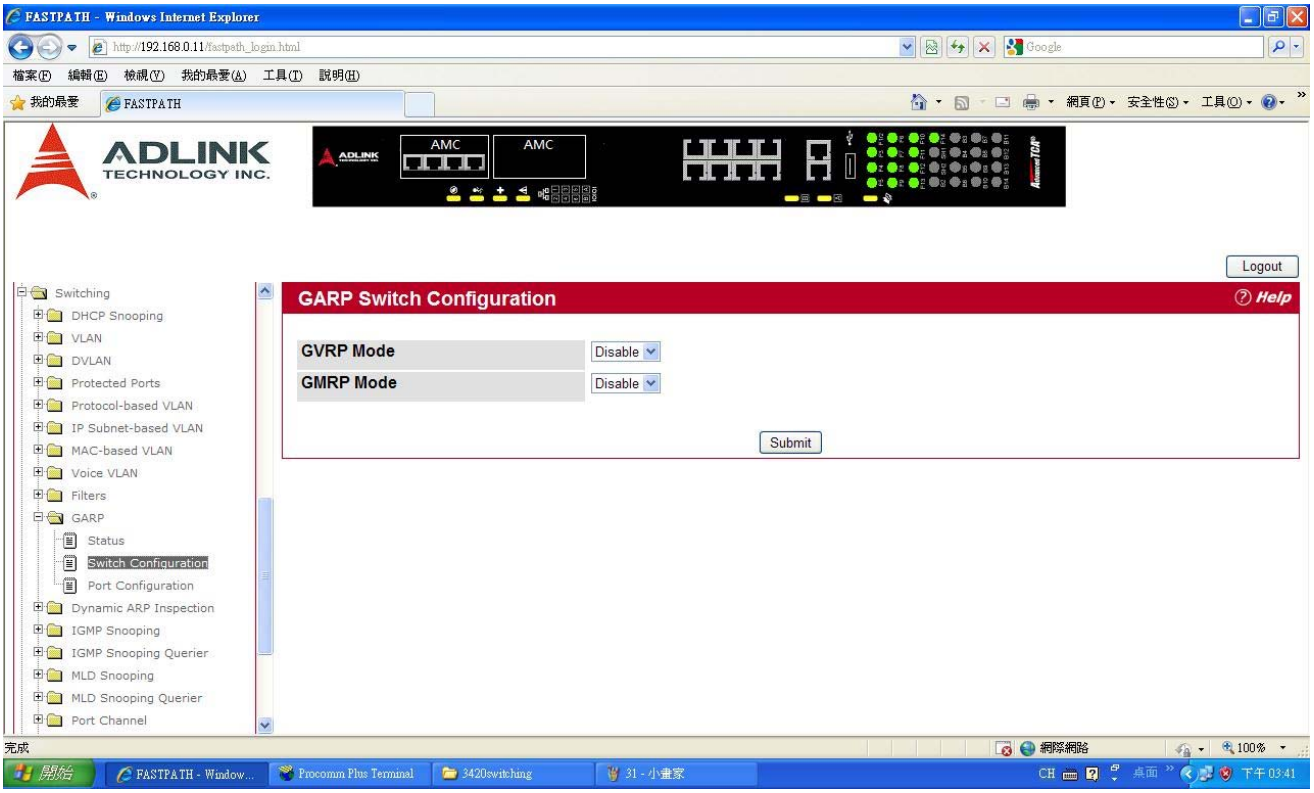
Field	Description
Switch GVRP	Shows whether the switch GVRP protocol is enabled or disabled.
Switch GMRP	Shows whether the switch GMRP protocol is enabled or disabled.
Interface	Identifies the system interface. If stacking is not supported, this field displays Port only.
Port GVRP Mode	Shows the GARP 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 Switching > GARP > Switch Configuration in the navigation tree.



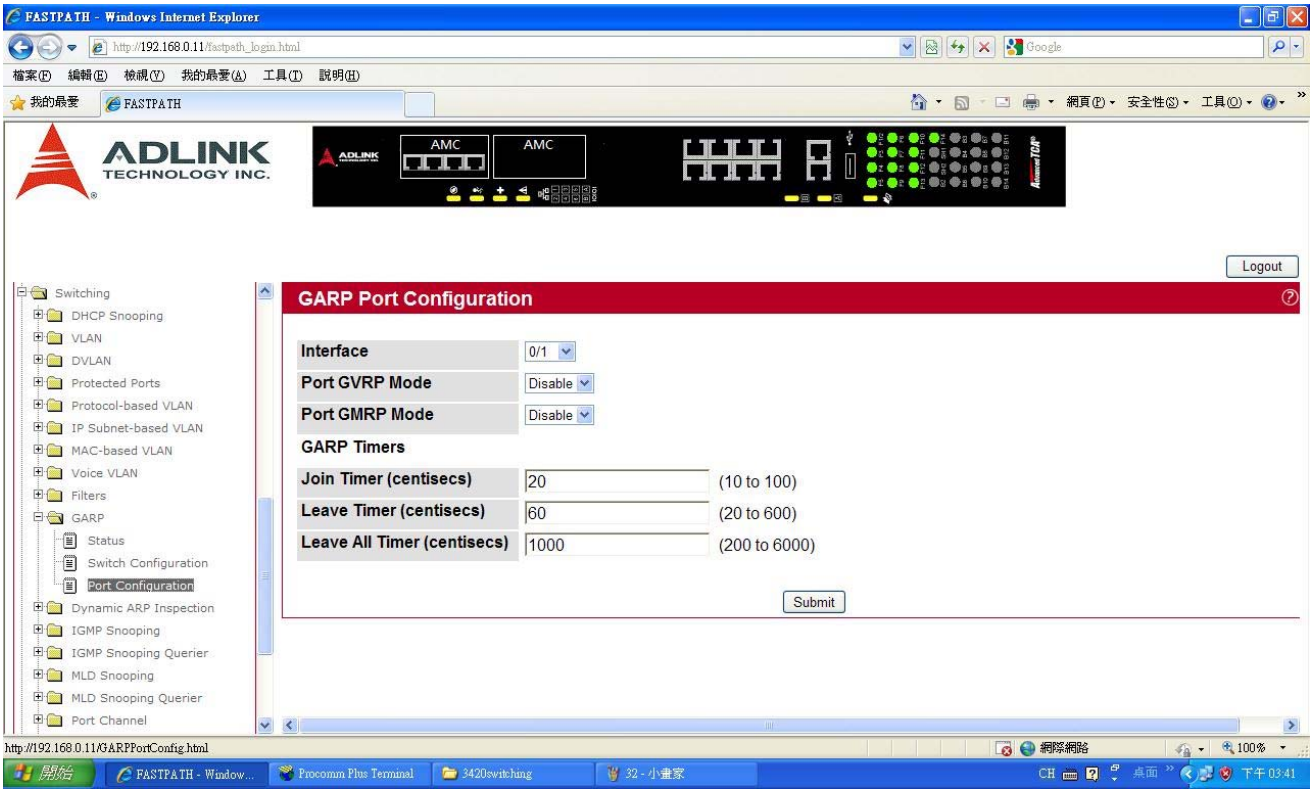
Field	Description
Switch GVRP Mode	Shows the GARP VLAN Registration Protocol administrative mode for the switch. The switch GVRP mode must be enabled for the ports to function in GARP protocols
Switch GMRP Mode	Shows the GARP Multicast Registration Protocol administrative mode for the switch. The switch GMRP mode must be enabled for the ports to function in GARP protocols

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 Switching > GARP > Port Configuration in the navigation tree.



Field	Description
Interface	Specifies interface on which to configure the GARP settings. If you select All from the drop-down menu
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
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

GARP Timers	
GARP Join Timer (centisecs)	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.

GARP Timers	
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.

5.12 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.

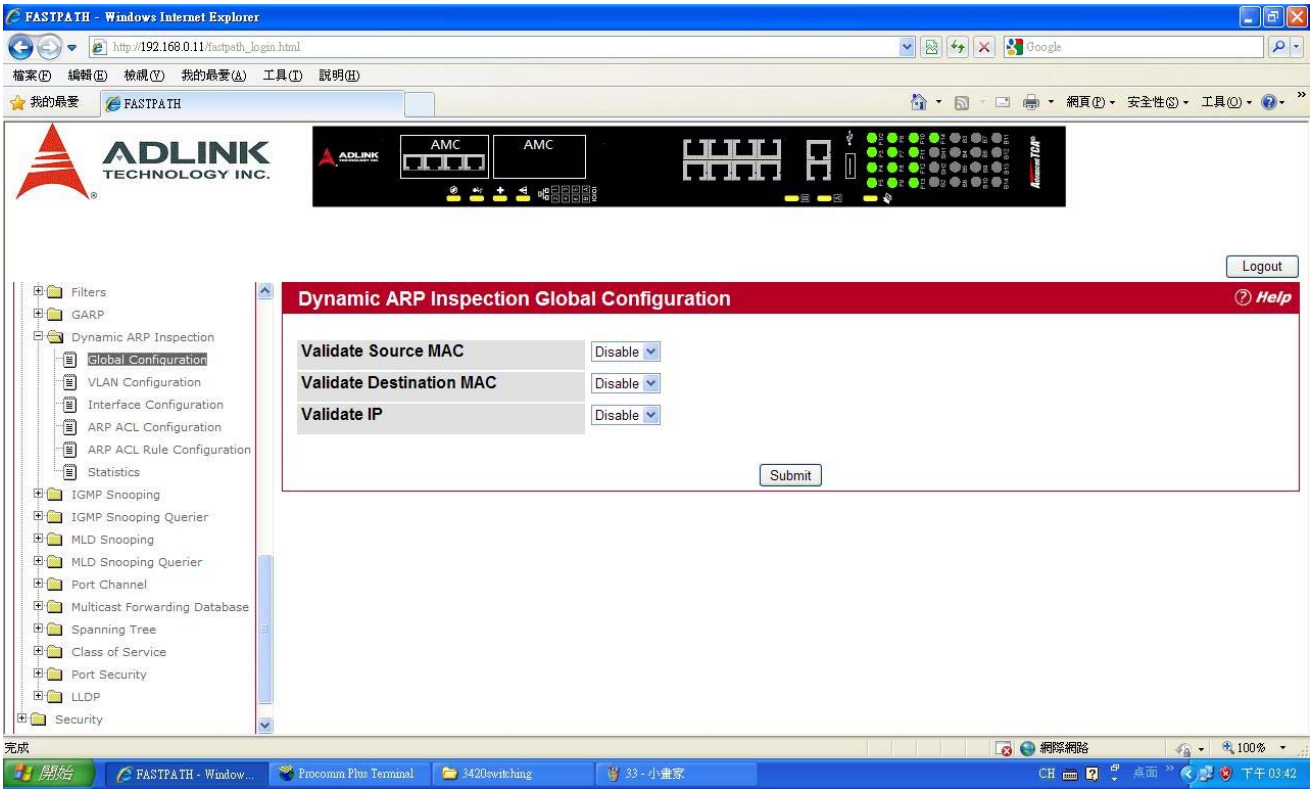
DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples.

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 Switching > Dynamic ARP Inspection > Global Configuration in the navigation tree.



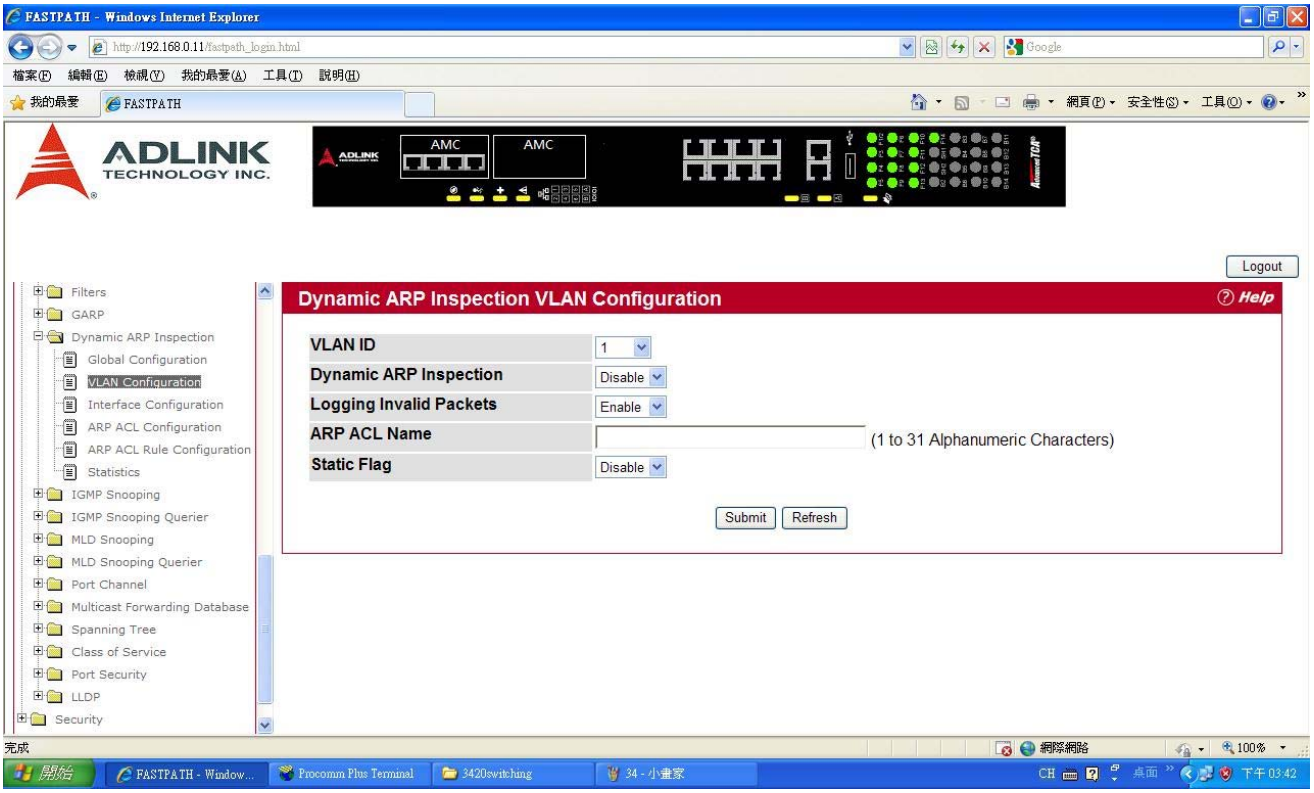
Field	Description
Validate Source MAC	Select the DAI Source MAC Validation Mode for the switch. If you select Enable, Sender MAC
Validate Destination MAC	validation for the ARP packets will be enabled. The default is Disable.
Validate IP	Select the DAI Destination MAC Validation Mode for the switch. If you select Enable, Destination MAC validation for the ARP Response packets will be enabled. The default is Disable.

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 Switching > Dynamic ARP Inspection > VLAN Configuration in the navigation tree.



Field	Description
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, the ARP Packet will be validated by the ARP ACL Rules only. If Disabled, the ARP Packet needs further validation by using the DHCP Snooping entries. The default is Disable.

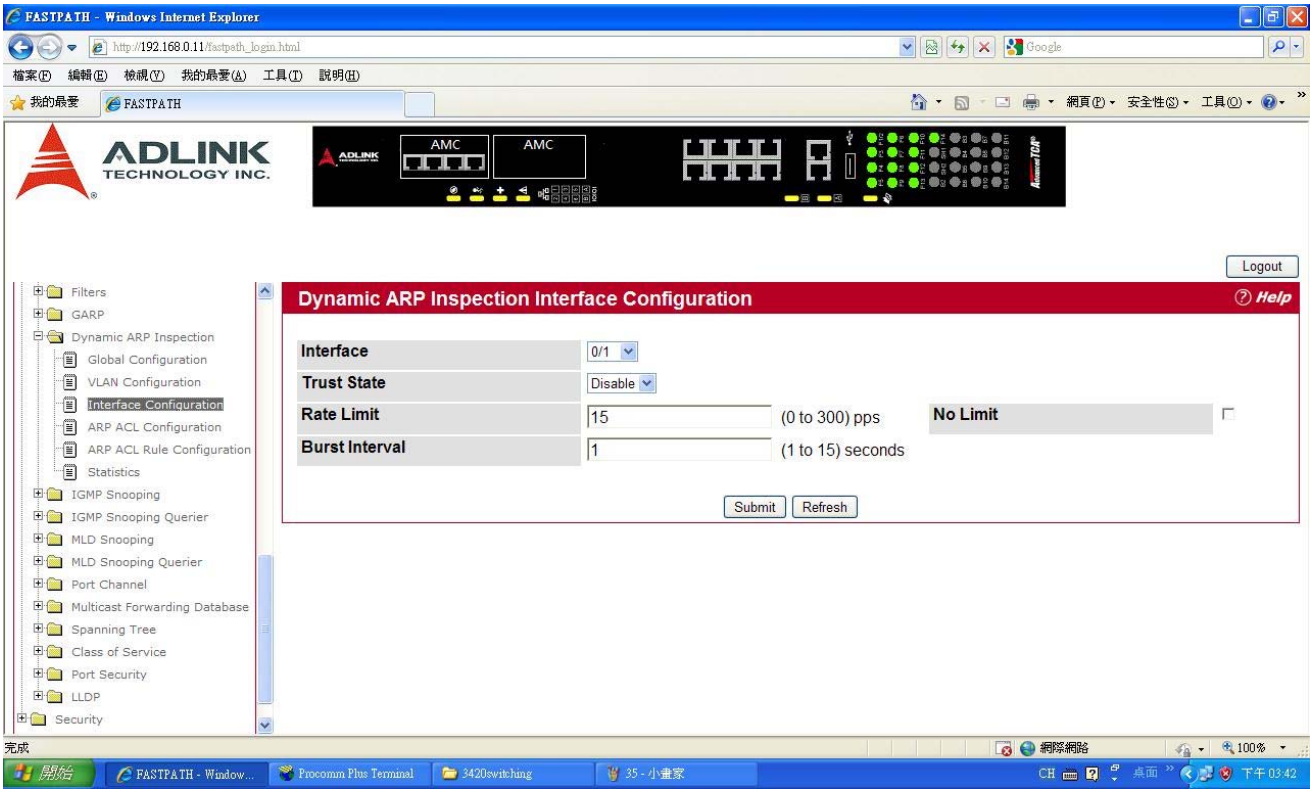
Click Submit to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.

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 Switching > Dynamic ARP Inspection > Interface Configuration in the navigation tree.



Field	Description
Interface	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, the Burst Interval has no meaning and shows as N/A (Not Applicable). The default is 1 second.

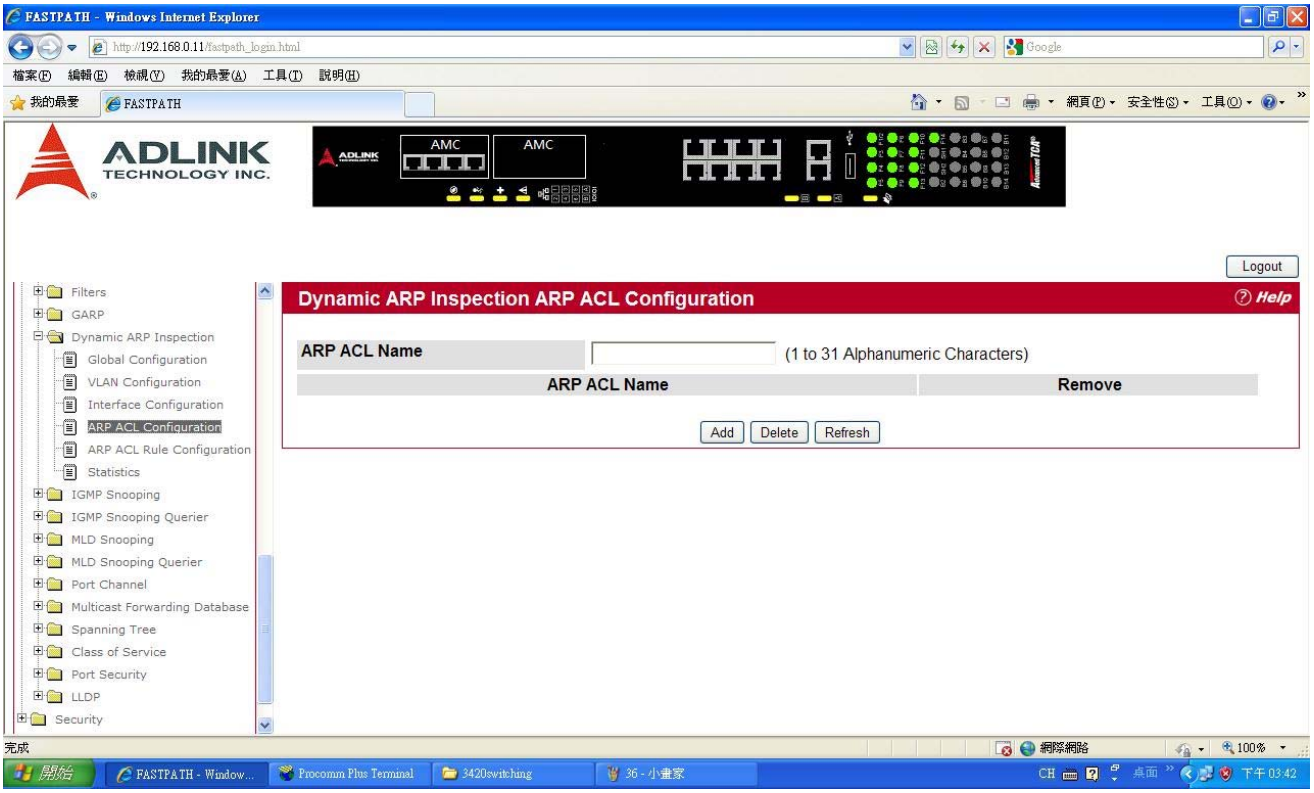
Click Submit to apply the new configuration and cause the change to take effect. These changes will not be retained across a power cycle unless a Save configuration is performed.

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 Switching > Dynamic ARP Inspection > ARP ACL Configuration in the navigation tree.



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.

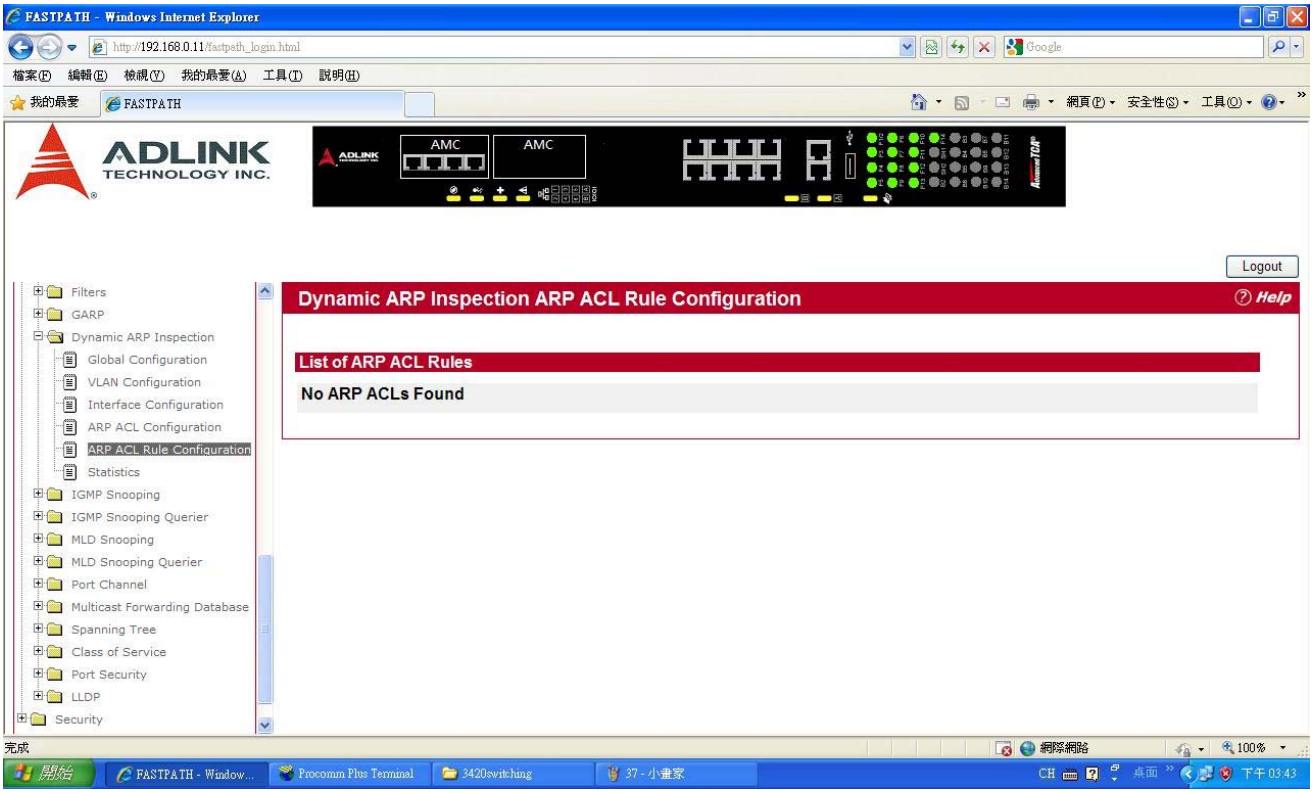
Click Delete to remove the configured ARP ACL entry you selected in the Remove column.

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 Switching > Dynamic ARP Inspection > ARP ACL Rule Configuration in the navigation tree.



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.

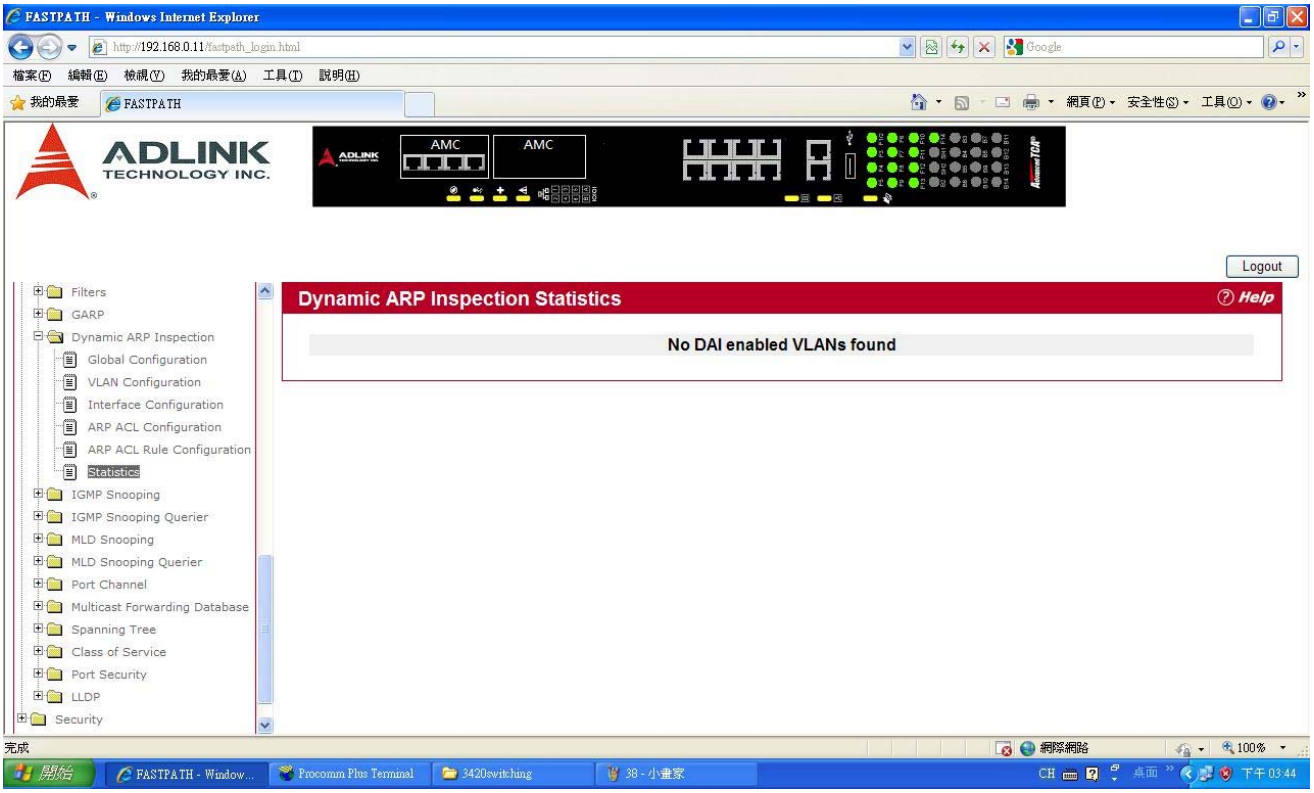
Click Submit to delete the entries selected in the Remove column.

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

DAI Statistics

Use the DAI Statistics page to display the statistics per VLAN.

To display the DAI Statistics page, click Switching > Dynamic ARP Inspection > Statistics in the navigation tree.



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 or 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.

5.13 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.

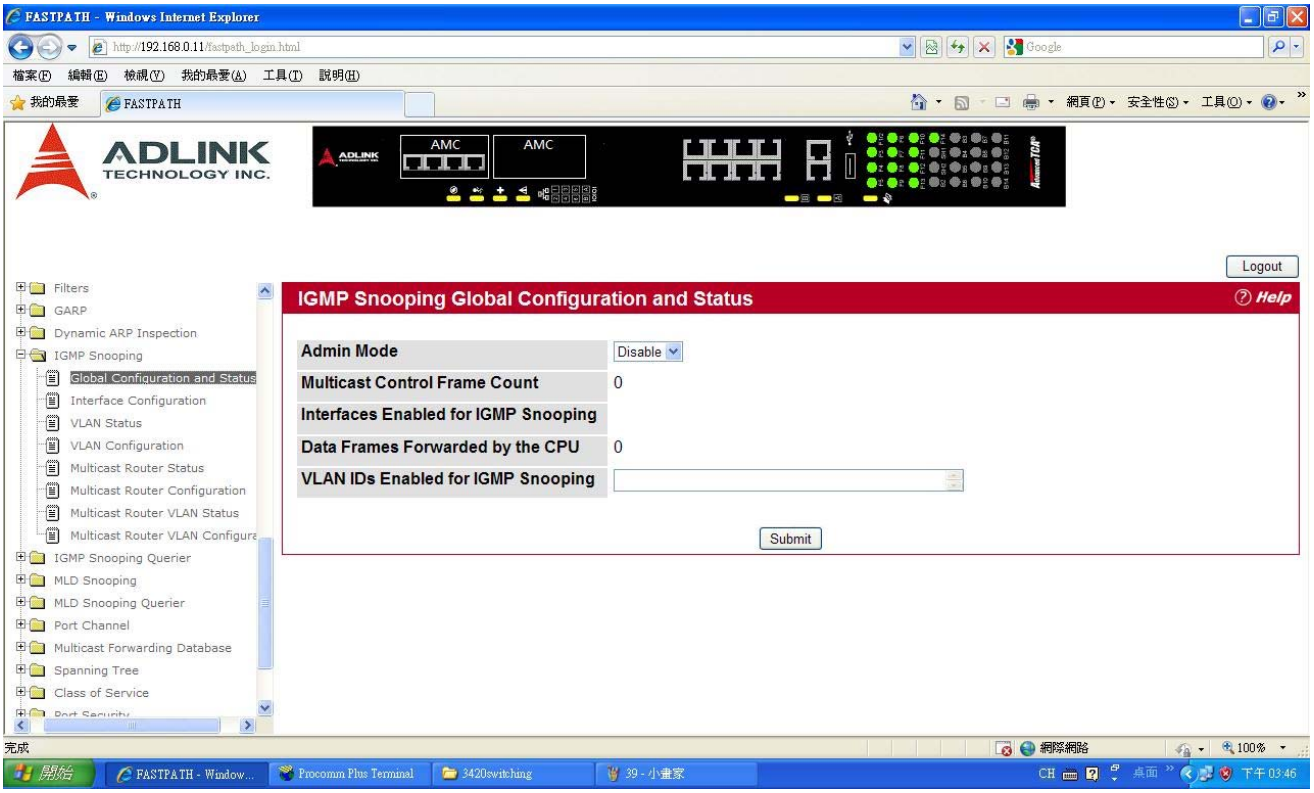
This approach works well for broadcast packets that are intended to be seen or processed by all connected nodes. In the case of multicast packets, however, this approach could lead to less efficient use of network bandwidth, particularly when the packet is intended for only a small number of nodes. Packets 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 Switching > IGMP Snooping > Configuration and Status in the navigation tree.



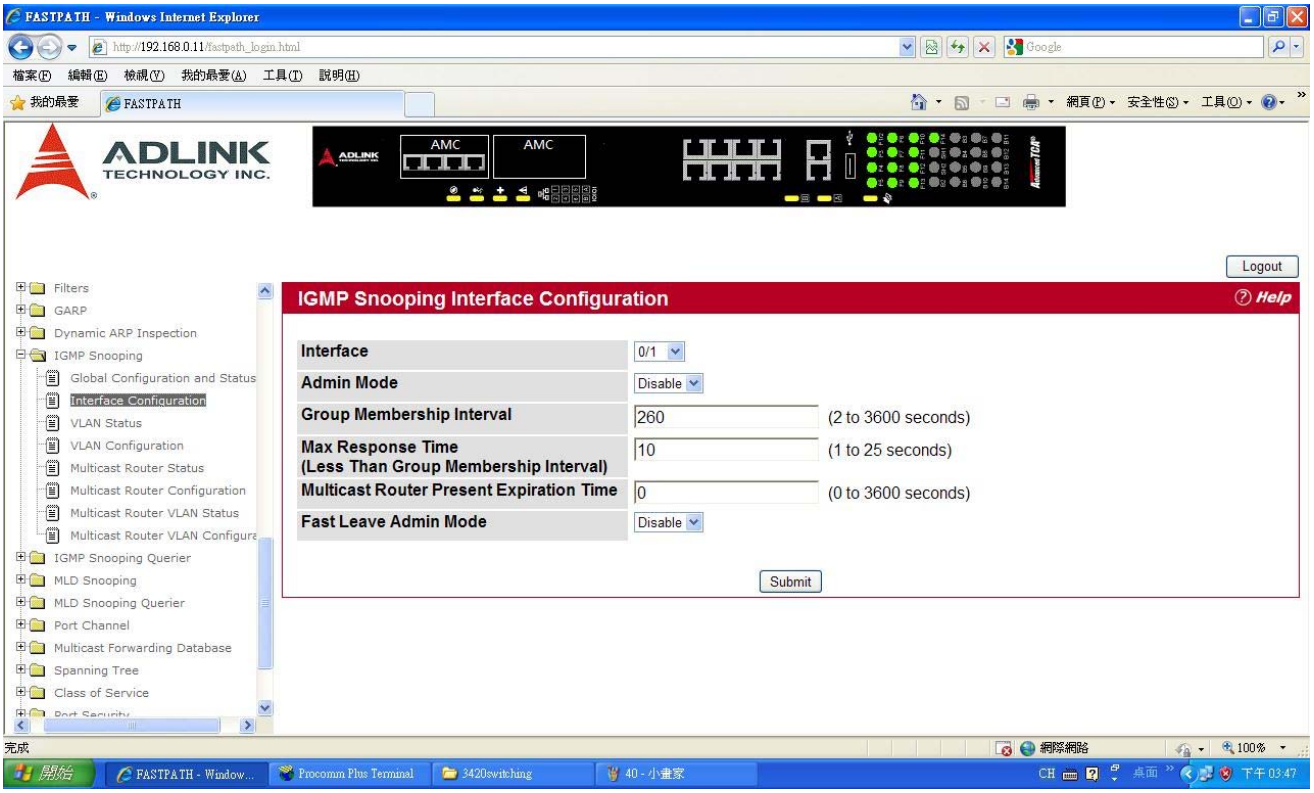
Field	Description
Admin Mode	Select the administrative mode for IGMP Snooping for the switch from the pulldown menu. The default is disable.
Multicast Control Frame Count	Shows the number of multicast control frames that have been processed by the CPU.
Interfaces Enabled for IGMP Snooping	Lists the interfaces currently enabled for IGMP Snooping. To enable interfaces for IGMP snooping, see “Interface Configuration” .
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 “VLAN Configuration” .

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 Switching > IGMP Snooping > Interface Configuration in the navigation tree.



Field	Description
Interface	Select the physical or LAG interfaces to configure. For platforms that support stacking, the field is Interface.
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	Specify the amount of time you want the switch to wait to receive a

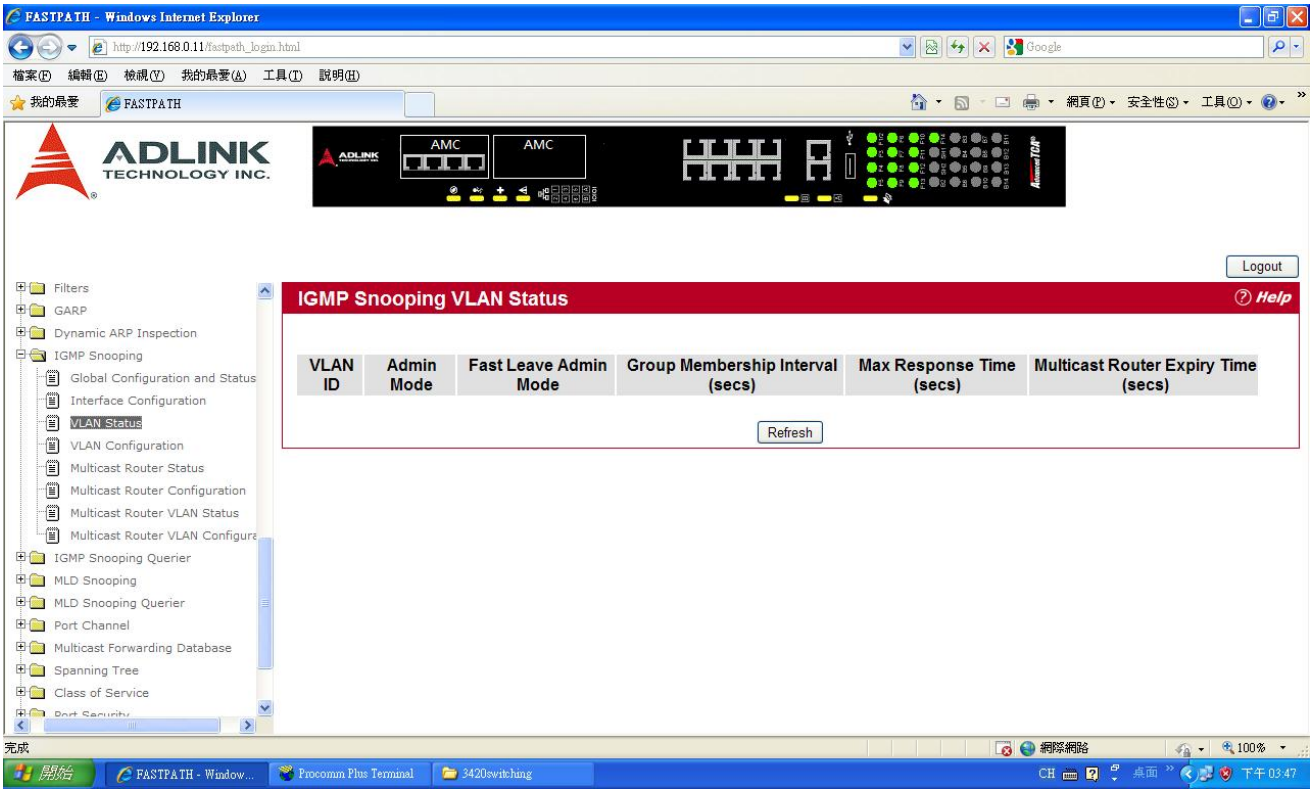
Field	Description
Expiration Time	query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite timeout; i.e., no expiration.
Fast Leave Admin Mode	Select the Fast Leave mode for 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 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 Switching > IGMP Snooping > VLAN Status in the navigation tree.



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.
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. This value may be configured.
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.

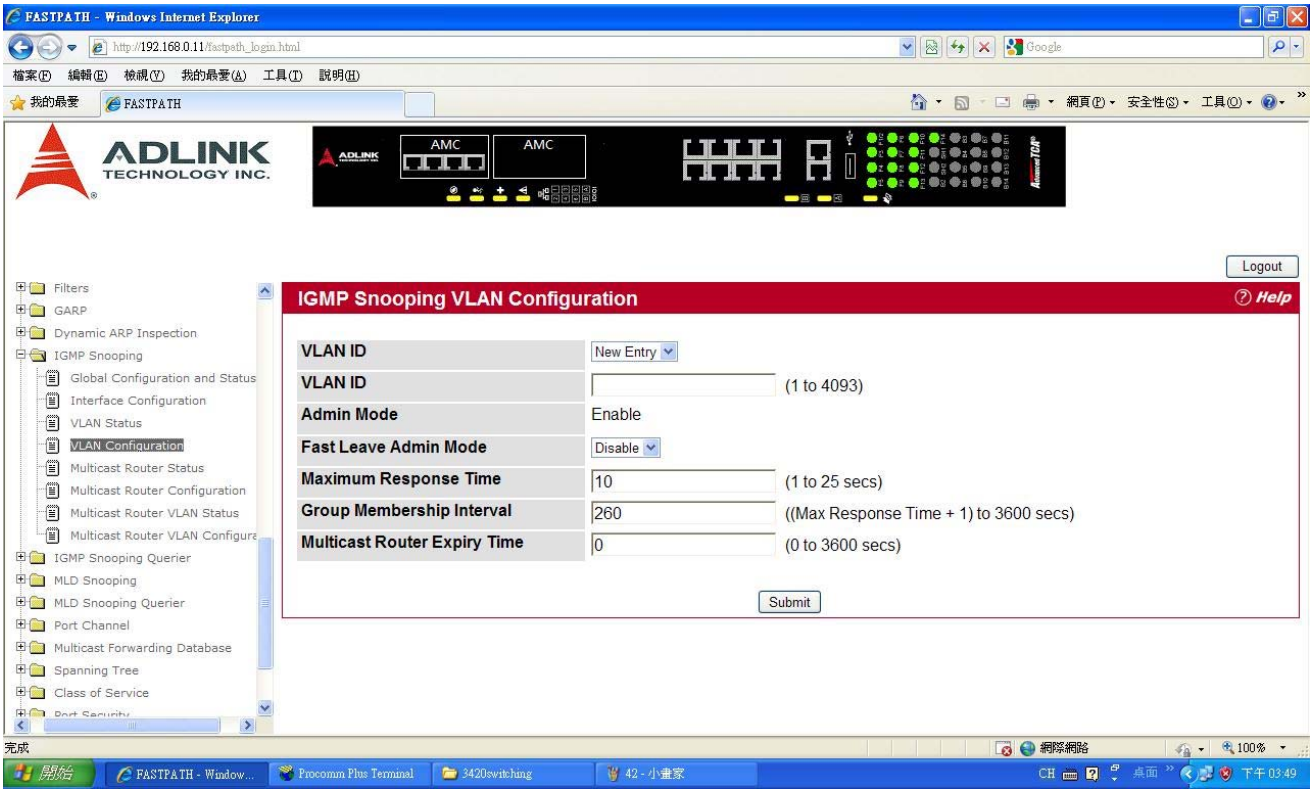
Field	Description
Multicast Router Expiry Time	Shows the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received.

Click Refresh to re-display the page with the latest information from the router.

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 Switching > IGMP Snooping > VLAN Configuration in the navigation tree.



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.

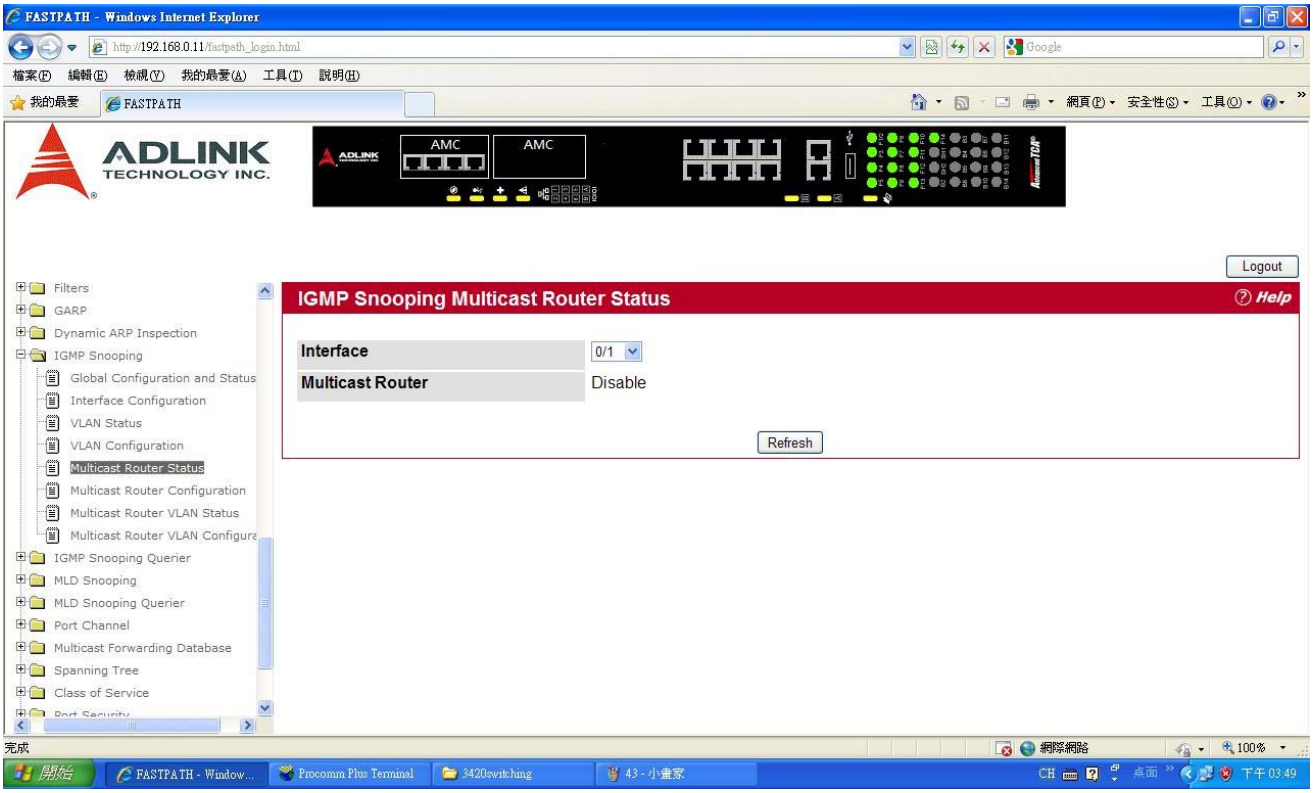
Field	Description
Group Membership Interval	The Group Membership Interval time is the amount of time in seconds that a switch waits for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMPv3 Maximum Response 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 IGMP Query Interval time value. The range is 1 to 3599 seconds.
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.

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 Switching > IGMP Snooping > Multicast Router Statistics in the navigation tree.



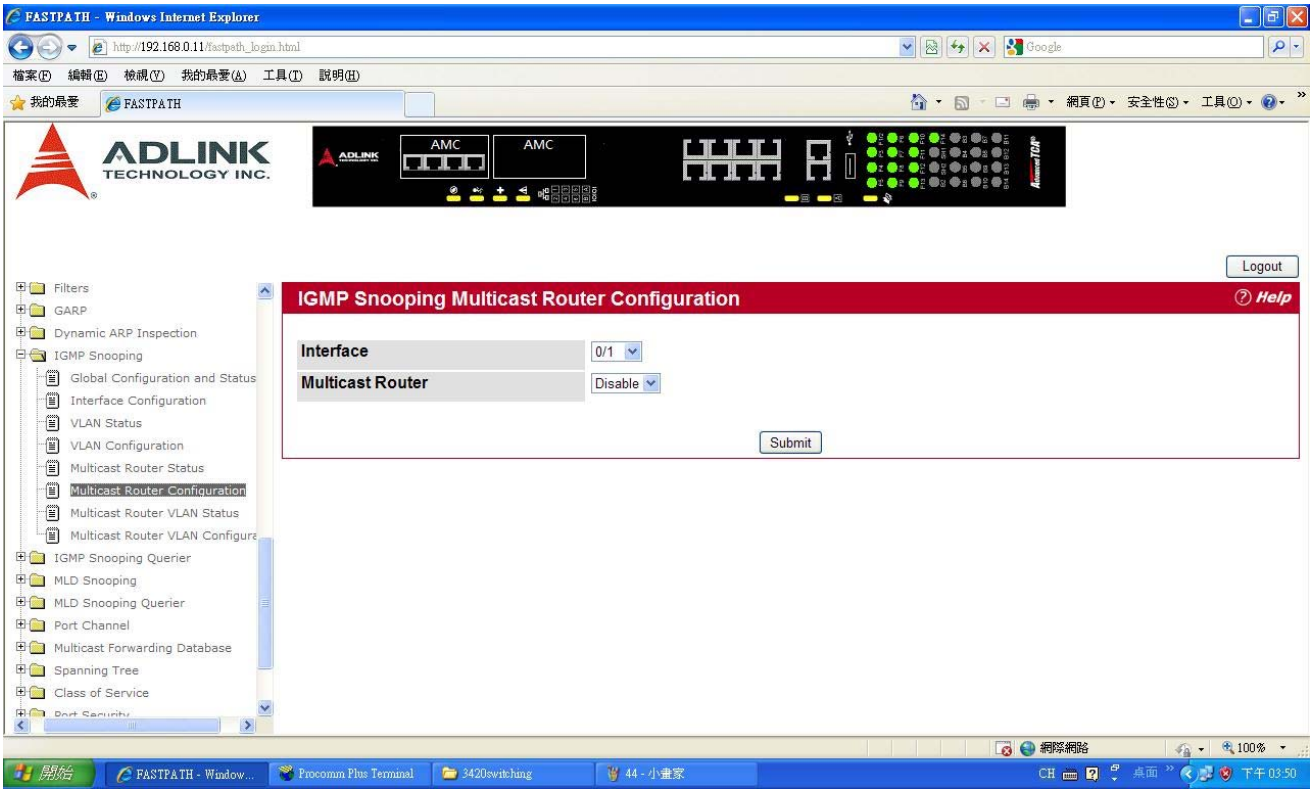
Field	Description
Interface	Select the physical or LAG interface to display. For platforms that support stacking, the field is named Interface.
Multicast Router	Shows whether the specified interface is configured as a multicast router interface.

Click Refresh to re-display the page with the latest information from the router.

Multicast Router 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 Snooping 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 Switching > IGMP Snooping > Multicast Router Configuration in the navigation tree.



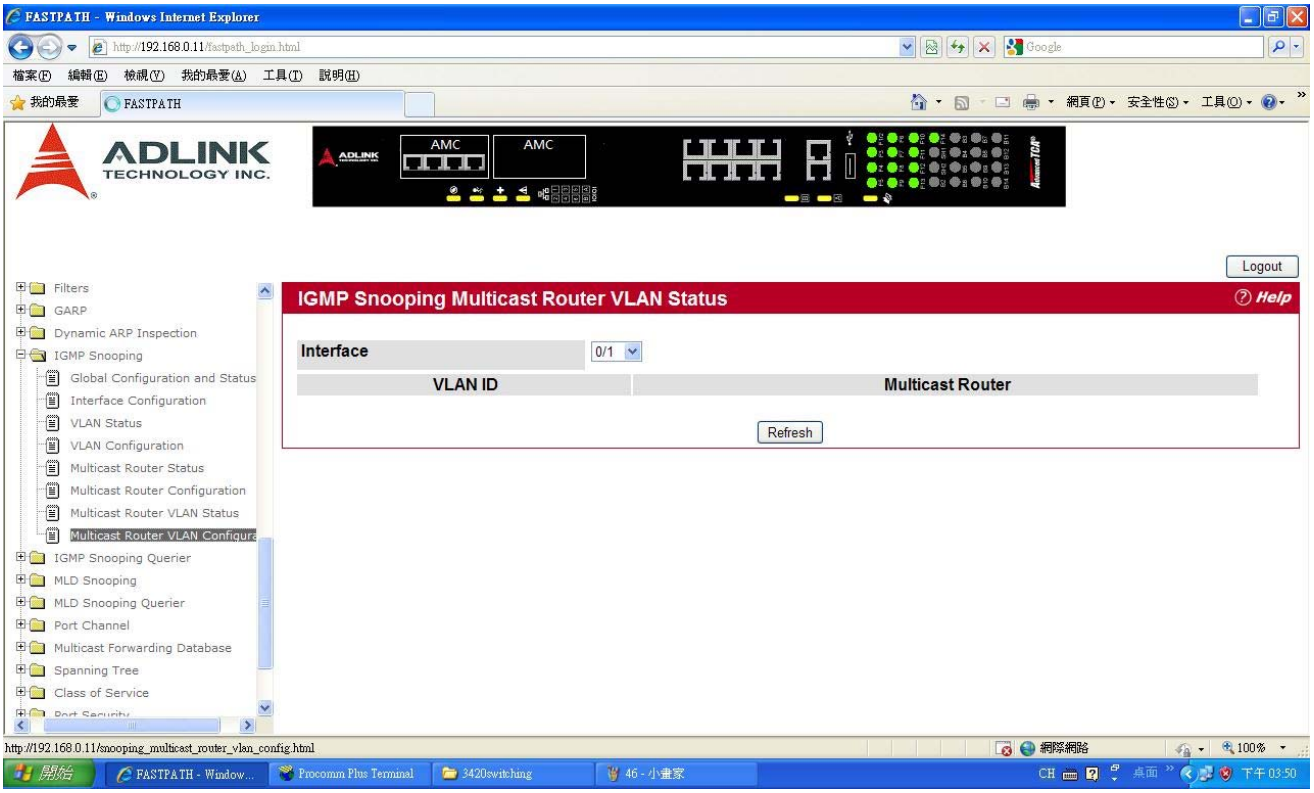
Field	Description
Interface	Select the physical or LAG interface to display. For platforms that support stacking, the field is named Interface.
Multicast Router	Set the multicast router status: • Enabled: The port is a multicast router interface. • Disabled: The port does not have a multicast router configured.

If you enable or disable multicast router configuration on an interface, click Submit to apply the new settings to the switch.

Multicast Router 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 Switching > IGMP Snooping > Multicast Router VLAN Status in the navigation tree.



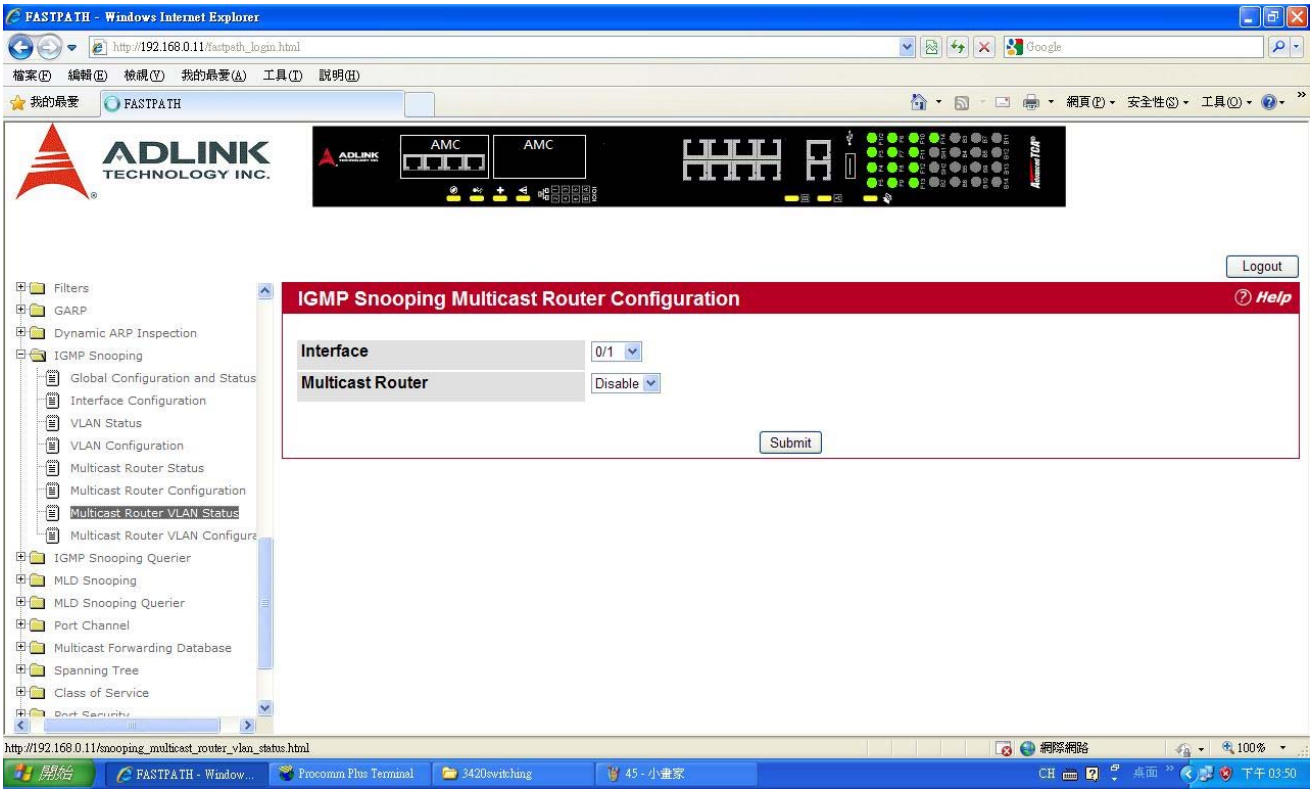
Field	Description
Interface	Select the physical or LAG interface to display. For platforms that support stacking, the field is Interface.
VLAN ID	If a VLAN is enabled for multicast routing on the interface, this field displays its ID.
Multicast Router	Indicates that the multicast router is enabled for the VLAN on this interface.

Click Refresh to re-display the page with the latest information from the router.

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 Switching > IGMP Snooping > Multicast Router VLAN Configuration in the navigation tree.



Field	Description
Interface	Select the physical or LAG interface to display. For platforms that support stacking, the field is Interface.
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.

5.14 Configuring IGMP Snooping Queriers

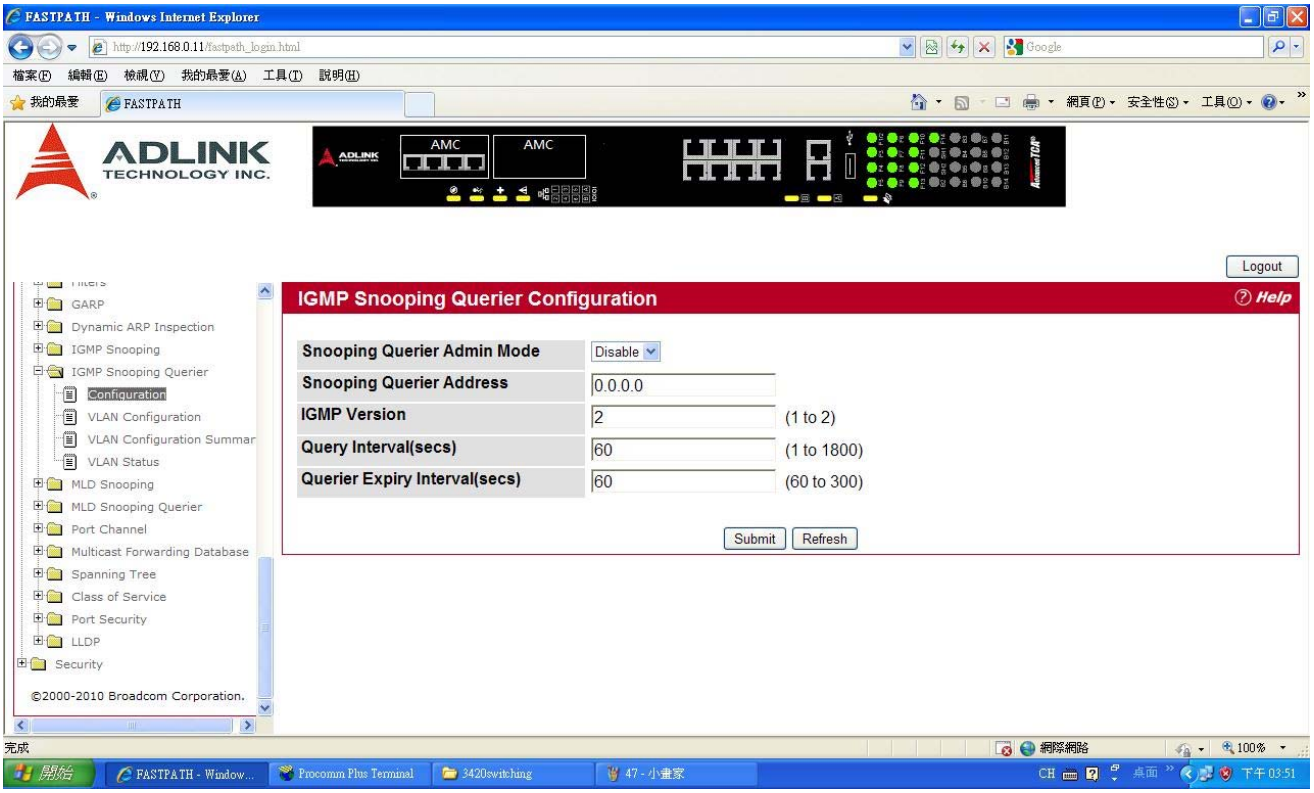
IGMP snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the 'IGMP querier'. The IGMP query responses, known as IGMP reports, keep the switch updated with the current multicast group membership on a port-by-port basis. If the switch does not receive updated membership information in a timely fashion, it will stop forwarding multicasts 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 Switching > IGMP Snooping Querier > IGMP Snooping Querier Configuration in the navigation tree.



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 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. The default value is 60.
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.

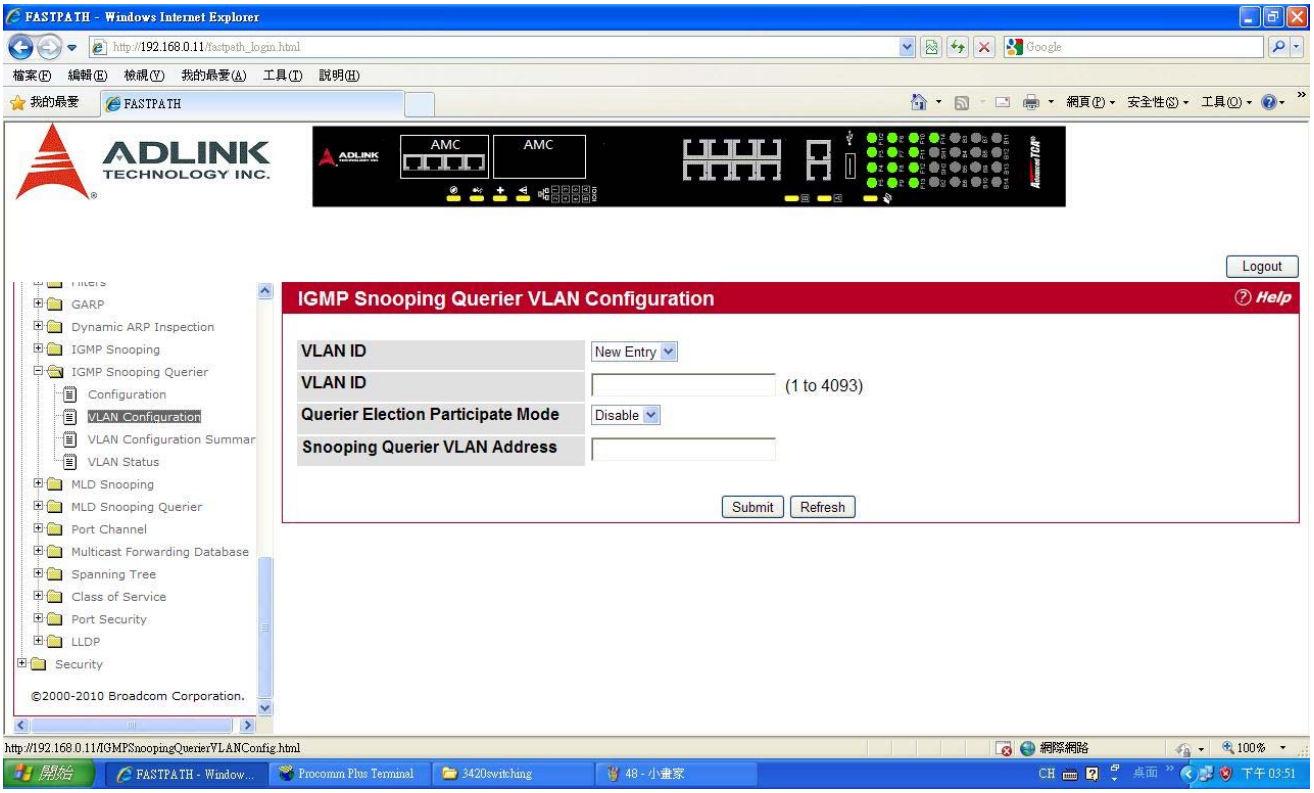
If you configure an IGMP snooping querier, click Submit to apply the new settings to the switch.

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 Switching > IGMP Snooping Querier > IGMP Snooping Querier VLAN Configuration in the navigation tree.



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 address in periodic IGMP queries sent on the specified VLAN.

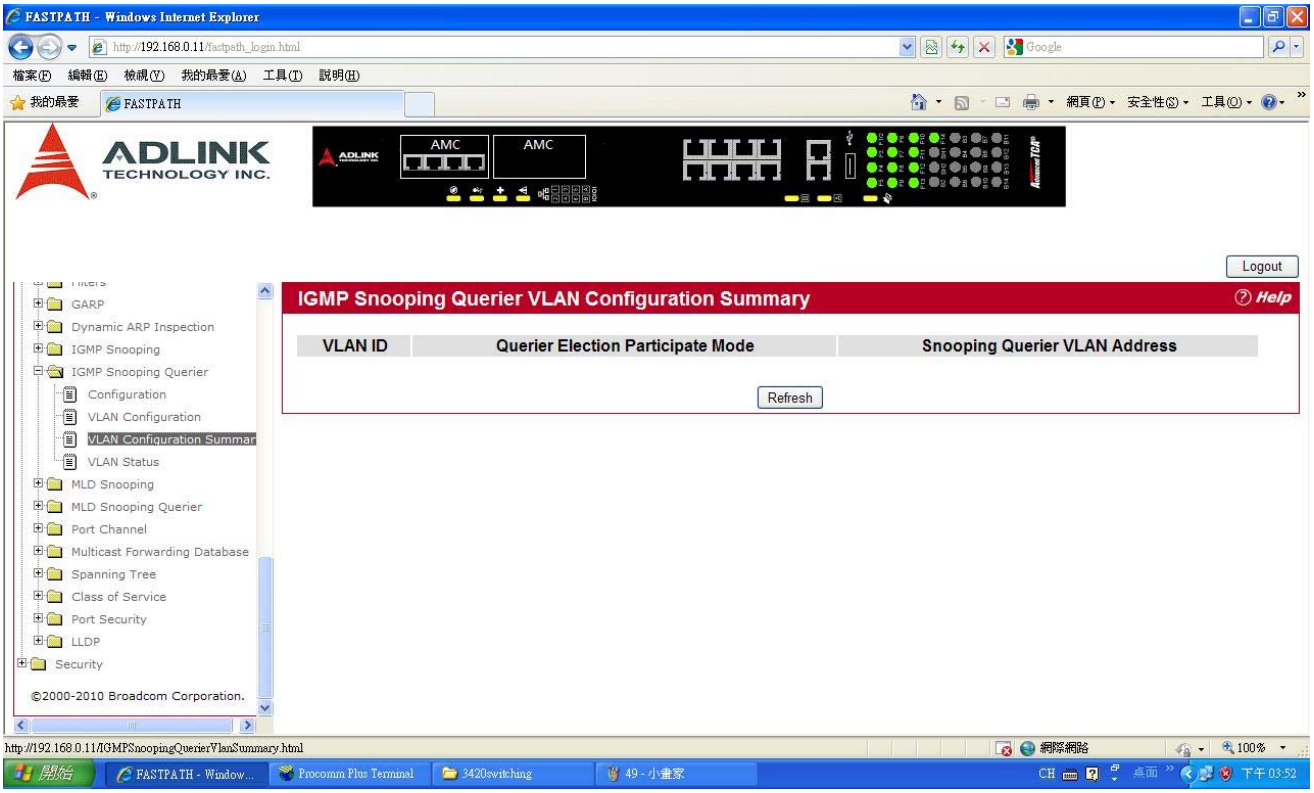
If you configure a snooping querier for a VLAN, click Submit to apply the new settings.

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 Switching > IGMP Snooping Querier > IGMP Snooping Querier VLAN Configuration Summary in the navigation tree.



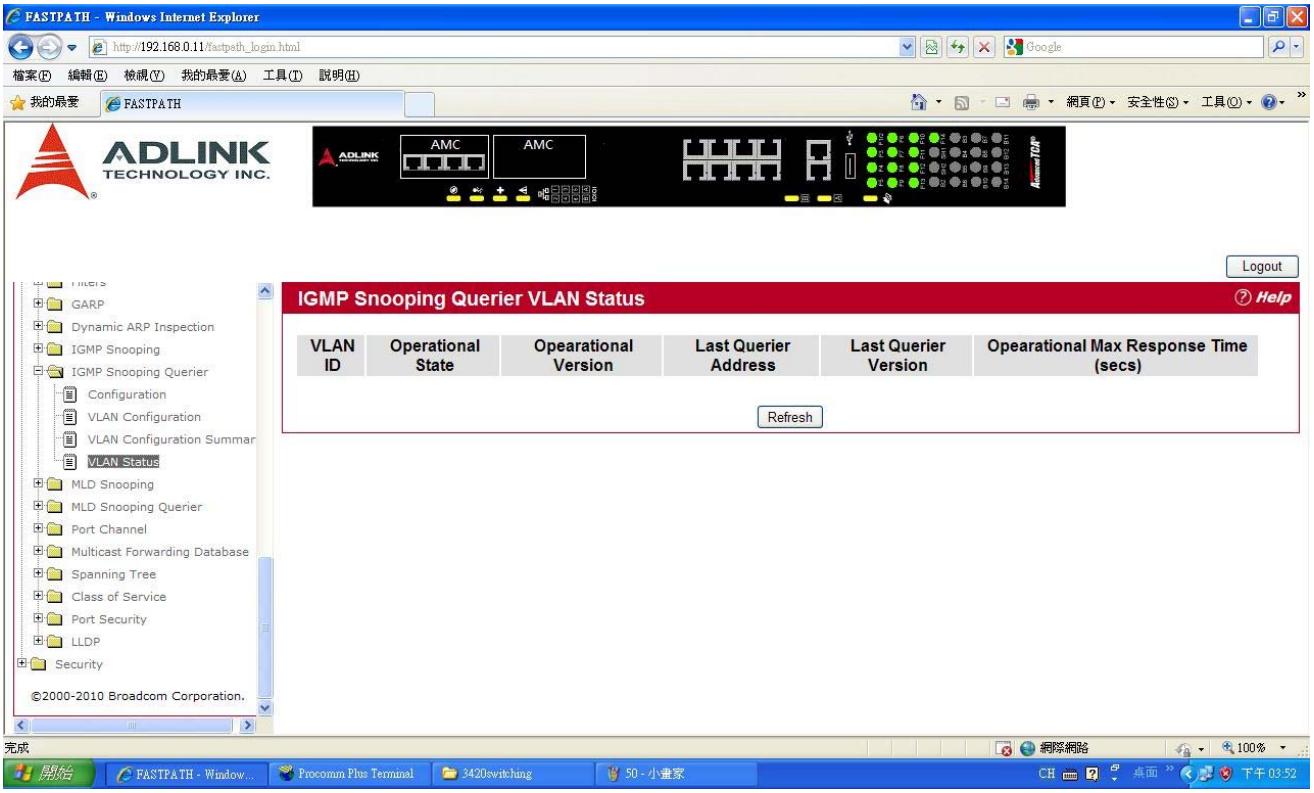
Field	Description
VLAN ID	Specifies the VLAN ID on which IGMP Snooping Querier is administratively enabled.
Querier Election Participate Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the VLAN, the snooping querier 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 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 Switching > IGMP Snooping Querier > IGMP Snooping Querier VLAN Status in the navigation tree.



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: • 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

Field	Description
	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.

5.15 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, 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.

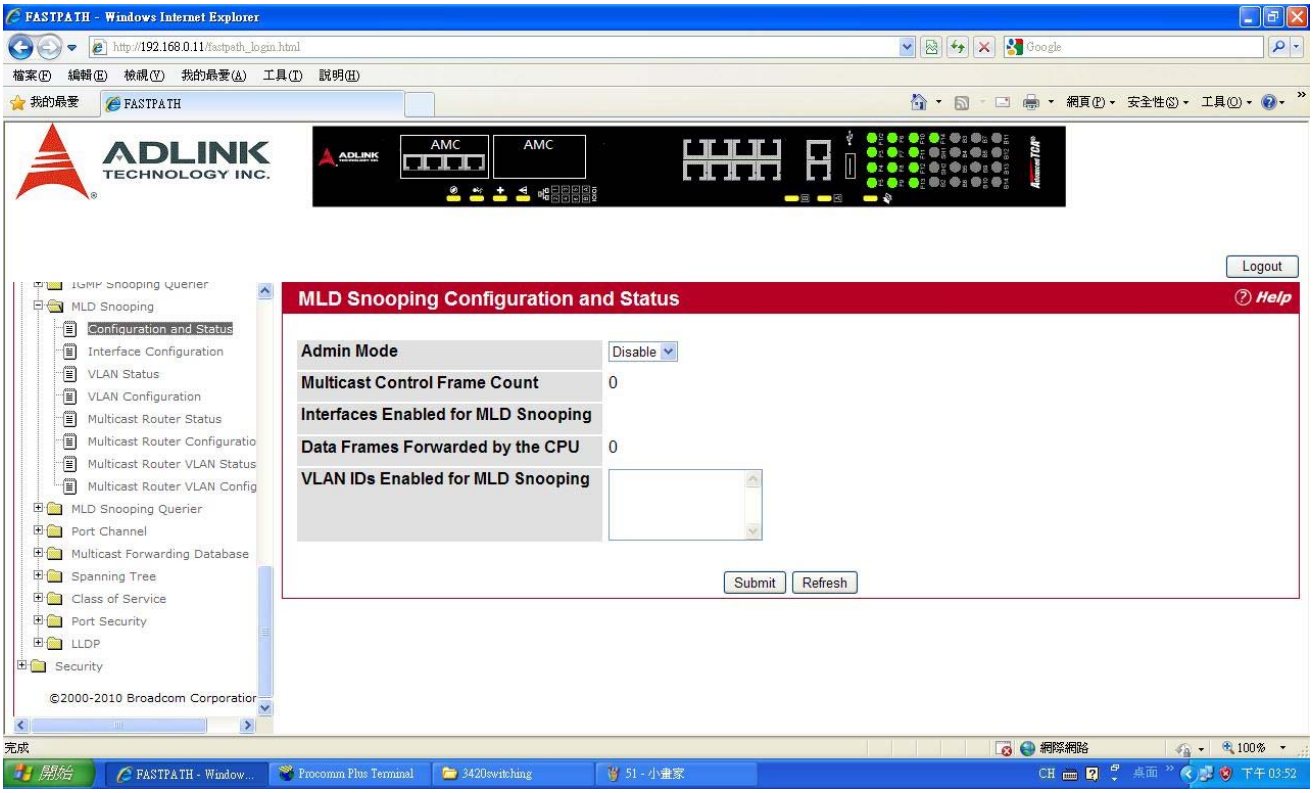
MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on its directly-attached links and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD version 1 (MLDv1) 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 Switching > MLD Snooping > Configuration and Status in the navigation tree.



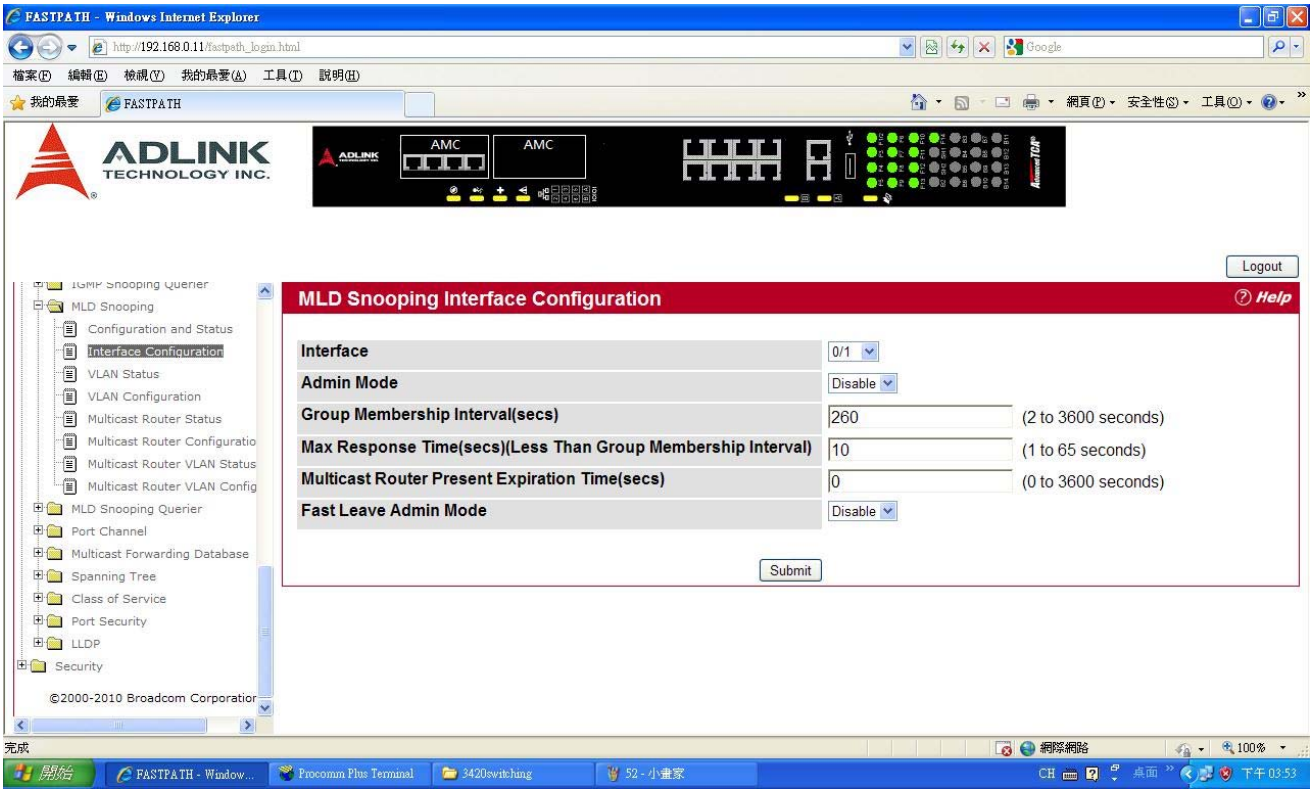
Field	Description
Admin Mode	Select the administrative mode for MLD Snooping for the switch from the pulldown menu. The default is disable.
Multicast Control Frame Count	Shows the number of multicast control frames that have been processed by the CPU.
Interfaces Enabled for MLD Snooping	Lists the interfaces currently enabled for MLD Snooping. To enable interfaces for MLD snooping, see “Interface Configuration”.
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”.

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 Switching > MLD Snooping > Interface Configuration in the navigation tree.



Field	Description
Interface	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.
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

Field	Description
	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 Switching > MLD Snooping > VLAN Status in the navigation tree.

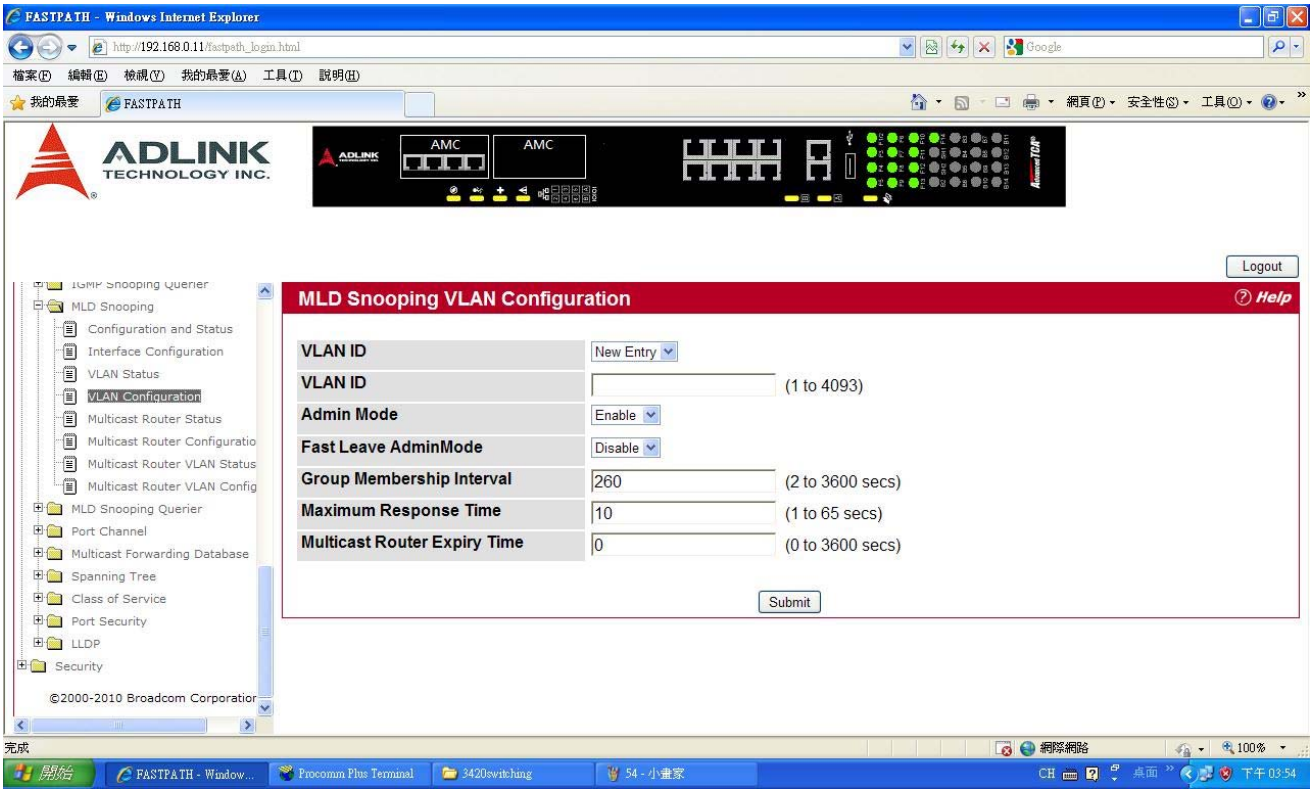


Field	Description
VLAN ID	Displays the VLAN IDs for which the MLD Snooping mode is Enabled.
Admin Mode	Shows the MLD Snooping Mode for the VLAN ID.
Fast Leave Admin Mode	Indicates whether MLD Snooping Fast-leave is active on the VLAN.
Group Membership Interval	Shows the amount of time in seconds that 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 Switching > MLD Snooping > VLAN Configuration in the navigation tree.



Field	Description
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

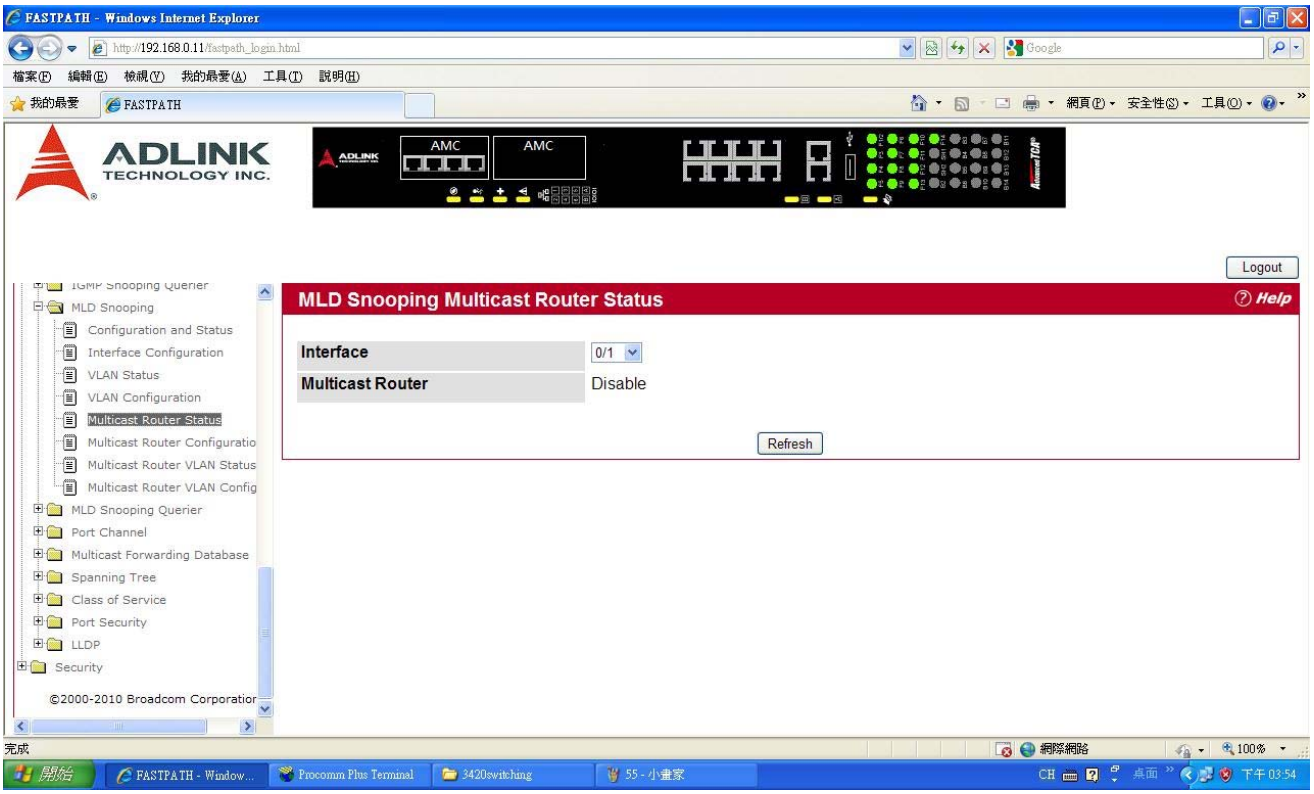
Field	Description
	value must be greater than the Maximum Response time value. The range is 2 to 3600 seconds.
Maximum Response Time	Enter the amount of time in seconds that a switch will wait after sending a query on an interface because it did not receive a report for a particular group in that interface. This value must be less than the Group Membership Interval value. The range is 1 to 3599 seconds.
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 Status

Use the MLD Snooping Multicast Router Status page to view multicast router functionality on selected ports. To access this page, click Switching > MLD Snooping > Multicast Router Statistics in the navigation tree.



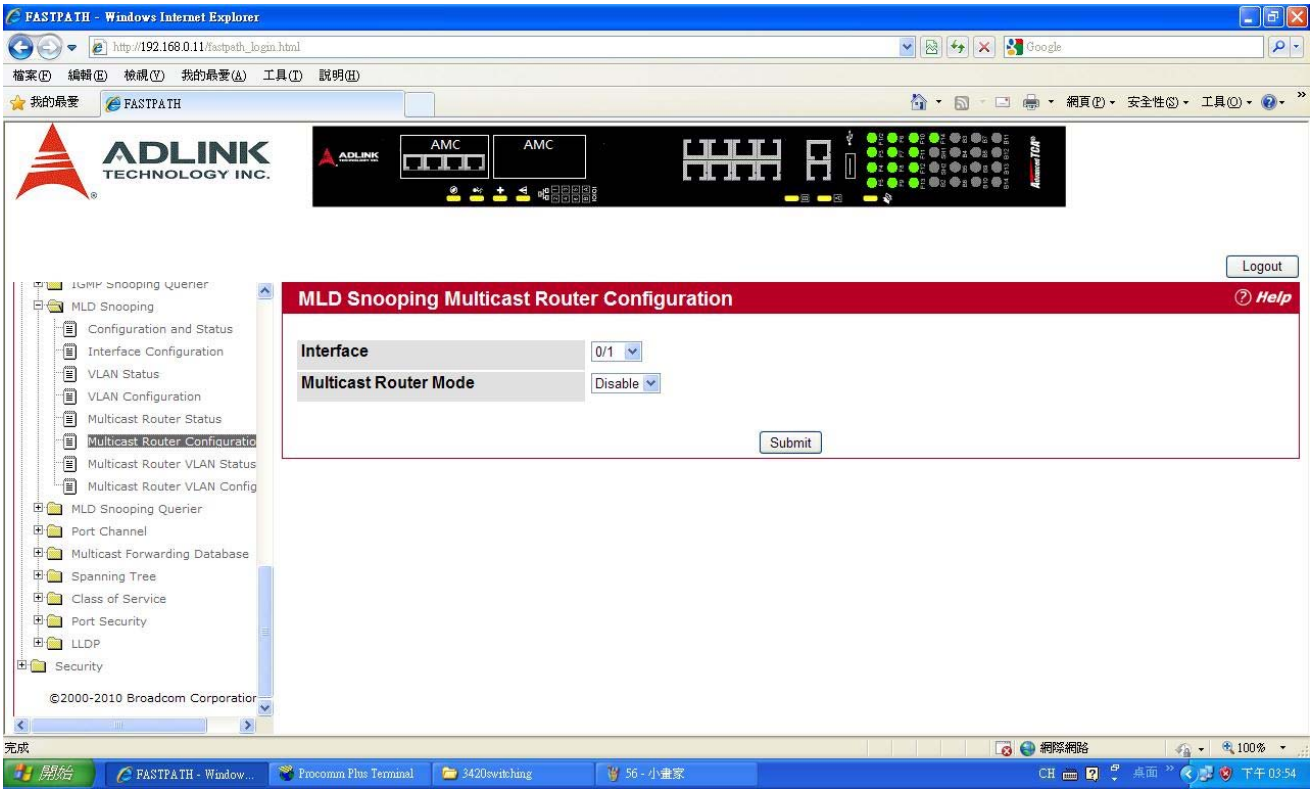
Field	Description
Interface	Select the unit, slot and port number with the information to view.
Multicast Router	Indicates whether the specified interface is configured to perform multicast routing.

Click Refresh to re-display the page with the latest information from the router.

Multicast Router 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 Switching > MLD Snooping > Multicast Router Configuration in the navigation tree.



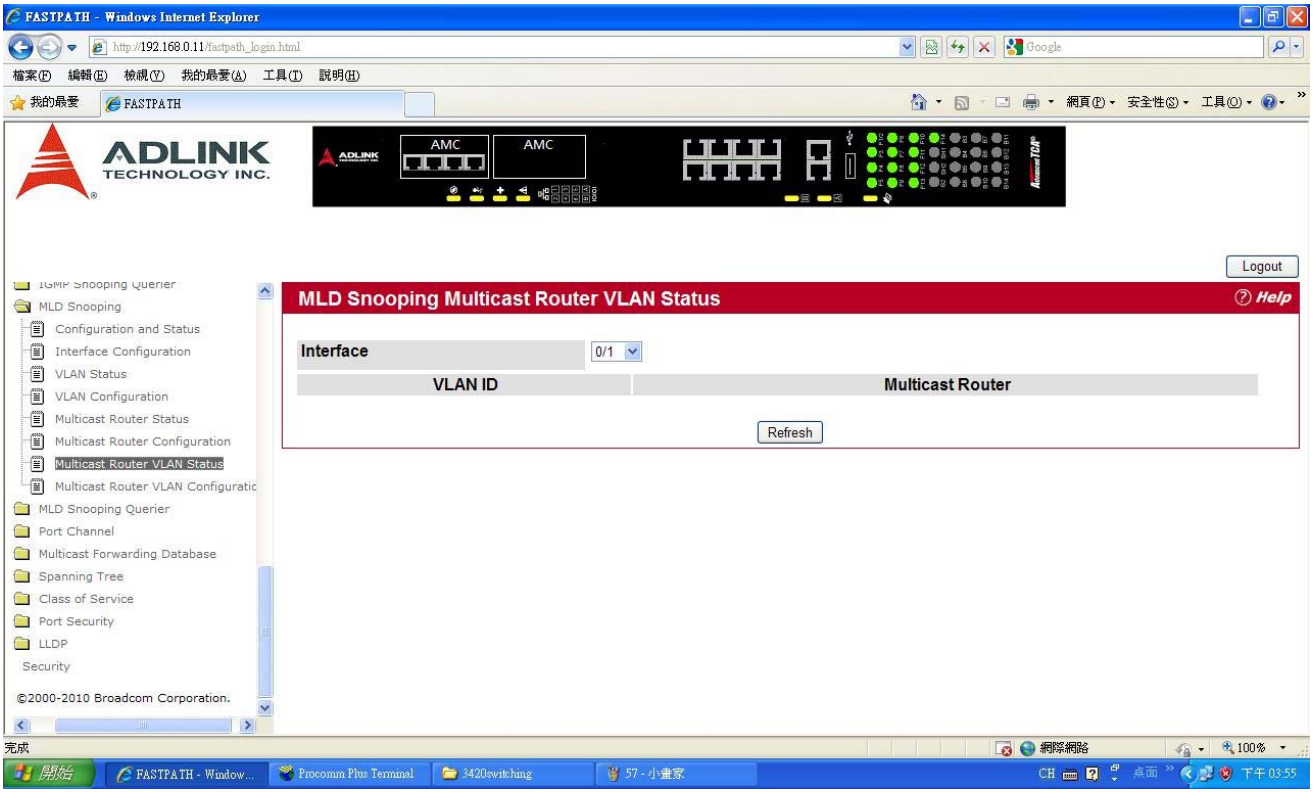
Field	Description
Interface	Select the physical or LAG interface to display.
Multicast Router	Set the multicast router status: • Enabled: The port is a multicast router interface. • Disabled: The port does not have multicast router configured.

If you enable or disable multicast router configuration on an interface, click Submit to apply the new settings to the switch.

Multicast Router 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 Switching > MLD Snooping > Multicast Router VLAN Status in the navigation tree.



Field	Description
Interface	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.

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 Switching > MLD Snooping > Multicast Router VLAN Configuration in the navigation tree.

Field	Description
Interface	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.

5.16 Configuring MLD Snooping Queriers

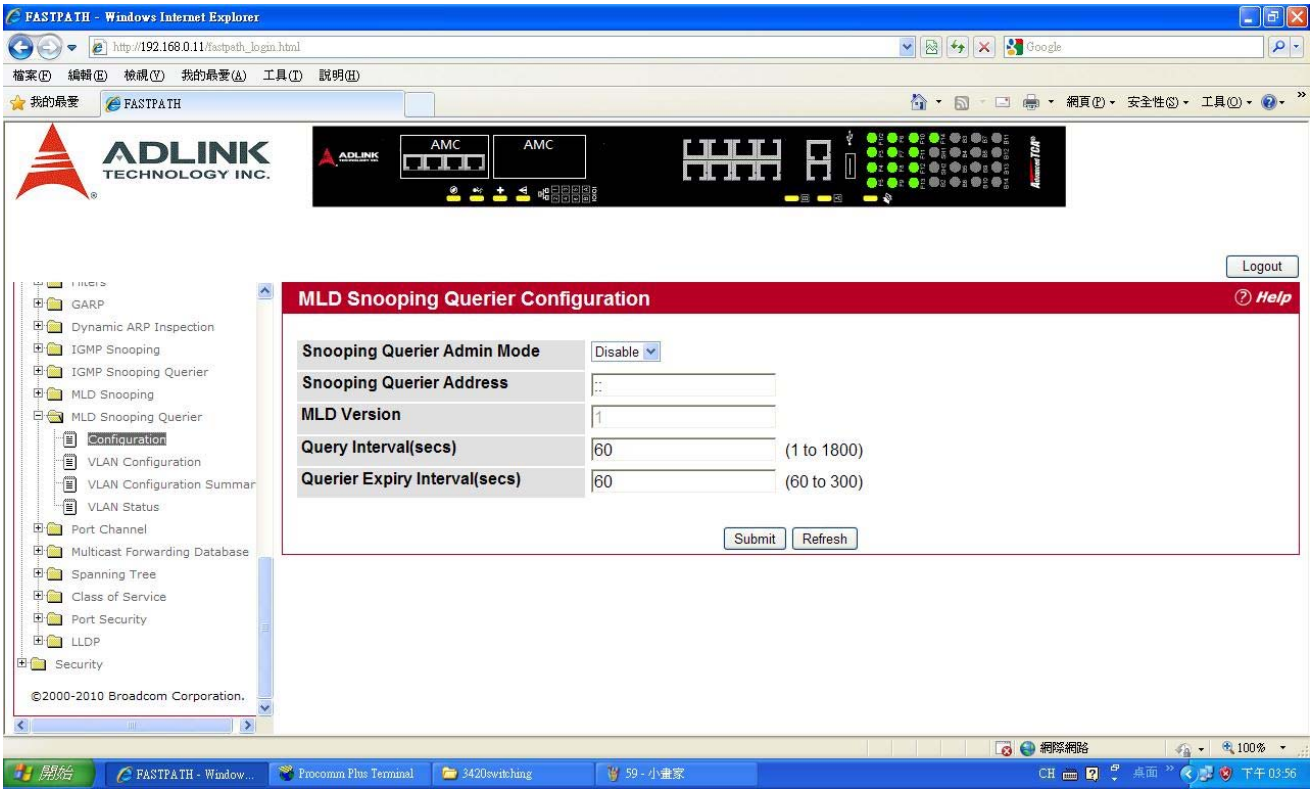
In an IPv6 environment, MLD Snooping requires that one central switch or router periodically query all end-devices on the network to announce their multicast memberships. This central device is the 'MLD querier'. The MLD query responses, known as MLD reports, keep the switch updated with the current 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 multicasts 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 Switching > MLD Snooping Querier > MLD Snooping Querier Configuration in the navigation tree.



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 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.
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.

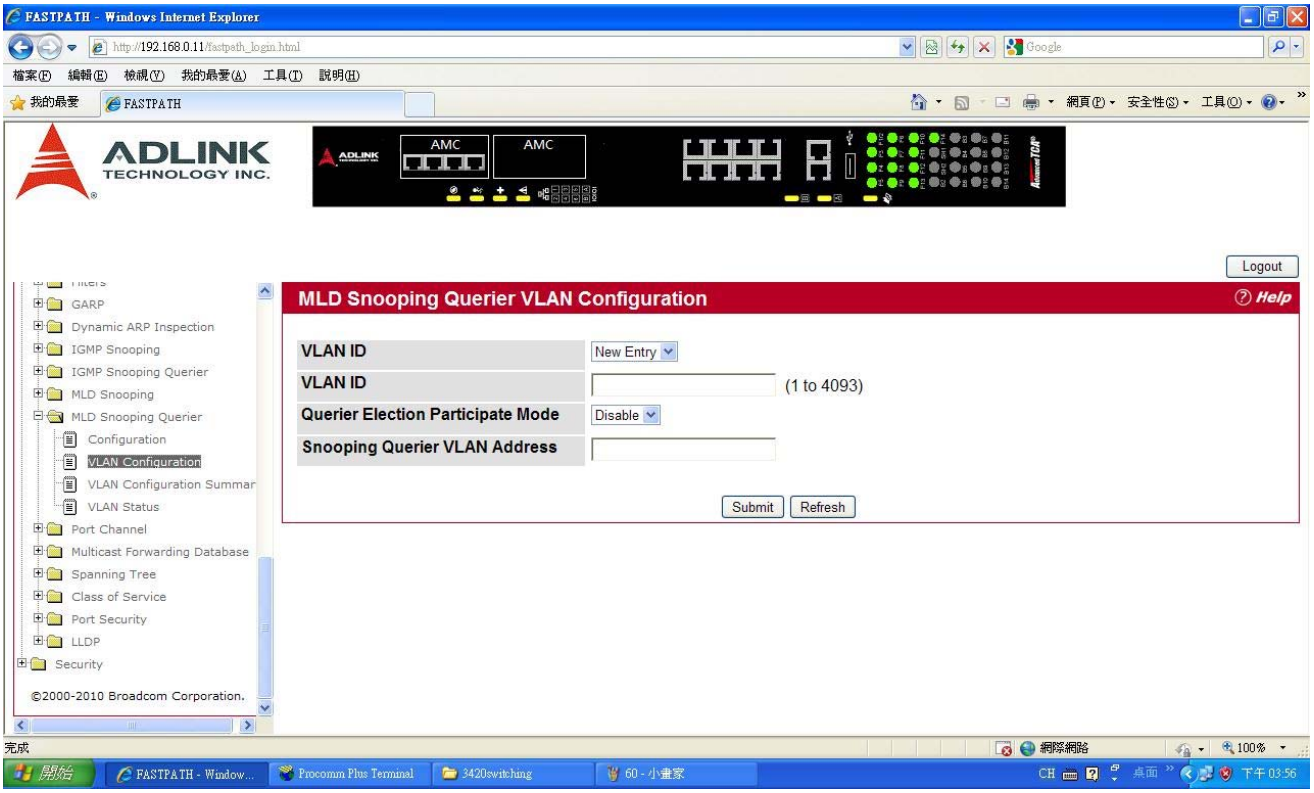
If you configure an MLD Snooping querier, click Submit to apply the new settings to the switch.

Click Refresh to redisplay 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 Switching > MLD Snooping Querier > MLD Snooping Querier VLAN Configuration in the navigation tree.



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 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 redisplay 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 Switching > MLD Snooping Querier > MLD Snooping Querier VLAN Configuration Summary in the navigation tree.



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 address in periodic IGMP queries sent on the specified VLAN.

Click Refresh to redisplay 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 Switching > MLD Snooping Querier > MLD Snooping Querier VLAN Status in the navigation tree.



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: • 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,

Field	Description
	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 redisplay the page with the latest information from the switch.

5.17 Creating Port Channels

Port-channels, 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-channel. The port channel by default becomes a member of the management VLAN.

A port-channel (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-channel interface does not require a partner system to be able to aggregate its member ports.

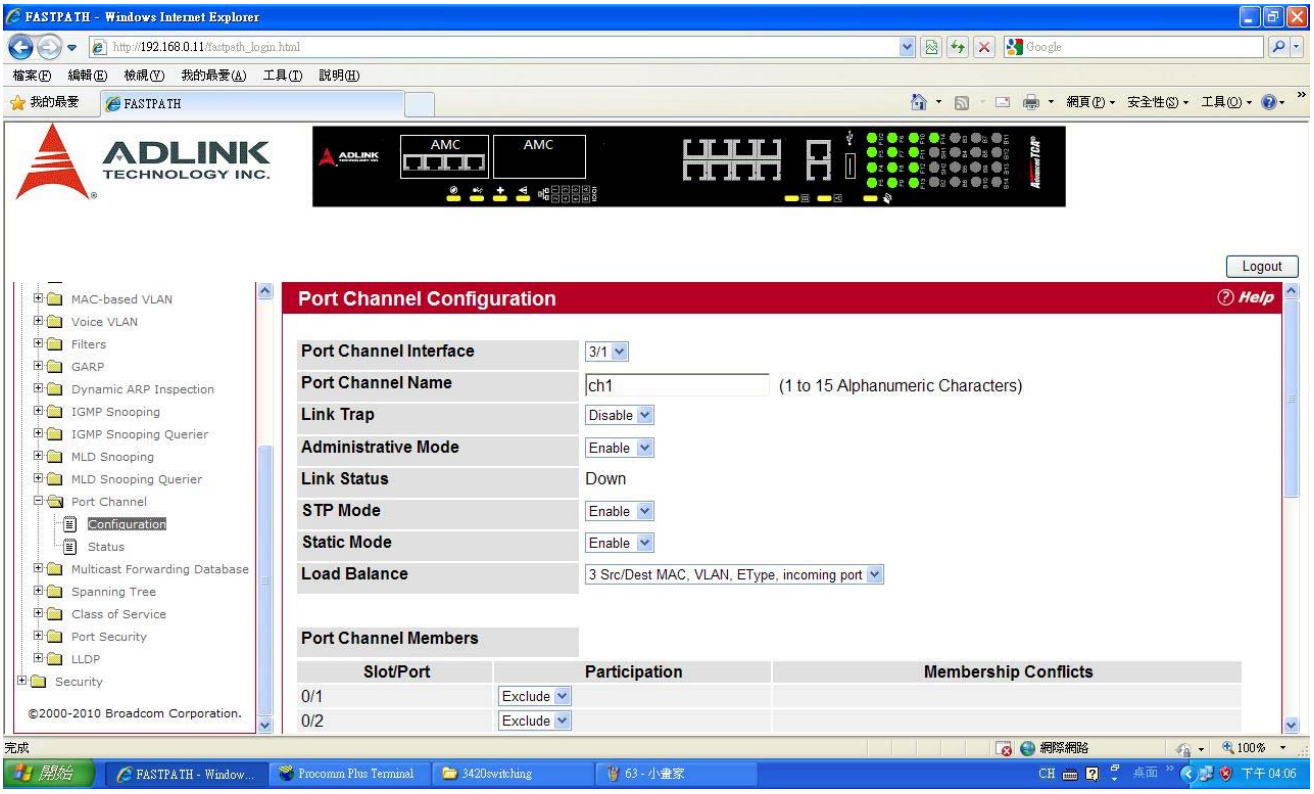
Note: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

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 Switching > Port Channel > Configuration in the navigation tree.



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.
Interface	After you create the port channel, this field identifies the Port Channel with the Slot/Port (or Interface for stacking platforms) 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.

Field	Description
Administrative Mode	Select enable or disable from the pulldown menu. When the Port Channel is disabled no traffic will flow and LACPDUs 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: • 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. • 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: •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.
Interface	This column lists the physical ports available on the system.
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. • Include: The port participates in the port channel. • Exclude: The port does not participate in the port channel, which is the default.

Field	Description
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

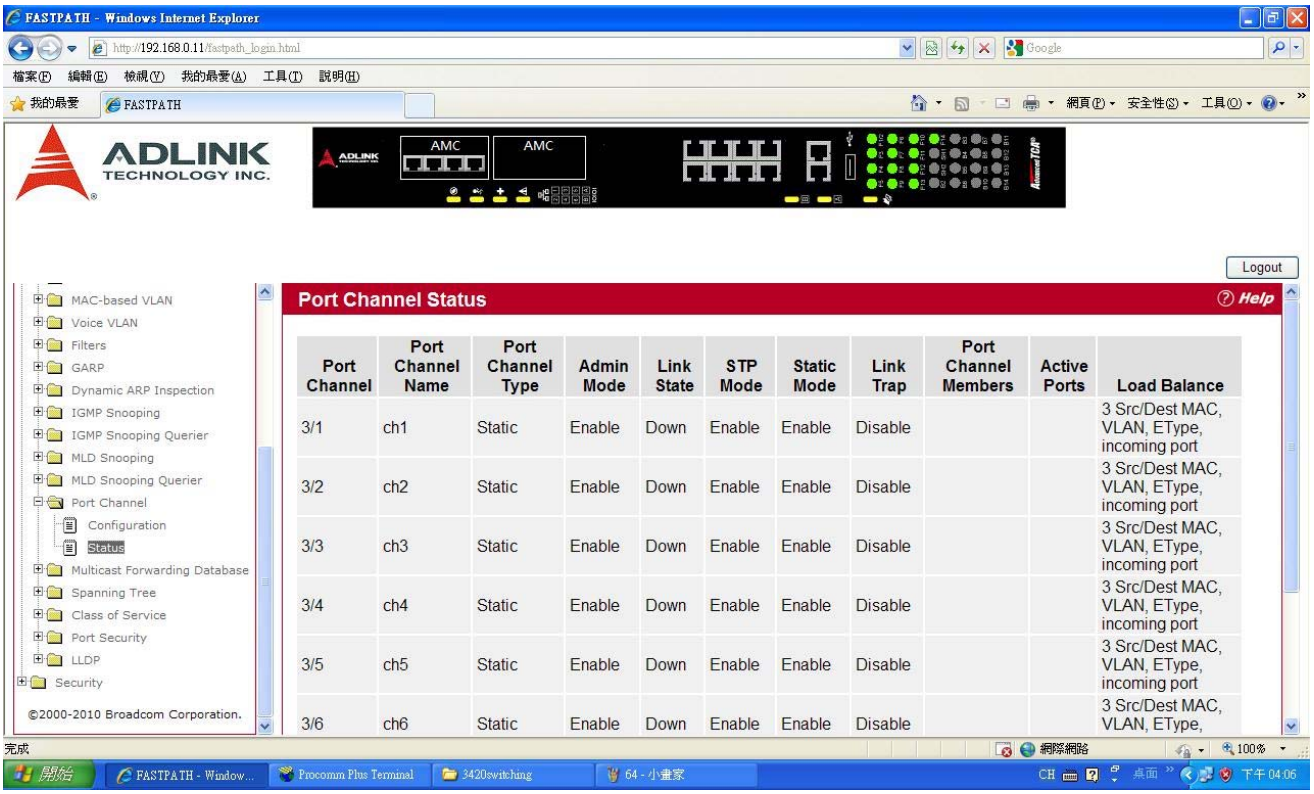
If you make any changes to this page, click Submit to apply the changes to the system.

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 Switching > Port Channel > Status in the navigation tree.



Field	Description
Port Channel	Identifies the port channel with the Slot/Port (or Interface for stacking platforms) 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: • Static: The port channel is statically maintained. • Dynamic: The port channel is dynamically maintained.
Admin Mode	Select enable or disable from the pulldown menu. When the Port Channel is disabled no traffic will flow and LACPDUs 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

Field	Description
Link Trap	Shows whether to send traps when link status changes. If the status is Enabled, traps are sent.
Static Mode	Shows whether static mode is enabled for this port channel.
Configured Ports	Lists the ports that are members of the Port Channel, in Slot/Port notation (Interface for stackable systems). 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 (Interface for stackable systems).
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: •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

5.18 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.

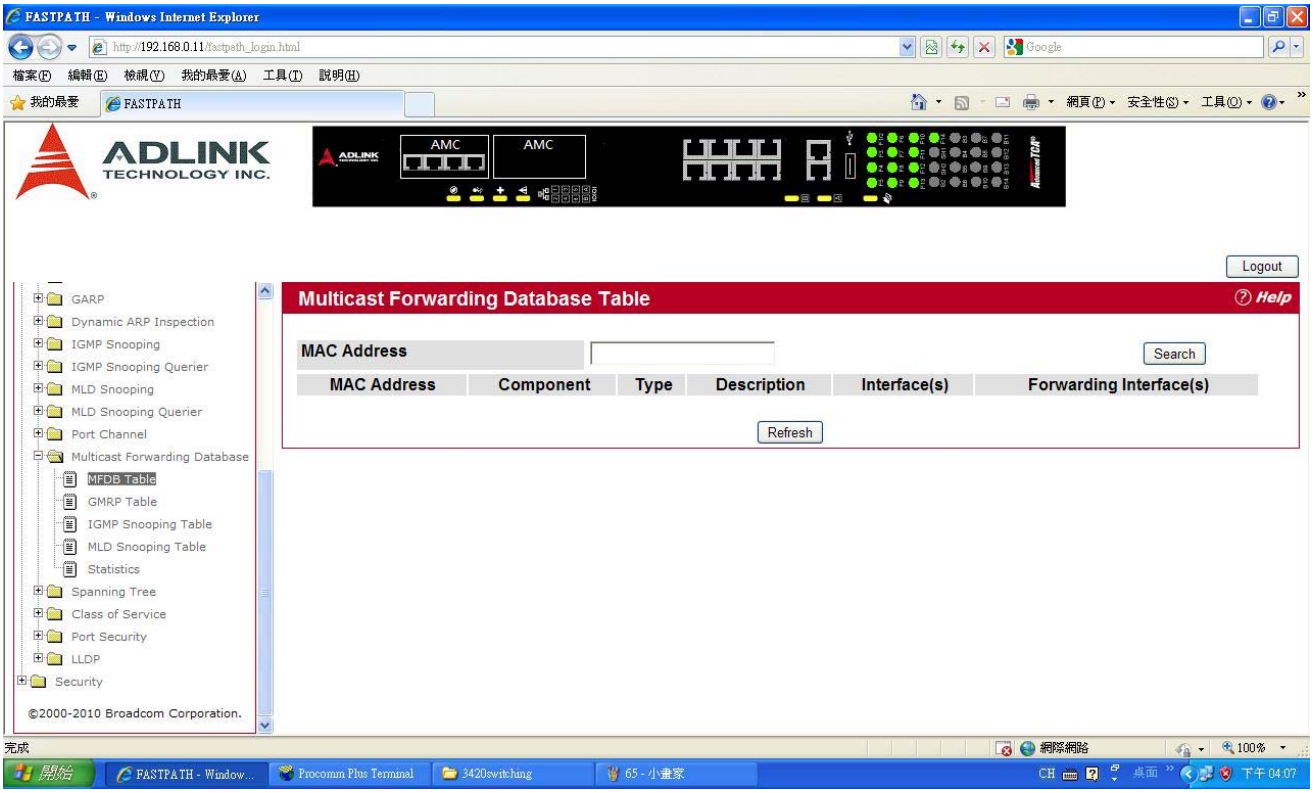
When a packet enters the switch, the destination MAC address is combined with the VLAN ID and a search is performed in the Layer 2 Multicast Forwarding Database. If no match is found, the packet is either flooded to all ports in the VLAN or discarded, depending on the switch configuration. If a match is found, the packet is forwarded only to the ports that are members of that multicast group.

This Multicast Support folder contains links to the following pages:

- MFDB Table
- MFDB GMRP Table
- MFDB IGMP Snooping Table
- MFDB MLD Snooping Table
- MFDB Statistics

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 Switching > Forwarding Database > MFDB Table in the navigation tree.



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. 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

Field	Description
	Management Configured, Network Configured and Network Assisted.
Interface	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the selected address. For platforms that support stacking, the field is Interface.
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.

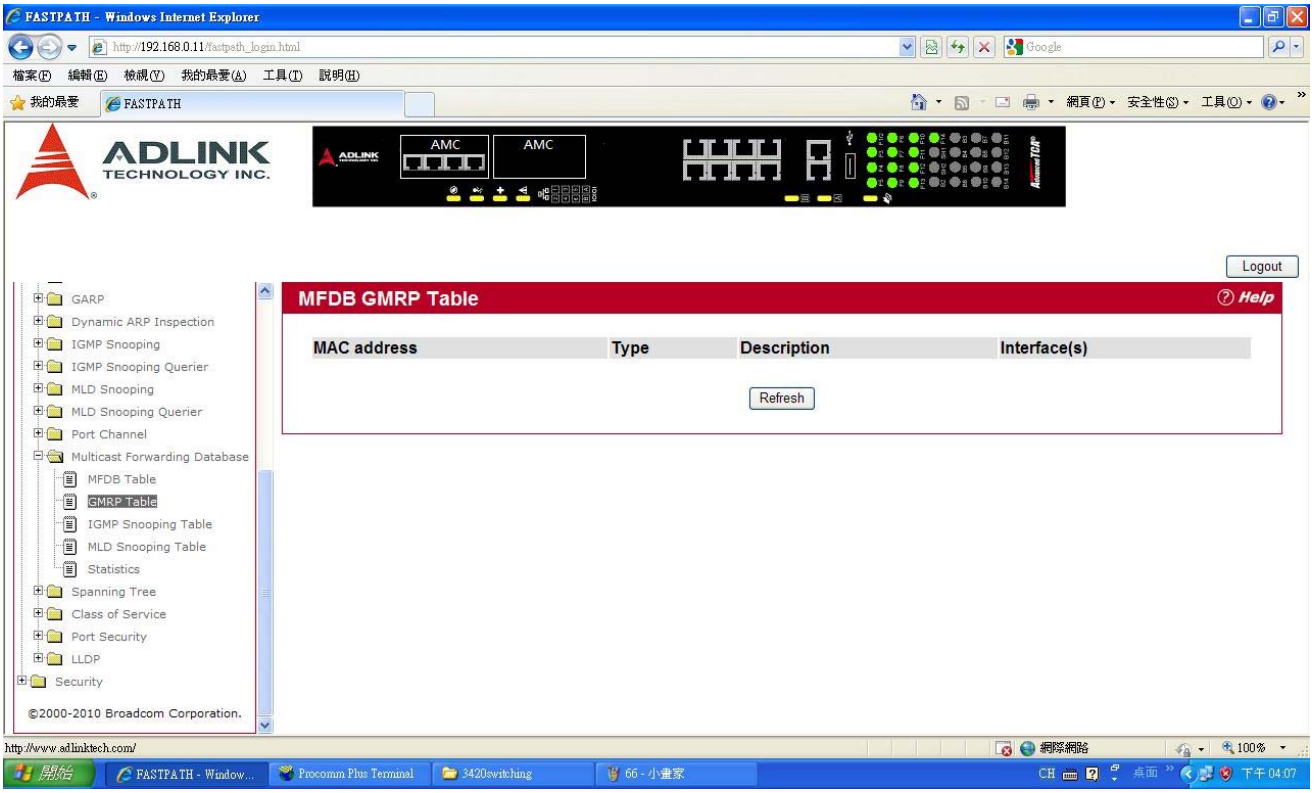
To search for a MAC address if the list is too long to scan, enter the MAC address in hex format and click Search.

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 Switching > Multicast Forwarding Database > GMRP Table in the navigation tree.



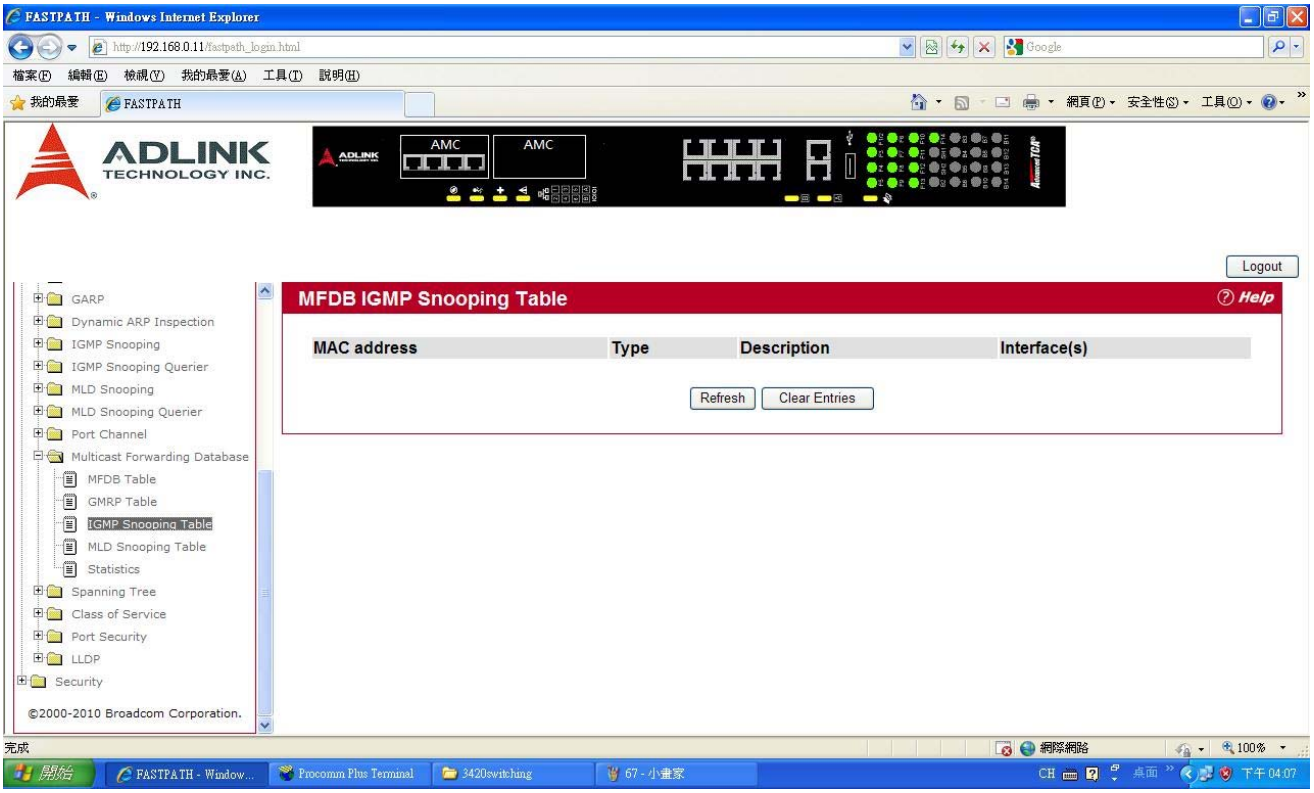
Field	Description
MAC Address	A VLAN ID/multicast MAC address pair for which the switch has forwarding and or filtering information. The format is 8 two-digit hexadecimal numbers that are separated by colons, for example 00:01:23:45:67:89:AB:CD.
Type	This displays the type of the entry. Static entries 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.
Interface	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address. For platforms that support stacking, the field is Interface.

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 Switching > Multicast Forwarding Database > IGMP Snooping Table in the navigation tree.



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.
Interface	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the associated address. For platforms that support stacking, the field is Interface.

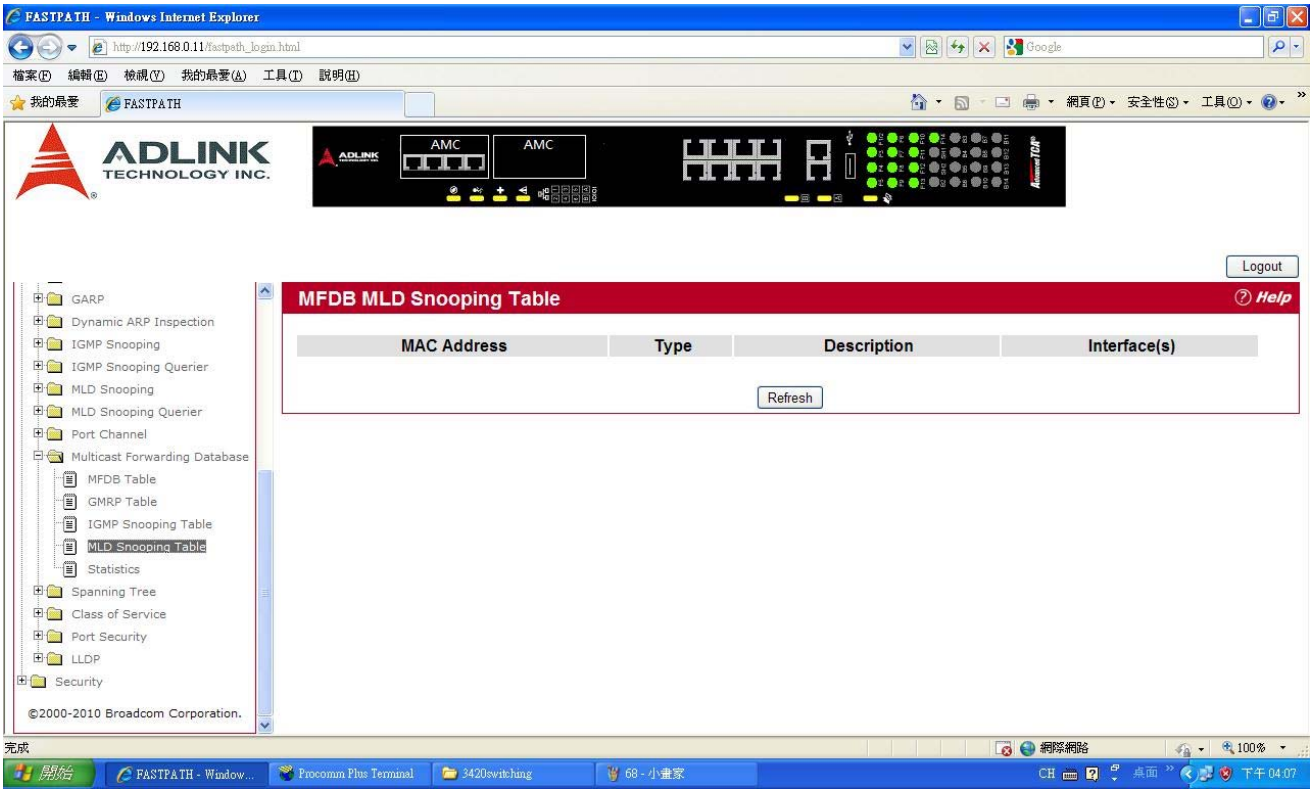
Click Refresh to update the information on the screen with the most current data.

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 Switching > Multicast Forwarding Database > MLD Snooping Table in the navigation tree.



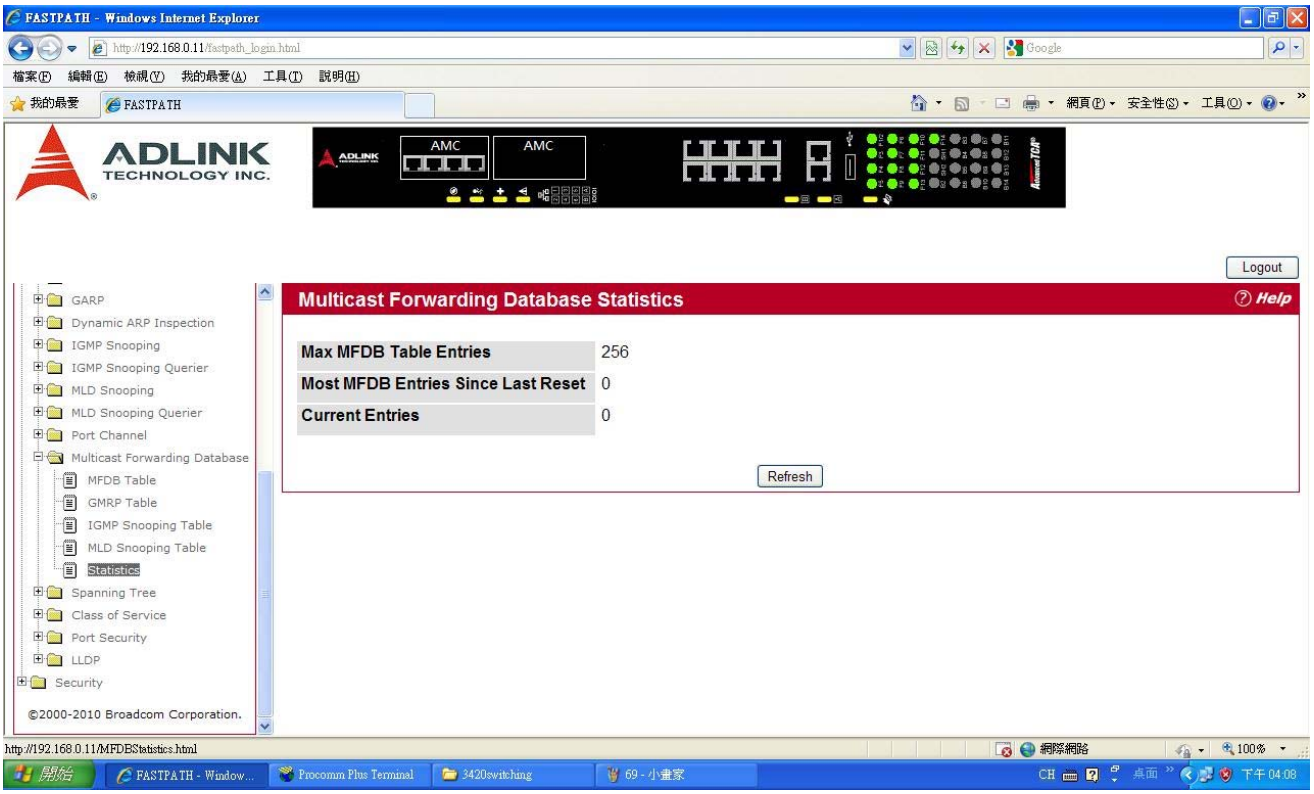
Field	Description
MAC Address	A VLAN ID/multicast MAC address pair for which the switch has forwarding and or filtering information. The format is 8 two-digit hexadecimal numbers that are separated by colons, for example, 00:01:23:45:67:89:AB:CD.
Type	This displays the type of the entry. Static entries 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.
Interface	The list of interfaces that are designated for forwarding (Fwd) and filtering (Flt) for the

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 Switching > Multicast Forwarding Database > Stats in the navigation tree.



Field	Description
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.

5.19 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”.

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.

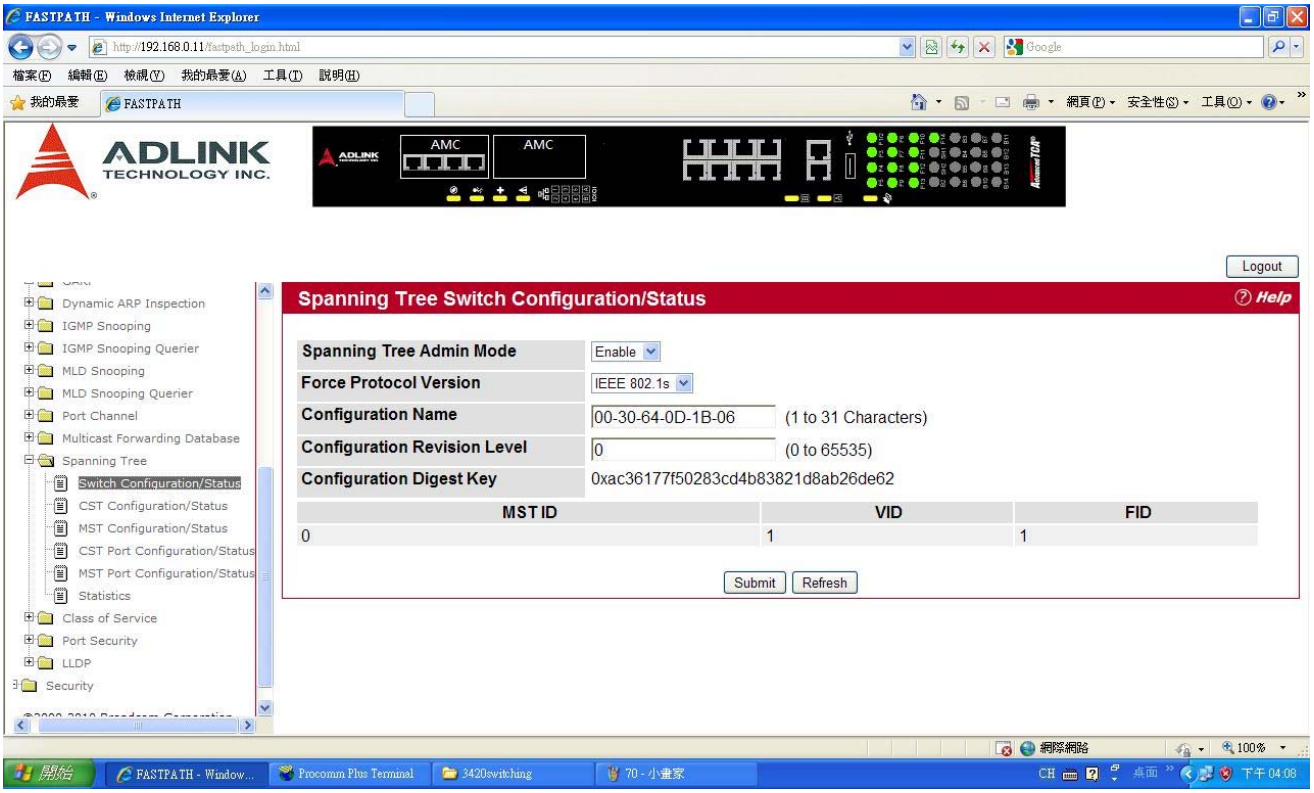
The Spanning Tree folder contains links to the following STP pages:

- Switch Configuration/Status
- CST Configuration/Status
- MST Configuration/Status
- CST Port Configuration/Status
- MST Port Configuration/Status
- Statistics

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 Switching > Spanning Tree > Switch Configuration/ Status in the navigation tree.



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: • 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.

Field	Description
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.

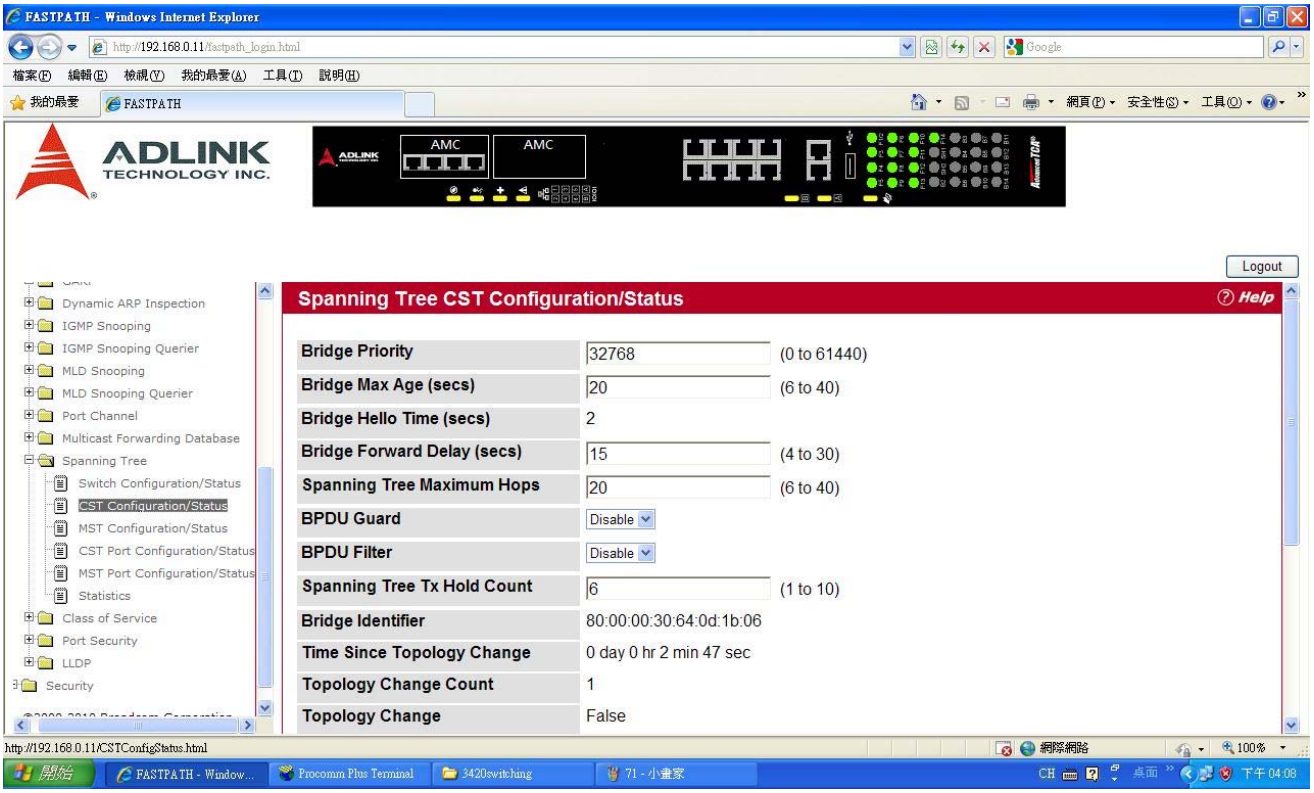
If you make any configuration changes, click Submit to apply the new settings to the switch.

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 Switching > Spanning Tree > CST Configuration/ Status in the navigation tree.



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.
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 * Bridge Forward Delay) – 1 and greater than or equal to 2 * (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 (Bridge Max Age / 2) – 1. The default hello time value is 2.

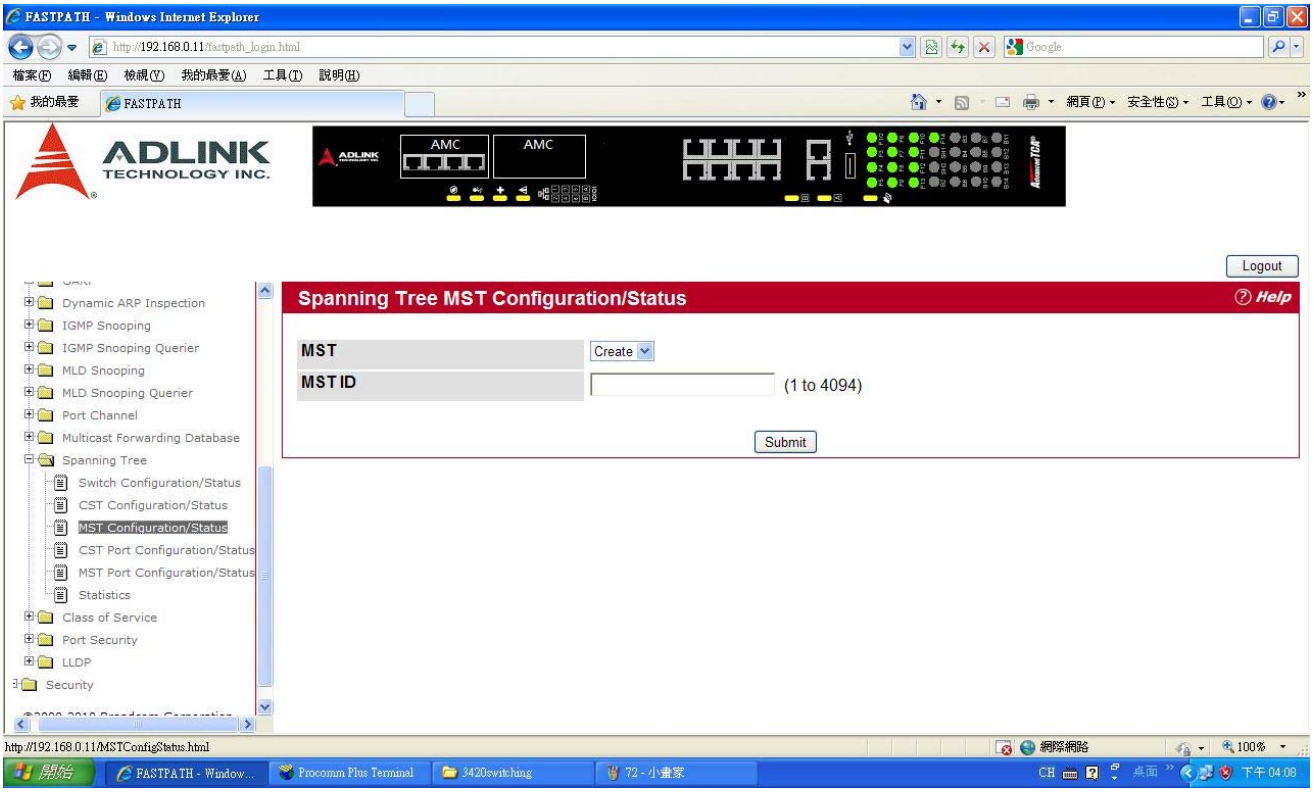
Field	Description
Bridge Forward Delay (secs)	Specifies the switch forward delay time, which indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The value must be greater or equal to (Bridge Max Age / 2) + 1. The time range is from 4 seconds 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 Switching > Spanning Tree ?MST Configuration/ Status 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



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.

Field	Description
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.

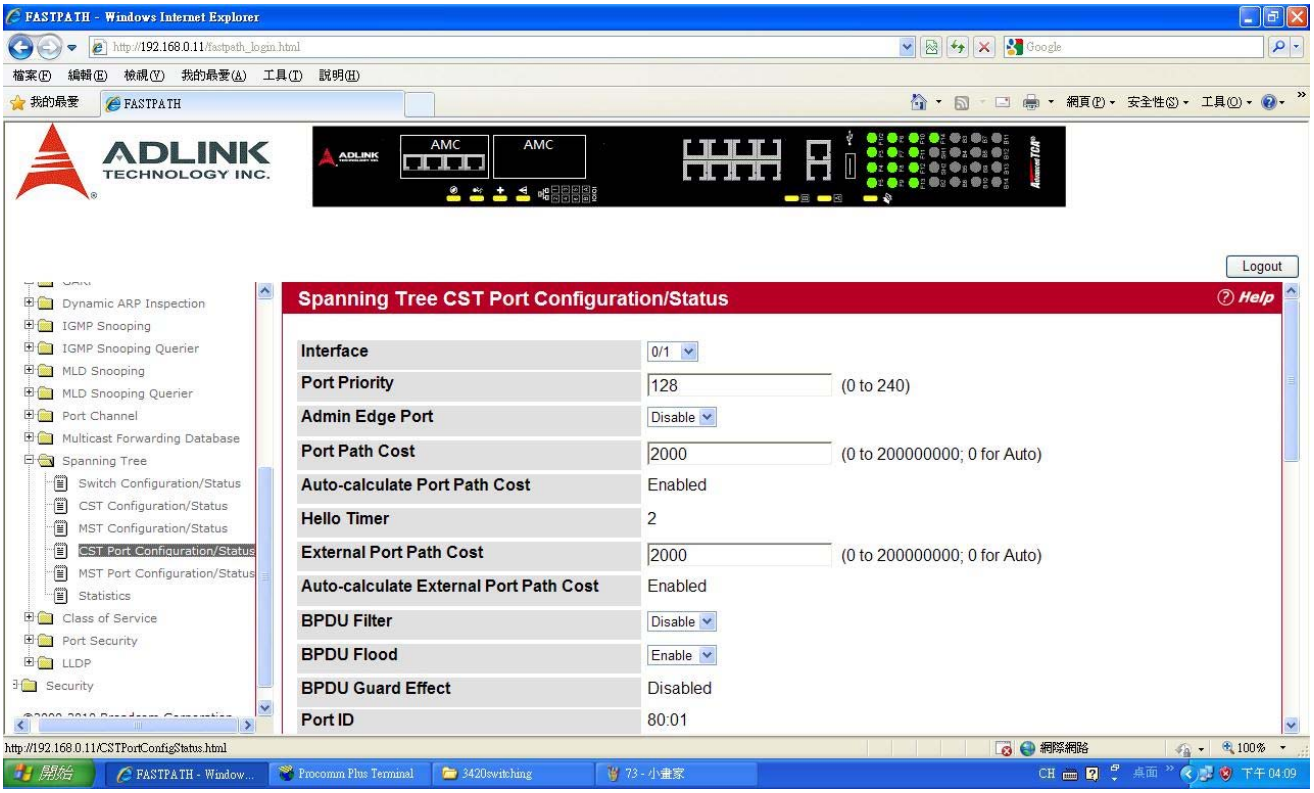
Click Force to force the port to send out 802.1w or 802.1D BPDUs.

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 Switching > Spanning Tree > CST Port Configuration/Status in the navigation tree.



Spanning Tree CST Port Configuration/Status Fields

Field	Description
Interface	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	Displays whether the path cost is automatically calculated (Enabled)

Field	Description
Cost	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 (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.
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: • 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

Field	Description
	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.
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.

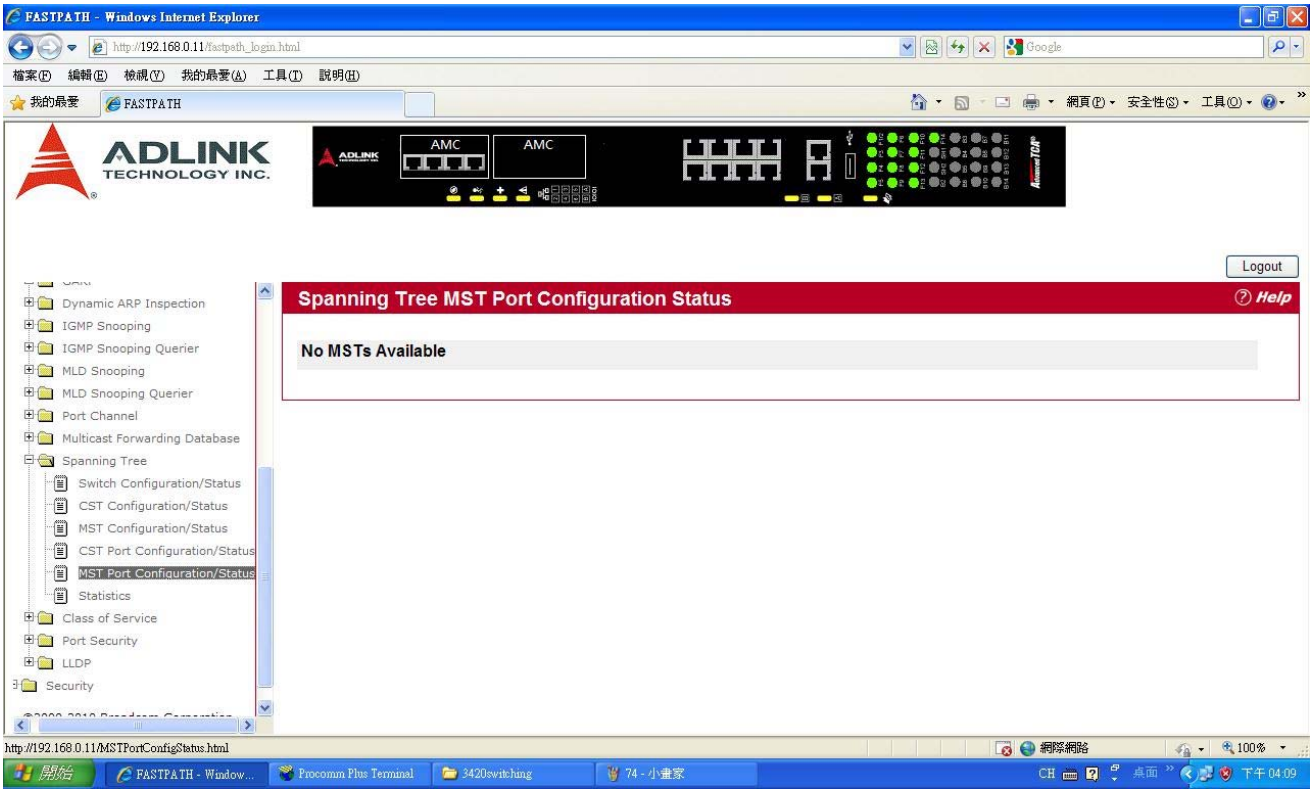
Click Force to force the port to send out 802.1w or 802.1D BPDUs.

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 Switching > 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



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.

Field	Description
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: • 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.
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.

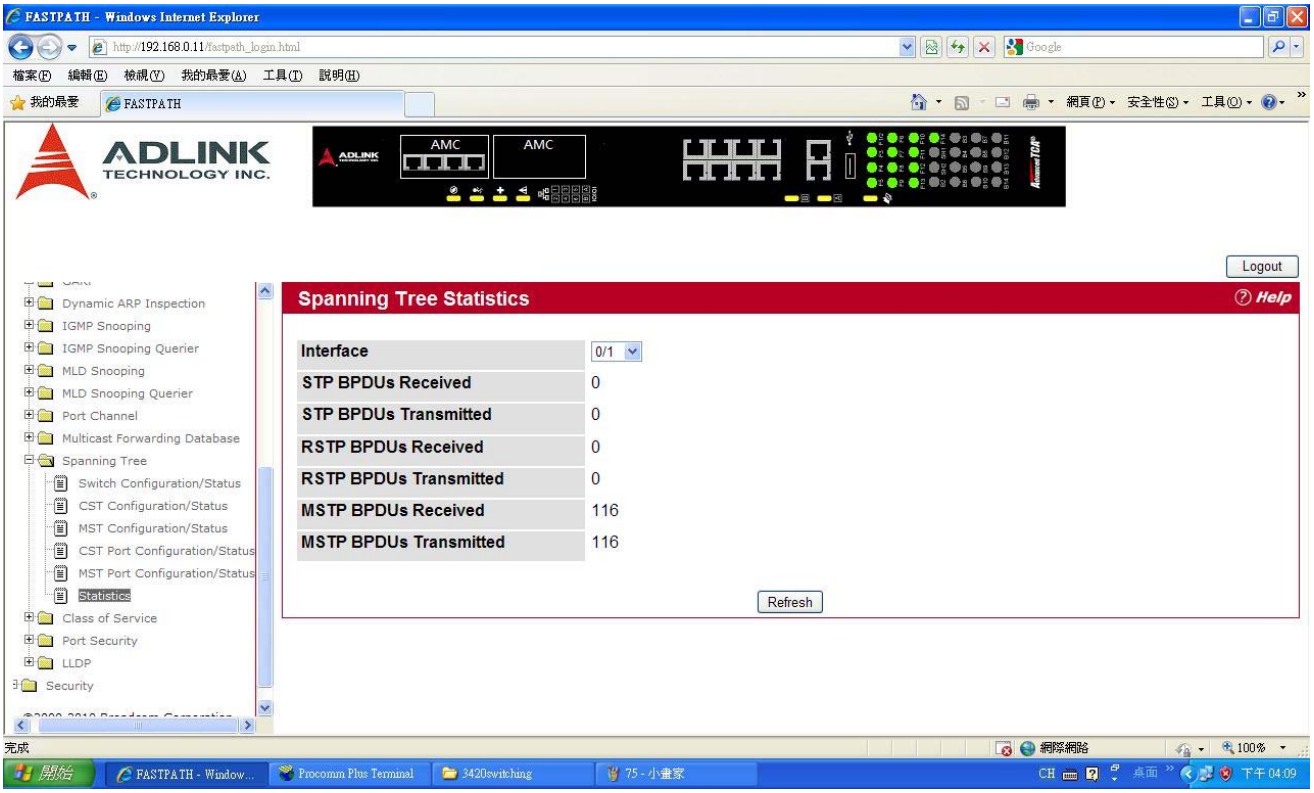
If you make any configuration changes, click Submit to apply the new settings to the switch.

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 Switching > Spanning Tree > Statistics in the navigation tree.

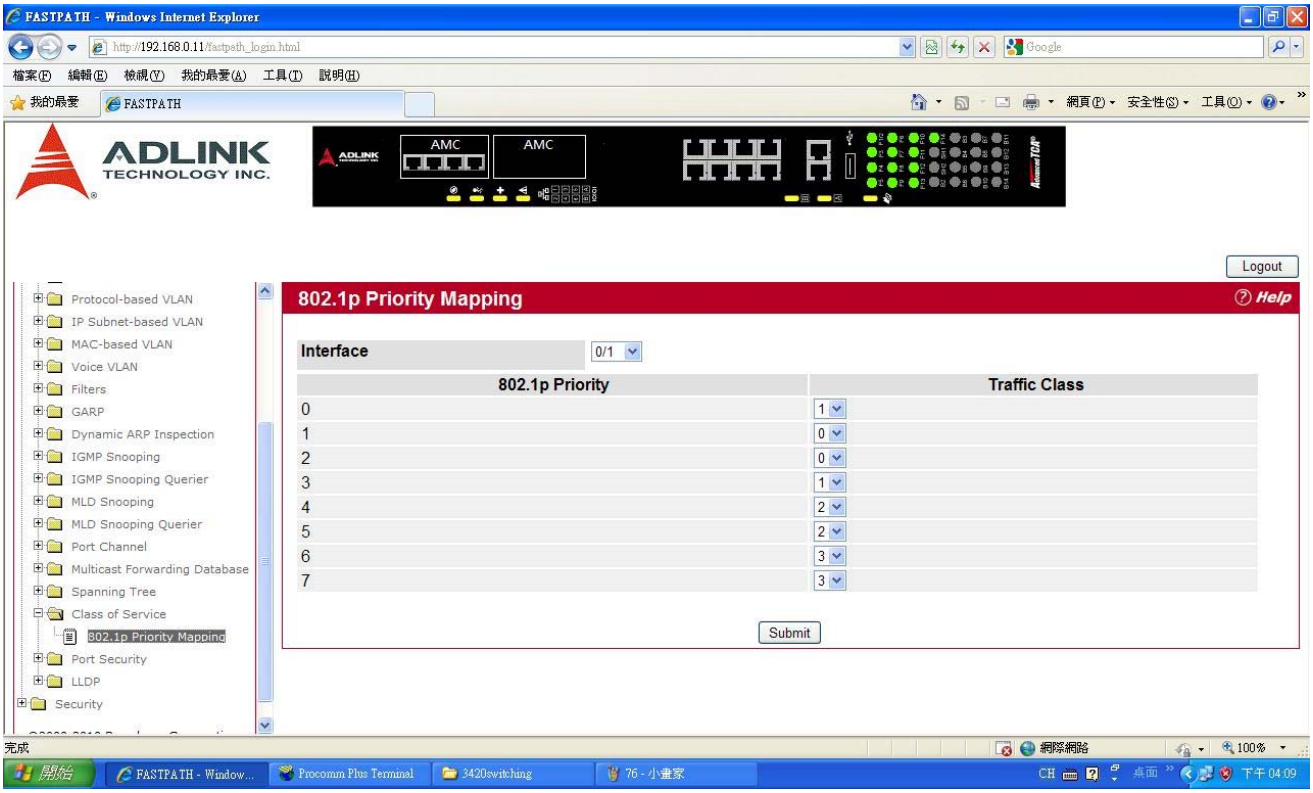


Field	Description
Interface	Select a physical or port channel interface to view its statistics. For platforms that support stacking, the field is Interface.
STP BPDUs Received	Number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Number of STP BPDUs transmitted from the selected port.
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.

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 Switching > Class of Service > 802.1p Priority Mapping in the navigation tree.



Field	Description
Interface	Selects the interface to which the class of service configuration is applied. For platforms that support stacking
802.1p Priority	Displays the 802.1p priority to be mapped. Priority goes from low (0) to high (7). For example
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

If you make any changes to the page, click Submit to apply the new values to the system.

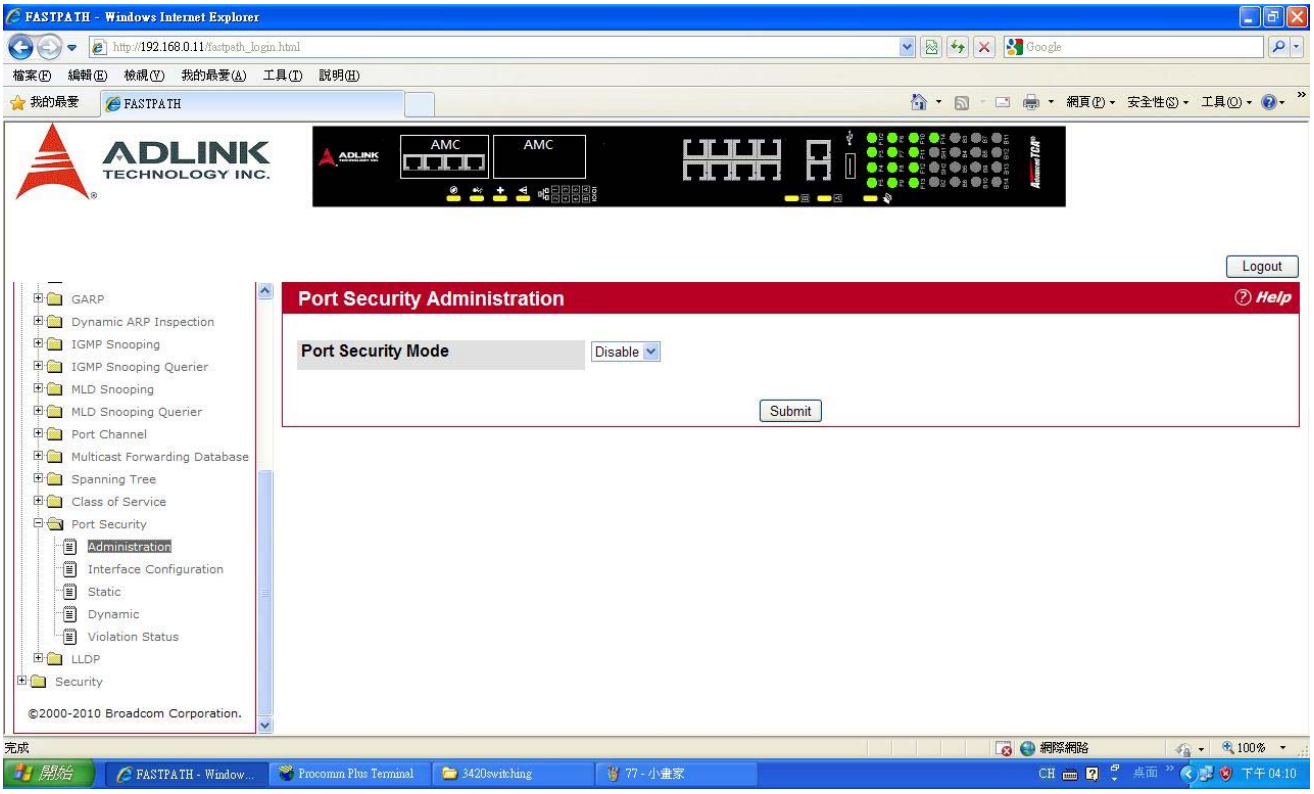
5.20 Configuring Port Security

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, 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”
Disabled ports can only be activated from the Configuring Ports page.
The Port Security folder contains links to the following pages:

- Port Security Administration
- Port Security Interface Configuration
- Port Security Static
- Port Security Dynamic
- Port Security Violation Status

Port Security Administration

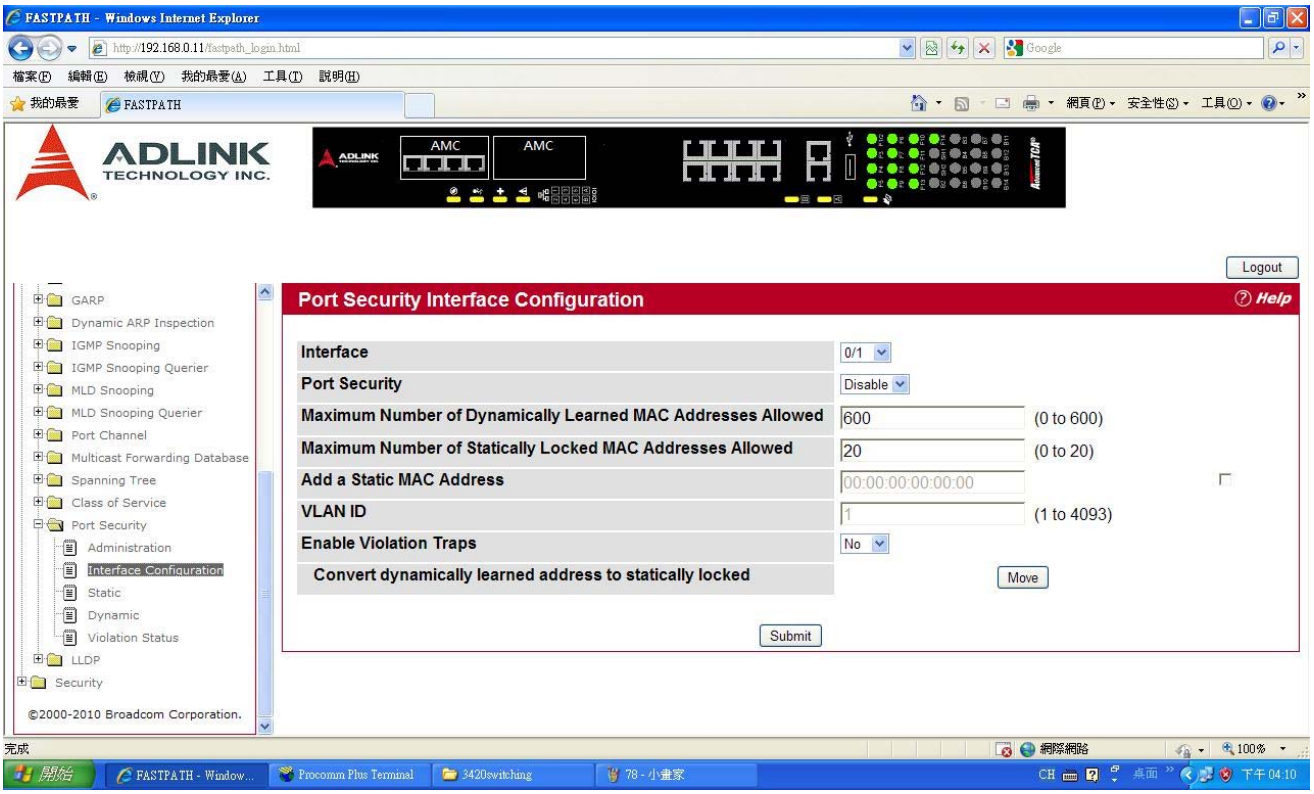
Use the Port Security Administration page to enable or disable the port security feature on your switch.
To access the Port Security Administration page, click Switching > Port Security > Port Security Administration in the navigation tree.



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 Switching > Port Security > Port Security Interface Configuration in the navigation tree.



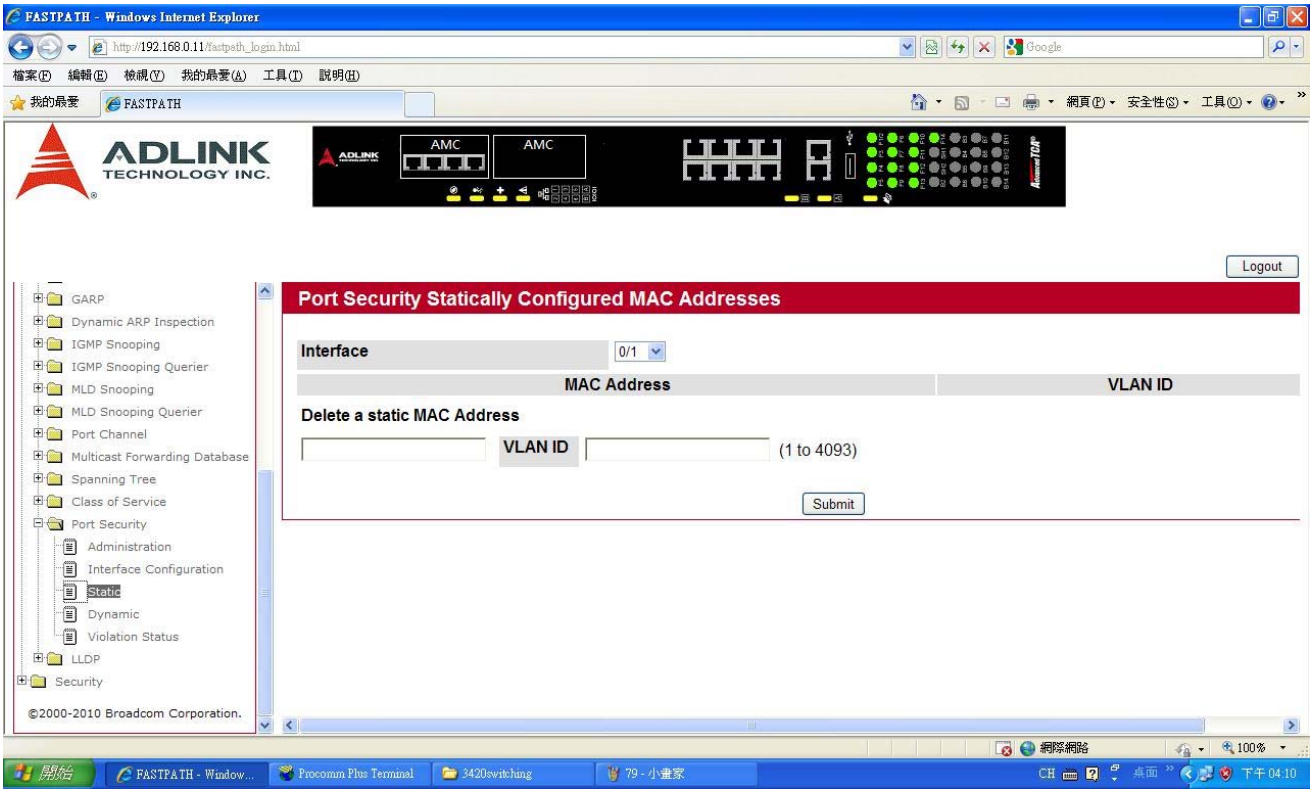
Field	Description
Interface	Select the physical interface or the LAG on which to configure port security information. For platforms that support stacking, the field is Interface.
Port Security	Determines whether port security is enabled. The default mode is Disable. • Enable: Locks the port so that only 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.

Field	Description
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 Switching > Port Security > Port Security Static in the navigation tree.

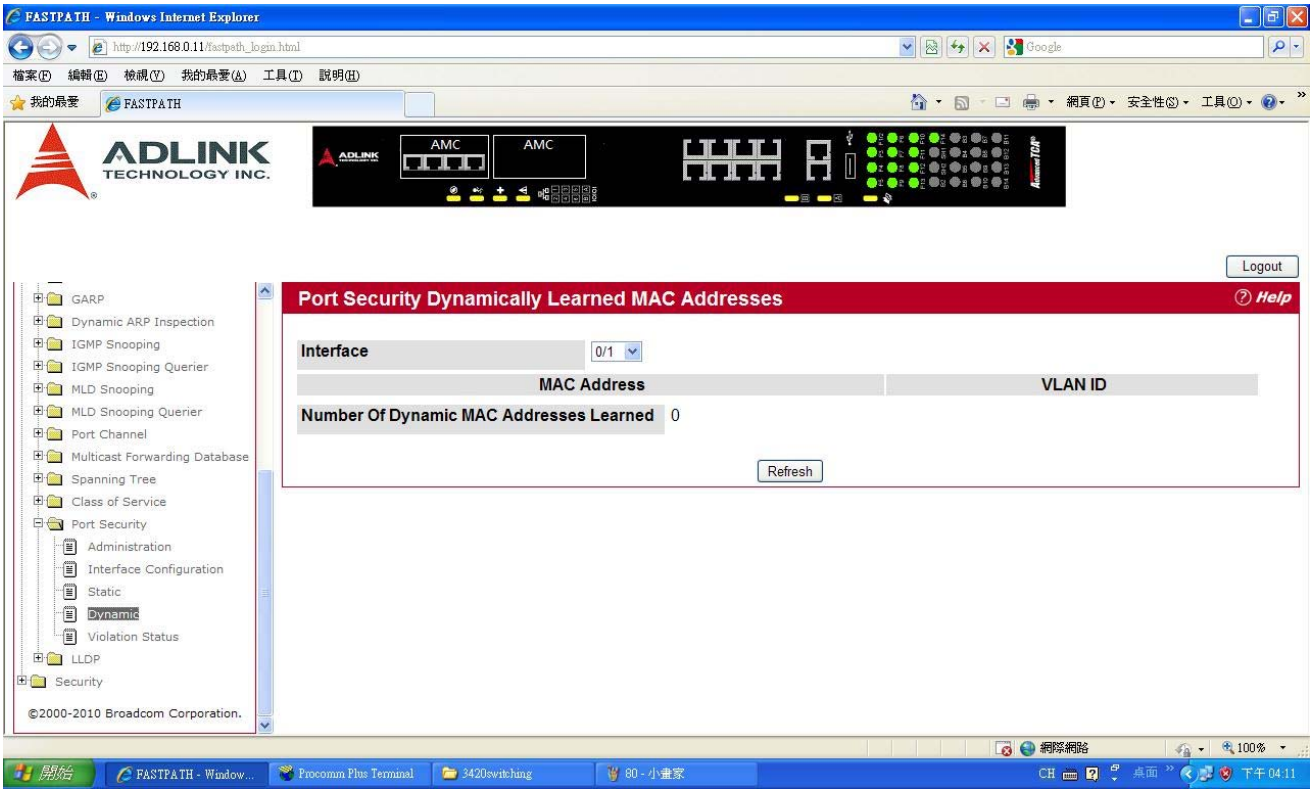


Field	Description
Interface	Select the physical interface or the LAG on which to view the dynamically learned MAC addresses. For platforms that support stacking, the field is Interface.
MAC Address	This column lists the static MAC addresses, if any, configured on the selected port.
VLAN ID	Displays the 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

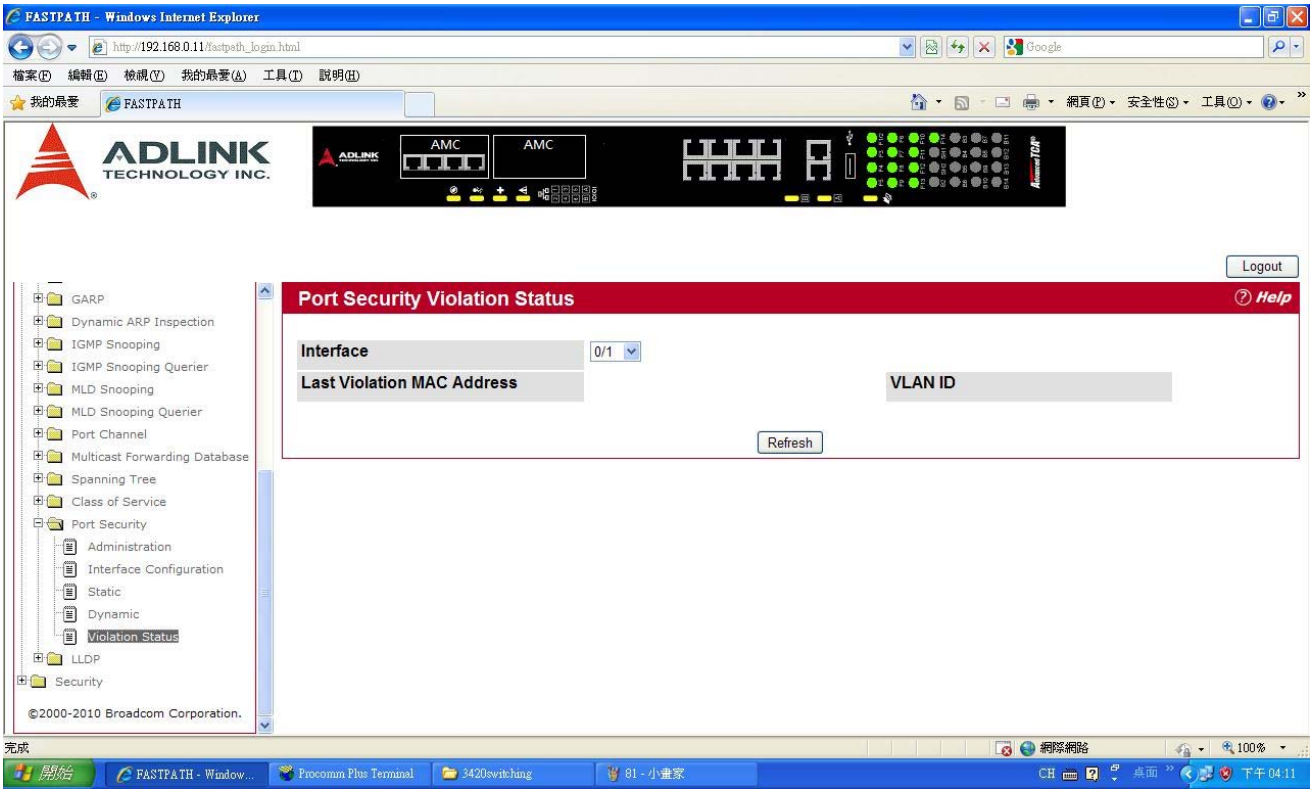
Use the Port Security Dynamic page to view a table with the dynamically learned MAC addresses on an interface. With dynamic locking, MAC addresses are learned on a “first arrival” basis. You specify how many addresses can be learned on the locked port.
To access the Port Security Dynamic page, click Switching > Port Security > Port Security Dynamic in the navigation tree.



Field	Description
Interface	Select the physical interface or the LAG on which to view the dynamically learned MAC addresses. For platforms that support stacking, the field is Interface.
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 Switching > Port Security > Port Security Violation Status in the navigation tree.



Field	Description
Interface	Select the physical interface or the LAG on which to view security violation information. For platforms that support stacking, the field is Interface.
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.

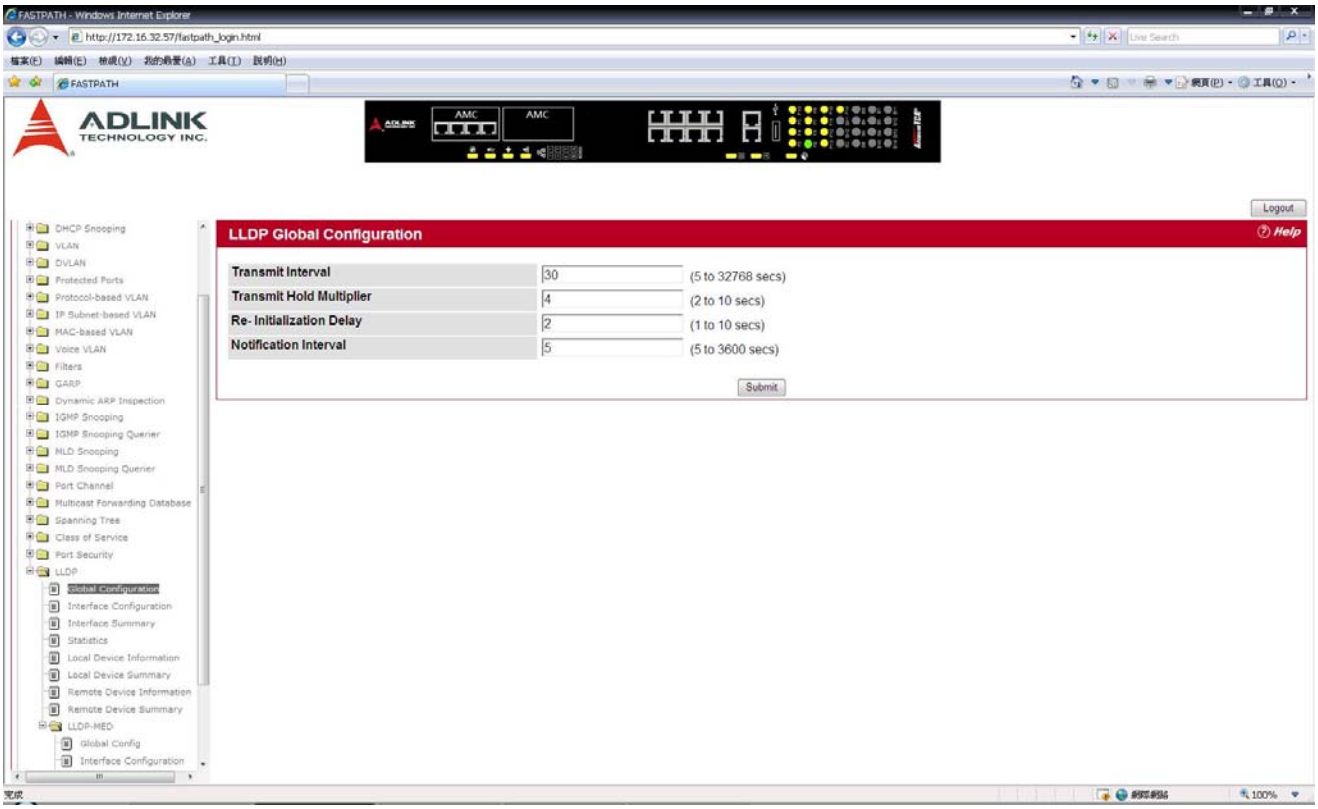
5.21 Managing LLDP

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.
FASTPATH® 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, 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.
The LLDP folder contains links to the following page:

- Global Configuration
- Interface Configuration
- Interface Summary
- Statistics
- Local Device Information
- Local Device Summary
- Remote Device Information
- Remote Device Summary
- LLDP-MED

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 Switching > LLDP > Global Configuration in the navigation tree.



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 second
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 5-3600seconds

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 Switching > LLDP > Interface Configuration in the navigation tree.



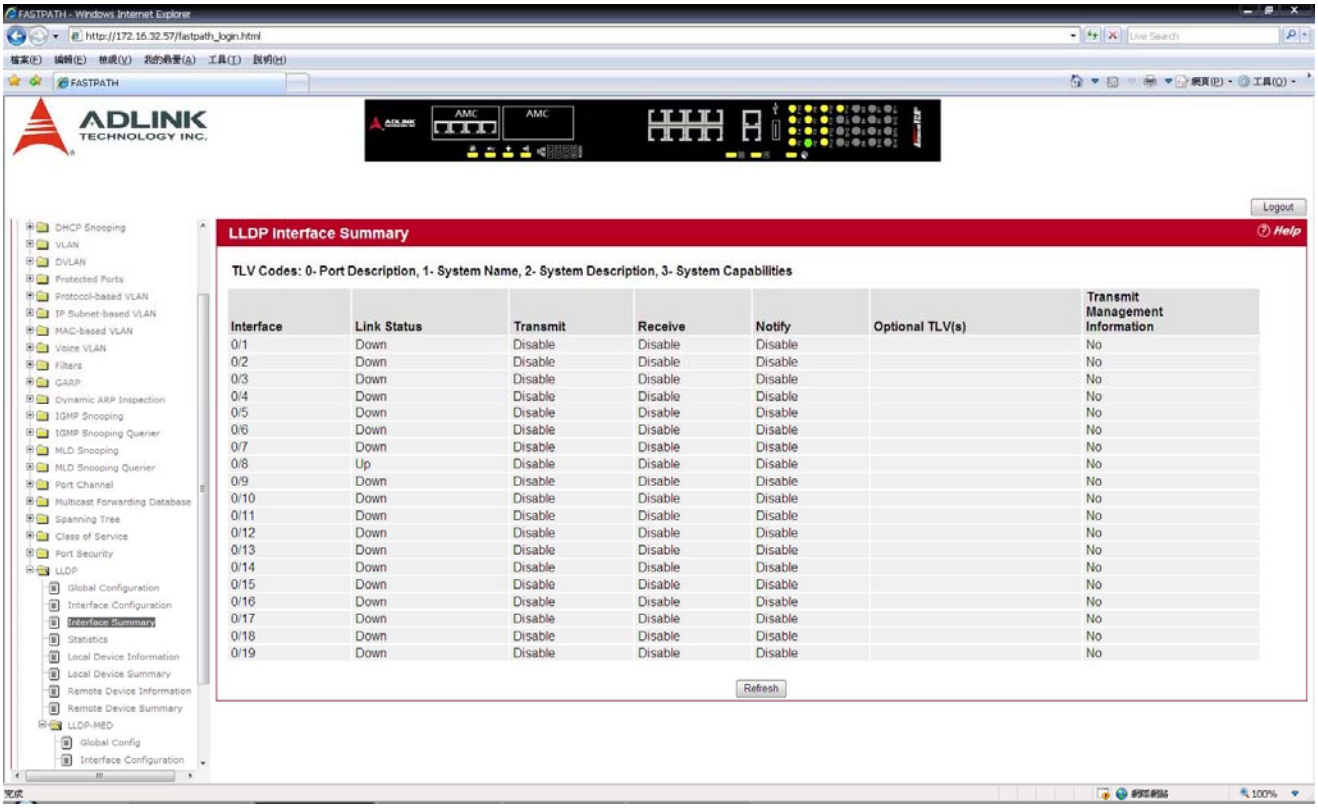
Field	Description
Interface	Specifies the port to be affected by these parameters.
Transmit	Enables or disables the transmission of LLDP protocol data units (PDUs). The default is disabled.
Receive	Enables or disables the ability of the port to receive LLDP PDUs. The default is disabled.
Notify	When 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: •System Name. To include system name TLV in LLDP frames. To configure the System Name, see “System Description” •System Description. To include system description TLV in LLDP frames.

Field	Description
	•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”

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 Switching > LLDP > Interface Summary in the navigation tree.



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. •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 Switching > LLDP > Statistics in the navigation tree.



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.

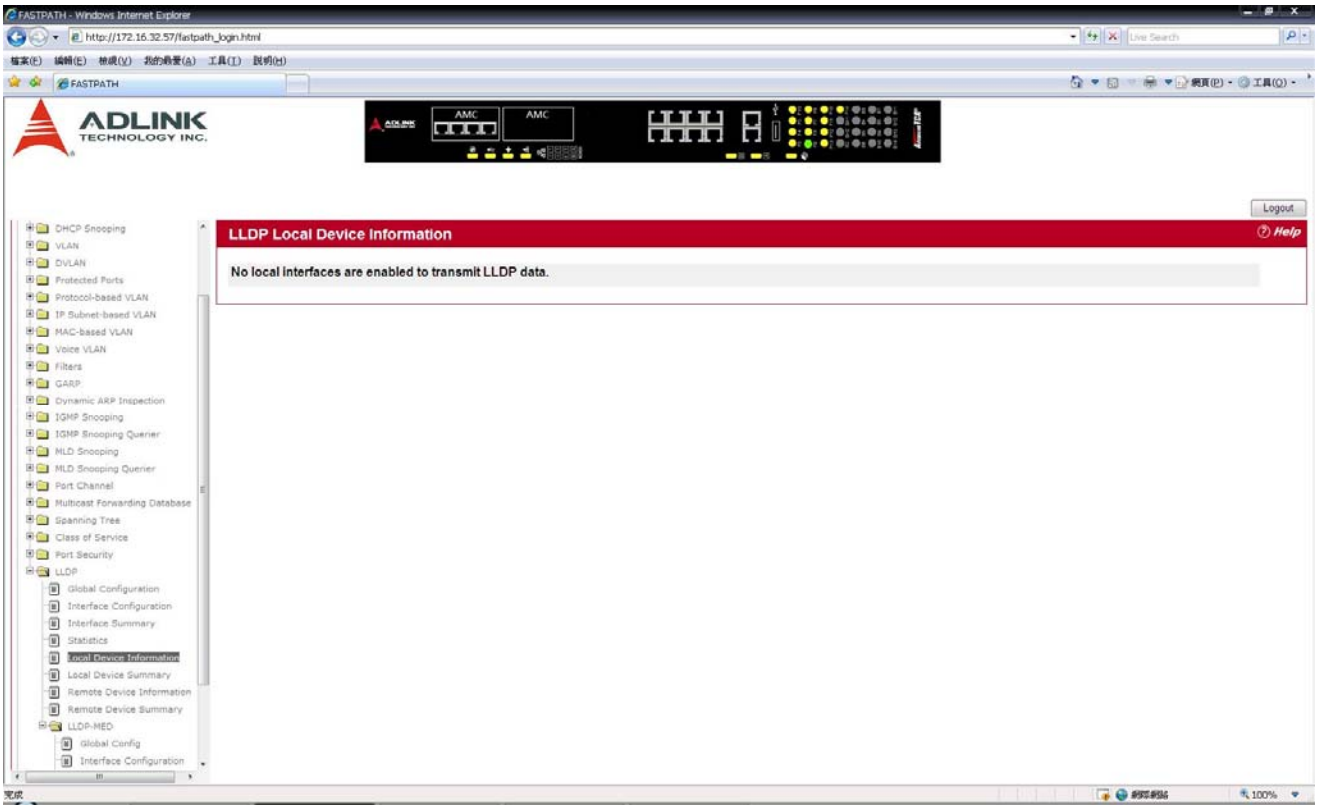
Field	Description
Port Statistics	
Interface	Displays the Interface for the interfaces.
Transmit Total	Displays the total number of LLDP frames transmitted by the LLDP agent on the corresponding port.
Receive Total	Displays the total number of valid LLDP frames received by the LLDP agent on the corresponding 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.
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 Switching > LLDP > Local Device Information in the navigation tree.



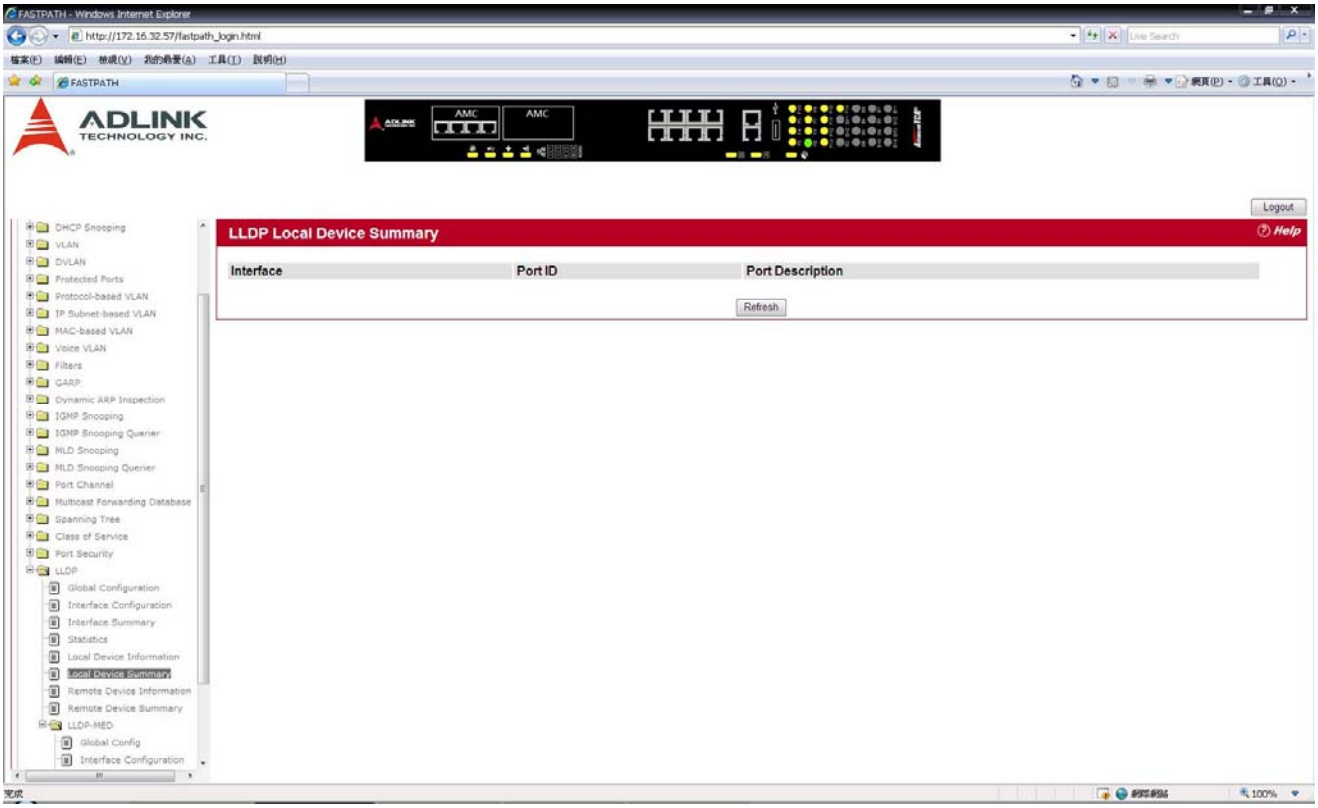
LLDP Local Device Information Fields

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 Switching > LLDP > Local Device Summary in the navigation tree.



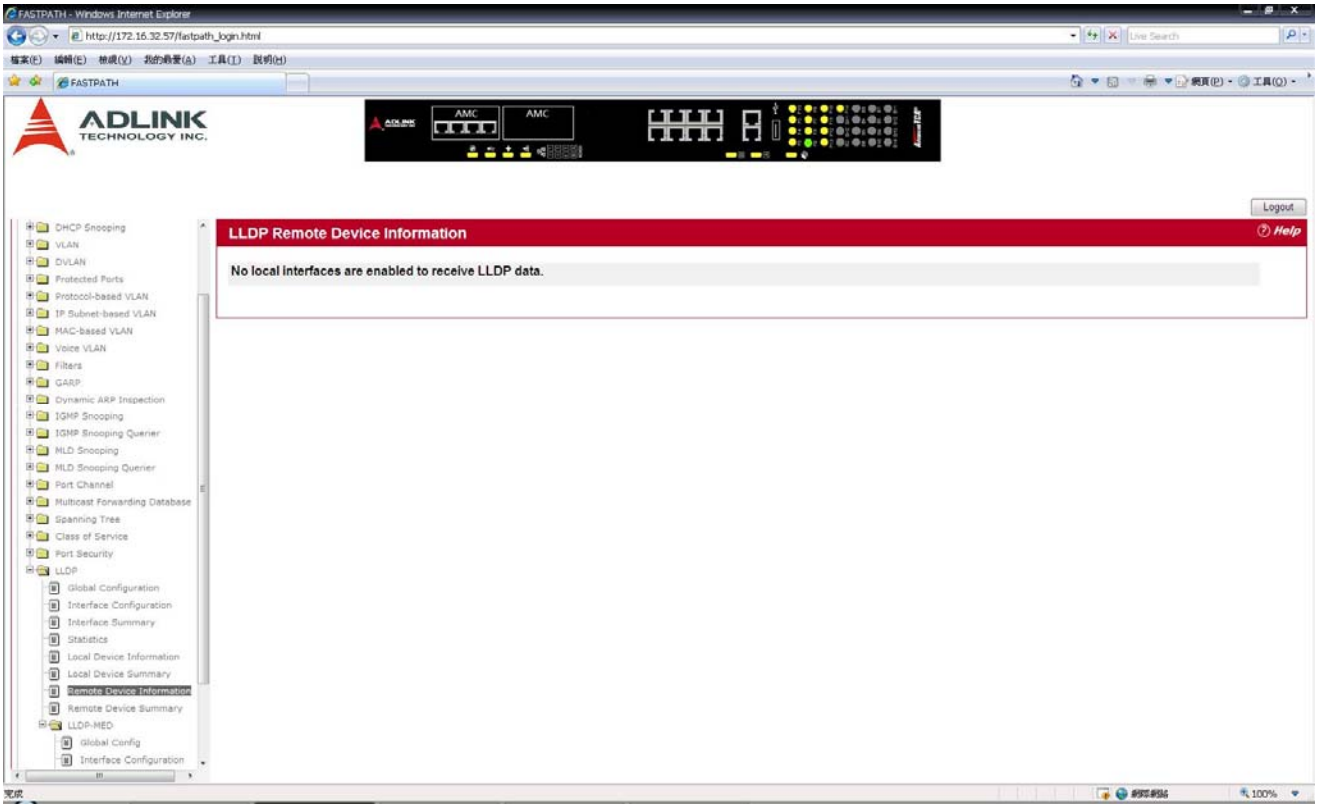
Field	Description
Interface	Displays the Interface on which LLDP-802.1AB frames can be transmitted.
Port ID	Displays the string describing the source of the port identifier.
Port Description	Displays the description of the port associated with the local system.

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 Switching > LLDP > Remote Device Information in the navigation tree.



LLDP Remote Device Information Fields

Field	Description
Local Interface	Select the Interface on the local system to display the LLDP information it has received. Note: If no LLDP data has been received on the select interface, 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.

Field	Description
System Description	Displays the description of the selected port associated with the remote system.
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 Switching > LLDP > Remote Device Summary in the navigation tree.



LLDP Remote Device Summary Columns

Field	Description
Local Interface	Shows the Interface 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.

5.22 LLDP-MED

The Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is an enhancement to LLDP that features:

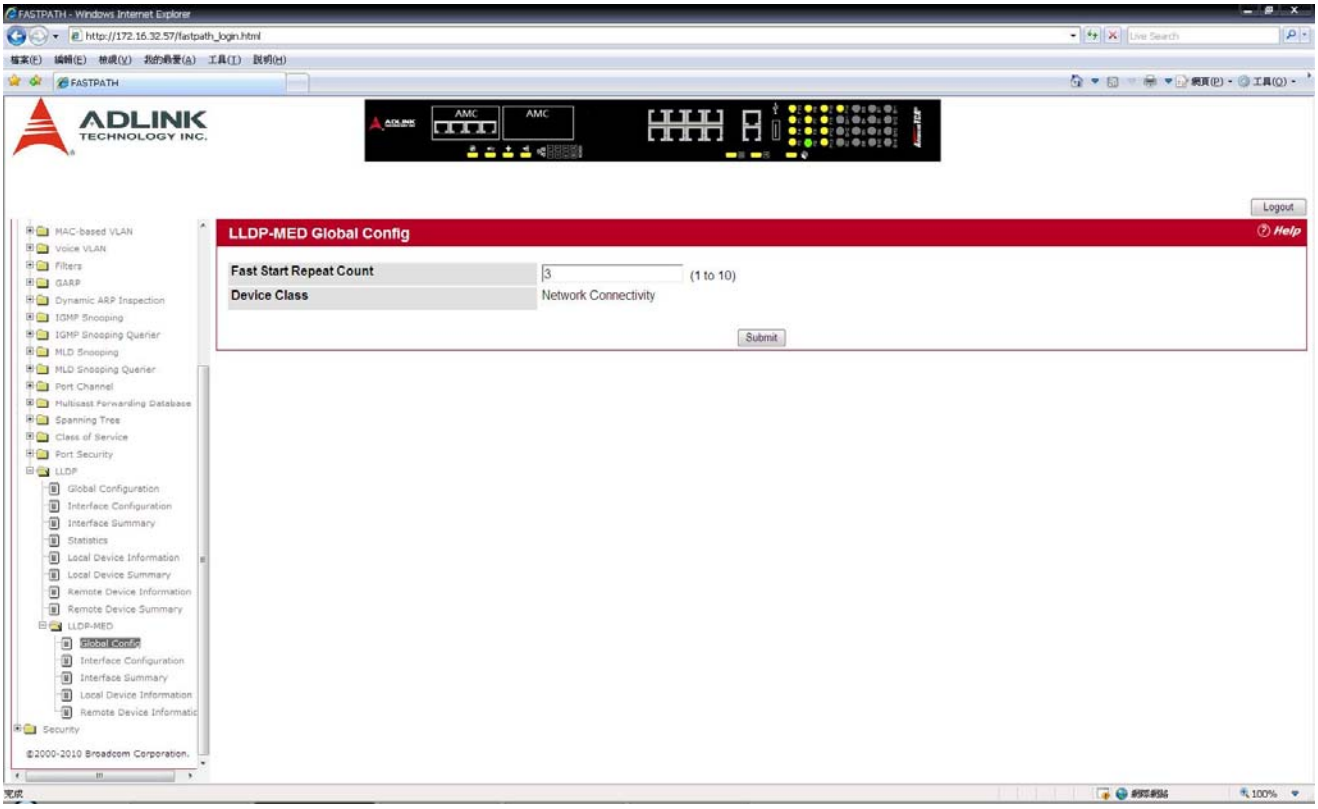
- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and DiffServ settings), enabling plug and play networking.
- Device location discovery for creation of location databases.
- Extended and automated power management of Power over Ethernet endpoints.
- Inventory management, enabling network administrators to track their network devices and determine their characteristics (manufacturer, software and hardware versions, serial/asset number).

The LLDP-MED folder provides access to the following pages:

- LLDP-MED Global Configuration
- LLDP-MED Interface Configuration
- LLDP-MED Interface Summary
- LLDP Local Device Information
- LLDP-MED Remote Device Information

LLDP-MED Global Configuration

Use this page to set global parameters for LLDP-MED operation. To display this page, click Switching > LLDP > LLDP- MED > Global Configuration in the navigation tree.

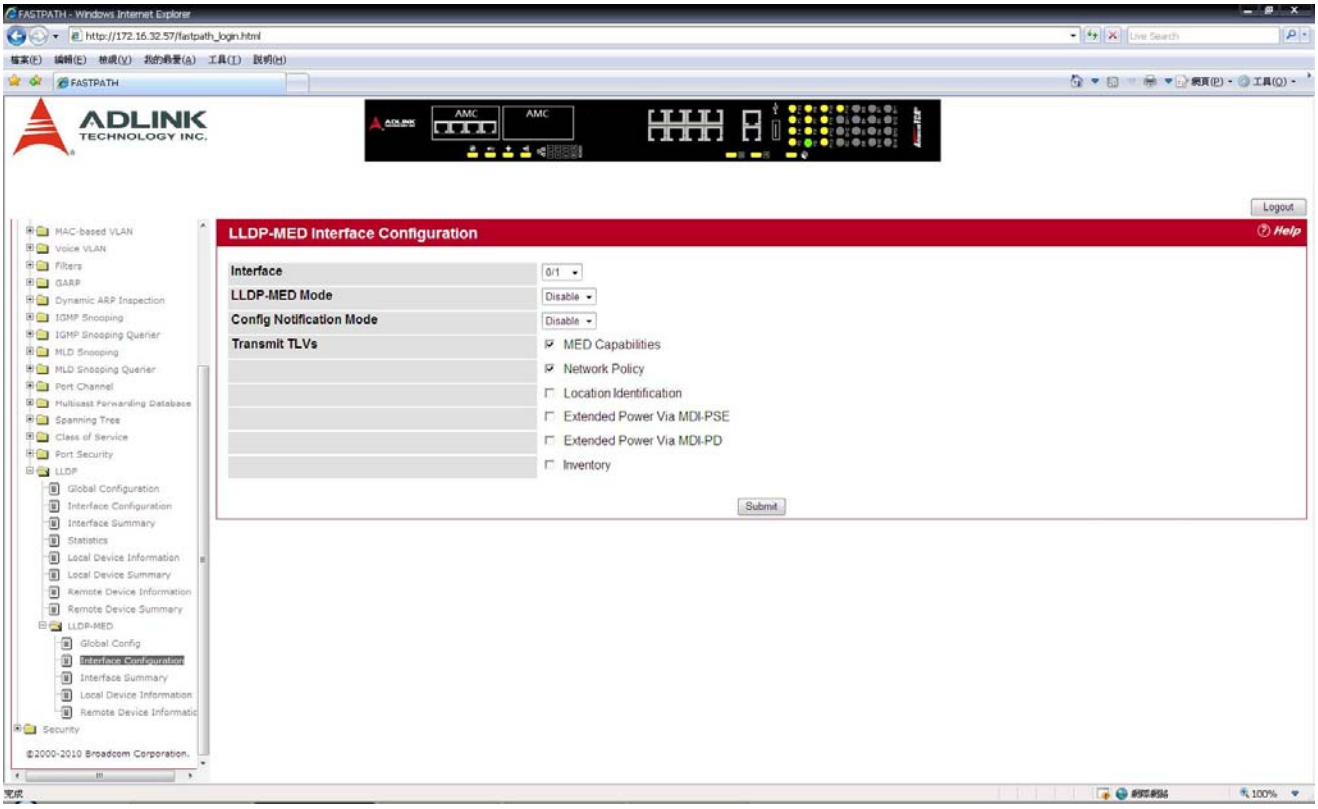


Field	Description
Fast Start Repeat Count	Specifies the number of LLDP PDUs that will be transmitted when the protocol is enabled. The range is from (1 to 10).The default value is 3.
Device Class	Specifies local device's MED Classification. The following three represent the actual endpoints: •Class I 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 updated 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 Switching > LLDP > LLDP-MED > Interface Configuration in the navigation tree.



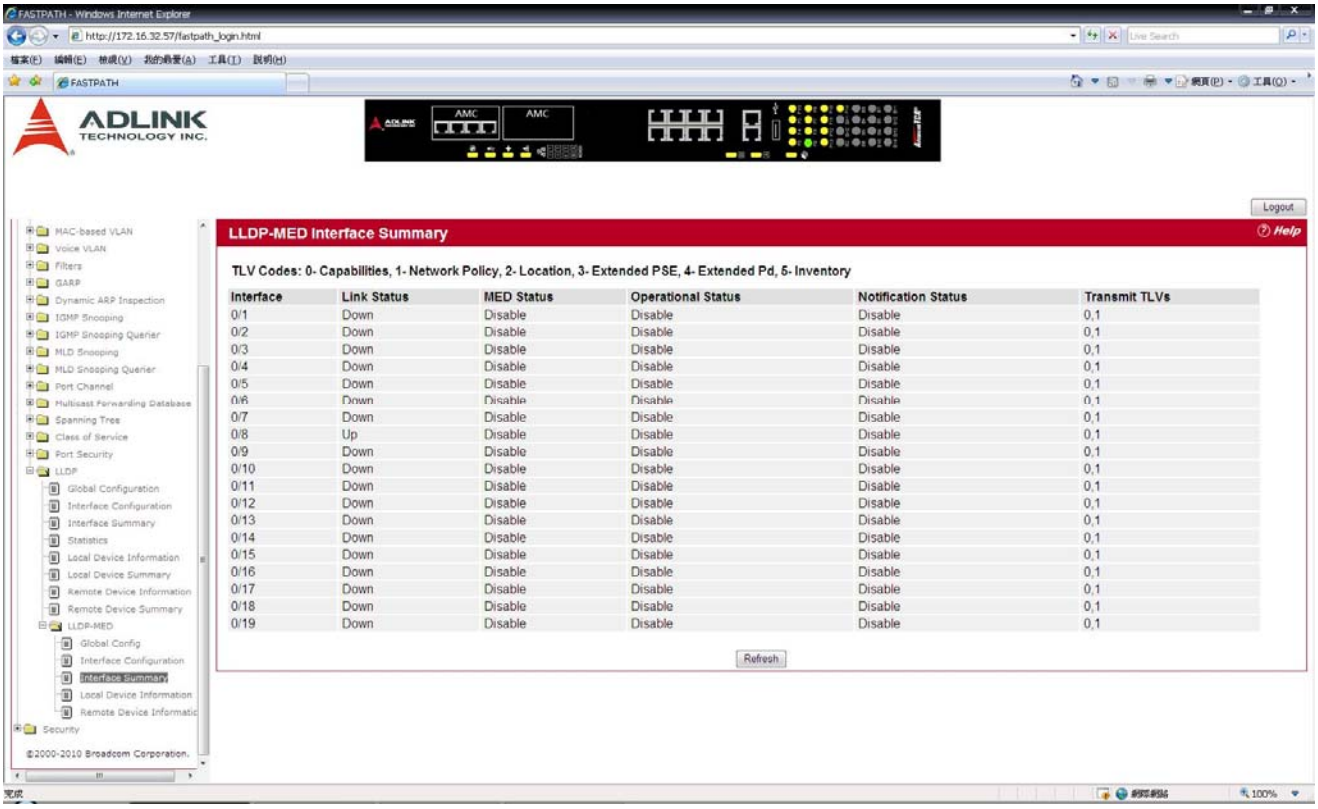
Field	Description
Interface	Selects the port that you want to configure LLDP-MED - 802.1AB on. You can select All to configure all interfaces on the DUT with the same properties. To view the summary of all interfaces, refer to the “LLDP-MED Interface Summary” . The Interface Configuration page will not 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 checkboxes 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: •MED Capabilities: Transmits the capabilities TLV in LLDP frames. •Network Policy: Transmits the network policy TLV in LLDP frames.

Field	Description
	•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 Switching > LLDP > LLDP-MED > Interface Summary in the navigation tree.

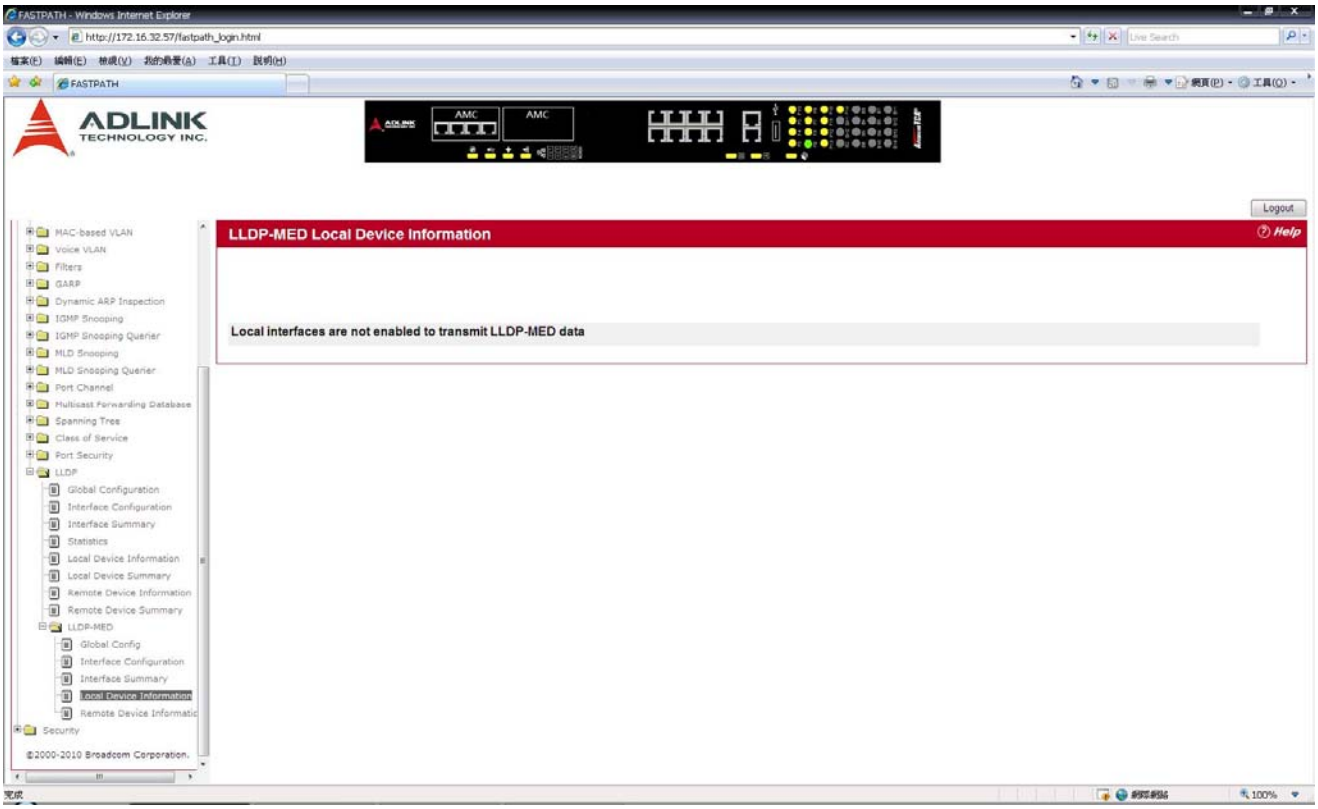


Field	Description
Interface	Specifies all the ports on which LLDP-MED can be configured.
Link Status	Specifies the link status of the ports as Up/Down.
MED Status	Specifies the transmit and/or receive LLDP-MED mode is enabled or disabled on this interface.
Operational Status	Specifies whether the interface 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 LLPD-MED information advertised on the selected local interface. To display this page, click Switching > LLDP > LLDP-MED > Local Device Information in the navigation tree.



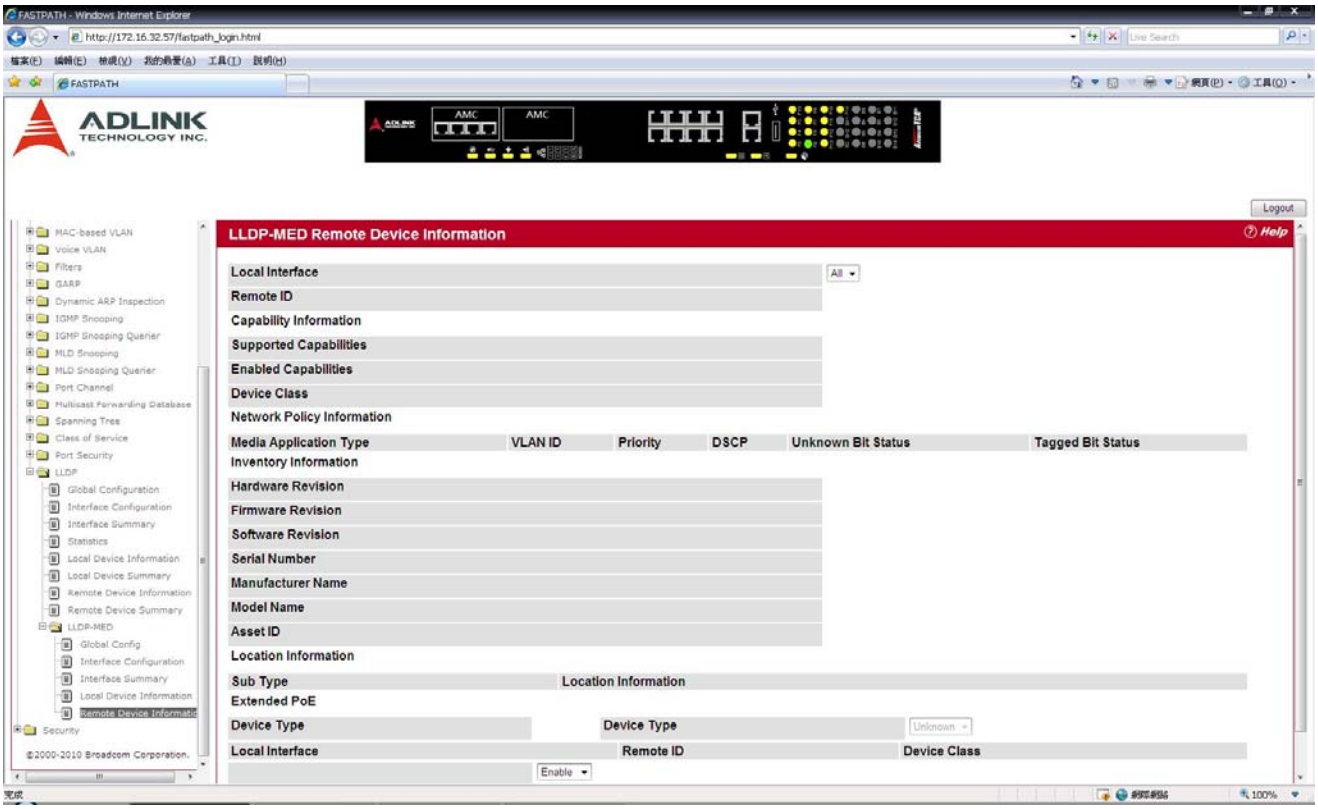
Field	Description
Interface	Select from the list of all the ports on which LLDP-MED frames can be transmitted.
Network Policy Information	Specifies if network policy TLV is present in the LLDP frames: • Media Application Type: Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, 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. This information is only displayed when a network policy TLV has been transmitted. • 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.

Field	Description
Inventory	Specifies the inventory TLV present in LLDP frames: • 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: • Sub Type: Specifies type of location information. • Location Information: Specifies the location information as a string for given type of location ID.
Extended PoE	Specifies if local device is a PoE device. • Device Type. Specifies power device type.
Extended PoE PSE	Specifies if extended PSE TLV is present in LLDP frame: • Available: Specifies available power sourcing equipment's power value in tenths of watts on the port of local device. • Source: Specifies power source of this port. • Priority: Specifies PSE port power priority.
Extended PoE PD	Specifies if extended PD TLV is present in LLDP frame. • Required: Specifies required power device power value in tenths of watts on the port of local device. • Source: Specifies power source of this port. • Priority: Specifies PD port power priority.

Click Refresh to update the page with the latest information from the router.

LLDP-MED Remote Device Information

This page displays information on LLPD-MED information received from remote clients on the selected local interface. To display this page, click Switching > LLDP > LLDP-MED > Remote Device Information in the navigation tree.



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: • 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.
Network Policy Information	Specifies if network policy TLV is received in the LLDP frames on this port: • Media Application Type: Specifies the application type. Types of application types are unknown, voicesignaling, guestvoice, guestvoicesignalling, softphonevoice, videoconferencing, streammingvideo, 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. This information is displayed only when a network policy TLV

Field	Description
	has been received on this port. • 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	Specifies the inventory TLV is received in LLDP frames on this port: • 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	Specifies if location TLV is received in LLDP frames on this port. • Sub Type: Specifies type of location information. • Location Information: Specifies the location information as a string for given type of location ID.
Extended PoE	Specifies if remote device is a PoE device. • Device Type. Specifies the remote device's PoE device type connected to this port.
Extended PoE PSE	Specifies if extended PSE TLV is received in LLDP frame on this port: • 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	Specifies if extended PD TLV is received in LLDP frame on this port. • 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.

5.23 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:

- Port Access Control
- Captive Portal Configuration
- RADIUS Settings
- TACACS+ Settings
- Secure HTTP
- Secure Shell

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.

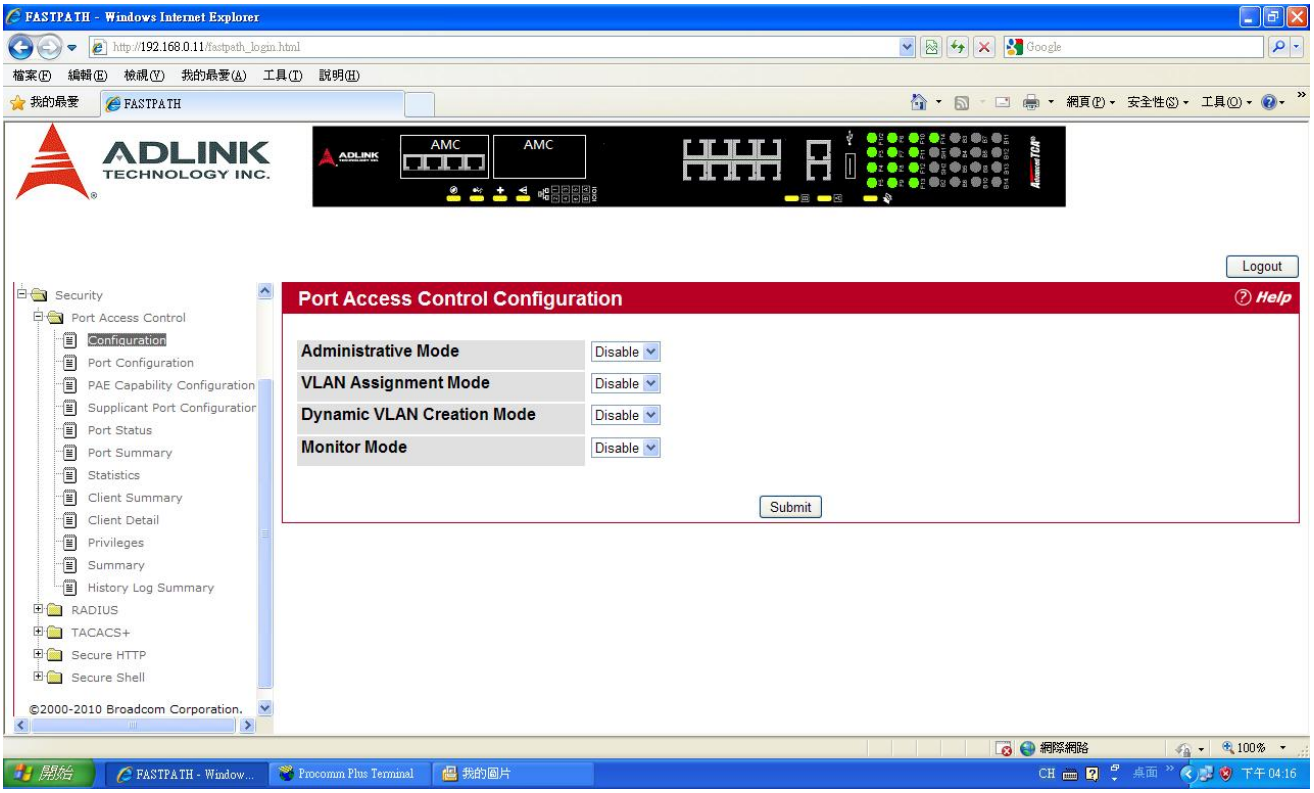
The Port Access Control folder contains links to the following pages that allow you to view and configure the 802.1x features on the system:

- Global Port Access Control Configuration
- Port Configuration
- Port Status
- Port Summary
- Port Access Control Statistics
- Client Summary
- Client Detail
- Port Access Privileges
- Port Access Summary

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 Port Based Access Control > Configuration in the navigation menu.



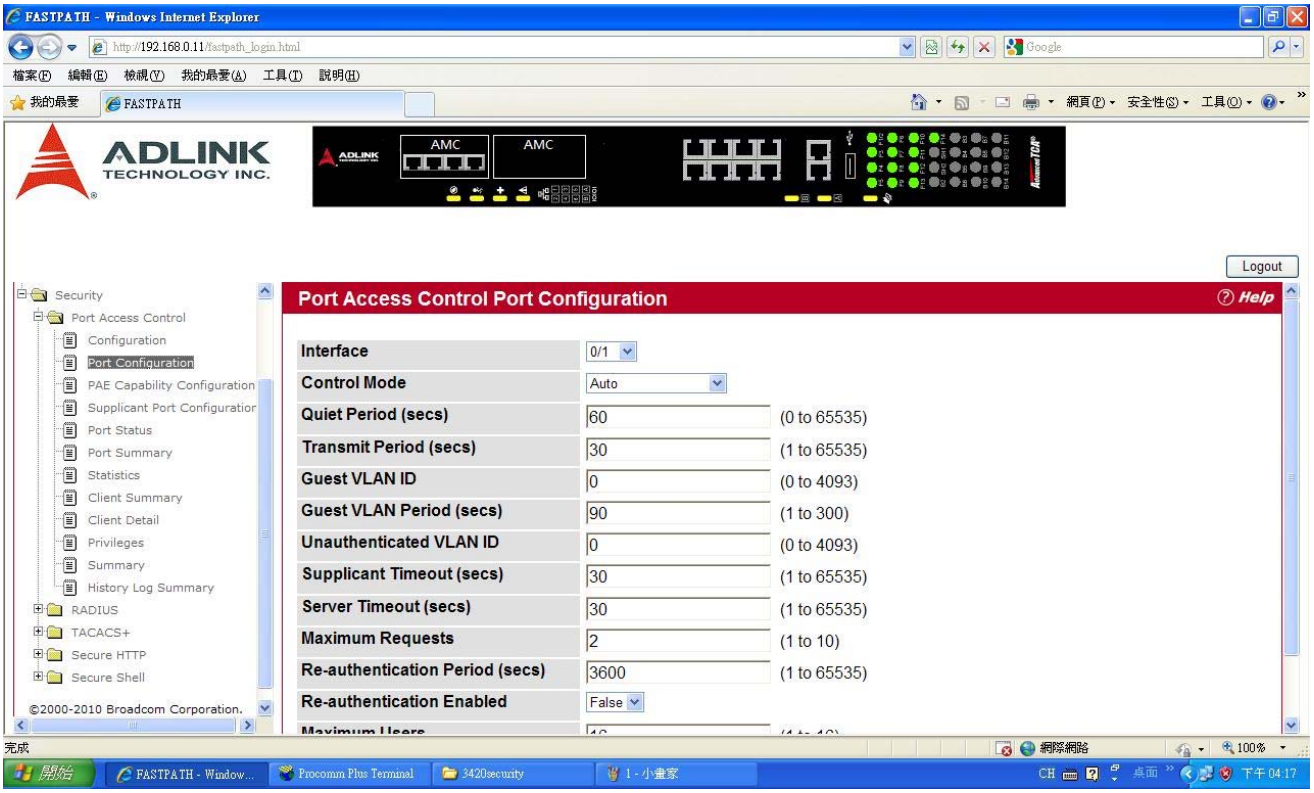
Field	Description
Administrative Mode	Select Enable or Disable 802.1x mode on the switch. The default is Disable. This feature permits port-based authentication on the switch. If enabled, when a supplicant is authenticated by a authentication server, the port that the supplicant is connected to is placed in a particular VLAN specified by the RADIUS server.
VLAN Assignment Mode	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.

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 Security > Port Based Access Control > Port Configuration in the navigation menu.



Field	Description
Interface	Selects the Unit and Port to configure.
Control Mode	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: • 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.
Quiet Period (secs)	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.

Field	Description
Transmit Period (secs)	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.
Guest VLAN ID	Defines the Guest VLAN ID on the interface. The valid range is 0 to 3965. The default value is 0. Changing the value will not change the configuration until you click the Submit button. Enter zero (0) to clear the Guest VLAN ID on the interface.
Guest VLAN Period (secs)	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. Changing the value will not change the configuration until you click the Submit button.
Unauthenticated VLAN ID	Defines the Unauthenticated VLAN ID for the selected port. The valid range is 0 to 3965. The default value is zero (0). Changing the value will not change the configuration until you click the Submit button. Enter zero (0) to clear the Unauthenticated VLAN ID on the interface.
Supplicant Timeout (secs)	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. Changing the value will not change the configuration until you click the Submit button.
Server Timeout (secs)	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. Changing the value will not change the configuration until you click the Submit button.
Maximum Requests	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.
Reauthentication Period (secs)	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. Changing the value will not change the configuration until you click the Submit button.
Reauthentication Enabled	Reauthenticates the selected port periodically, when enabled. The default value is False. Changing the value will not change the configuration until you click the Submit button.
Maximum Users	Defines the maximum number of clients that can get authenticated

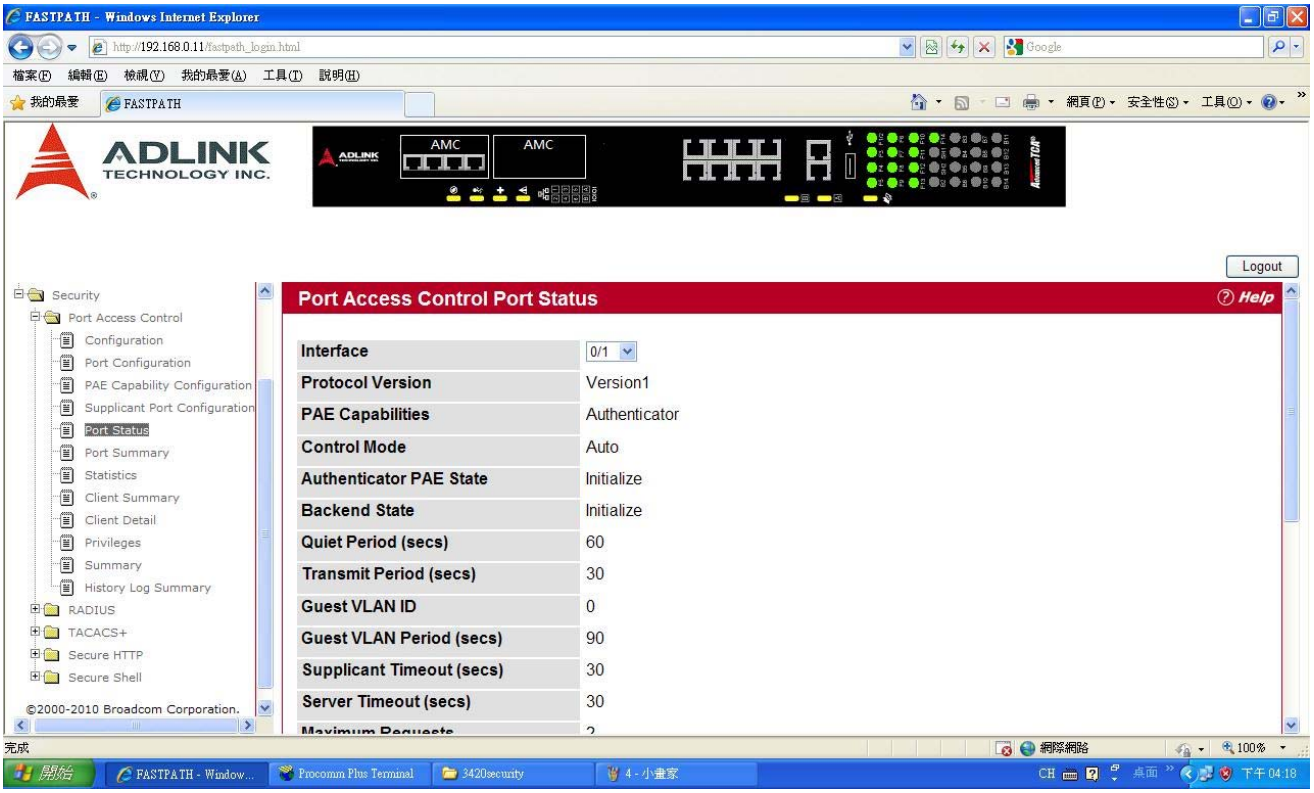
Field	Description
	on the port in the MAC-based dot1x authentication mode. The range is 1 to 16. The default value is 16. Changing the value will not change the configuration until you click the Submit button.

- 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 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 Based Access Control Port Status page, click Security > Port Based Access Control > Port Status in the navigation menu.



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	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: • 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.

Field	Description
	• MAC-based: Sets the mode of the interface to authentication on a per supplicant basis.
Authenticator PAE State	This field displays the current state of the authenticator PAE state machine. Possible values are as follows: •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: •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

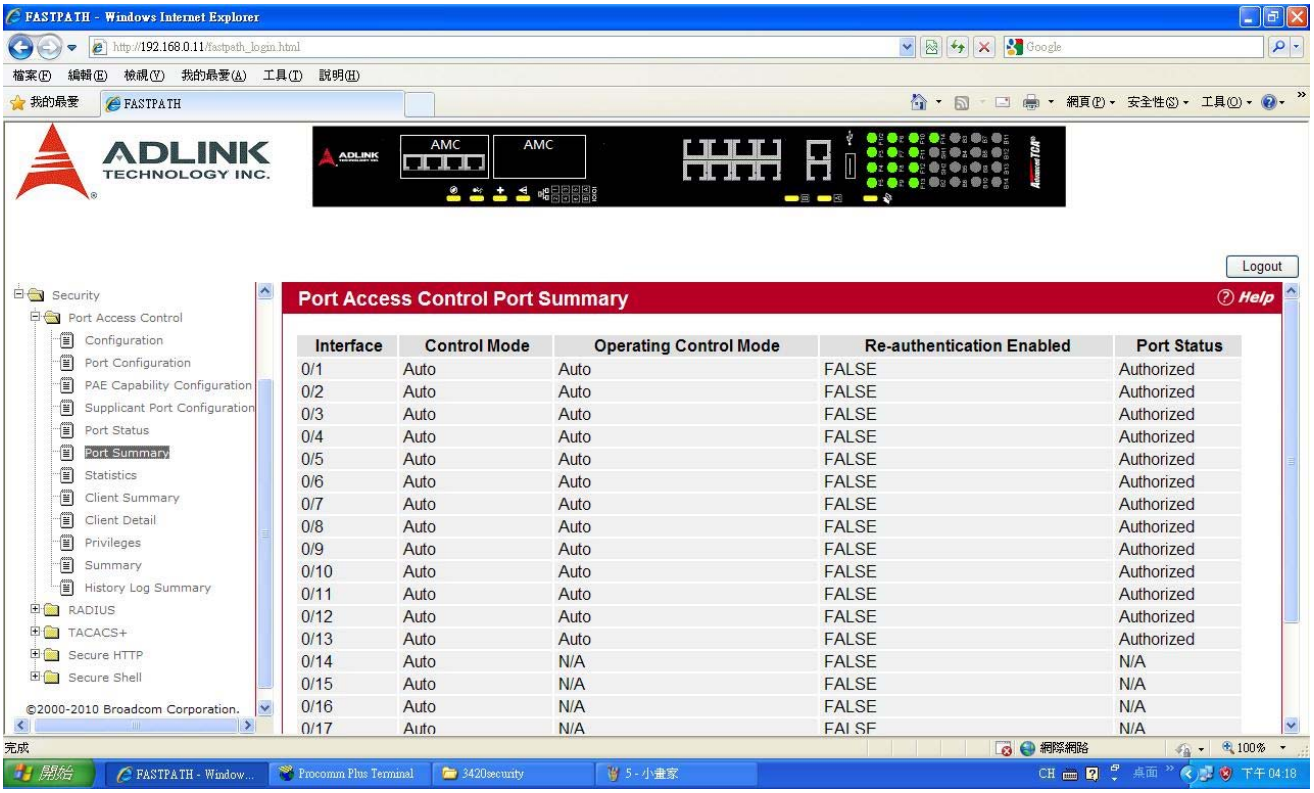
Field	Description
	VLAN Authentication. The value is in the range of 1 to 300.
Supplicant Timeout	Displays the configured supplicant timeout for the selected port. The supplicant timeout is the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. 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.
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: •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

Field	Description
	'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.
Session Termination Action	Displays the Termination Action set by the RADIUS Server for the selected port. Possible values are: •Default •Reauthenticate If the termination action is Default then, at the end of the session, the client details are initialized. Otherwise, re-authentication is attempted. Note: This field is displayed only when the port control mode of the selected port is not MAC-based.
Logical Port	Displays the logical port number associated with the supplicant that is connected to the port. This field is not configurable. Note: This field is displayed when the port control mode of the selected port is MAC- based.
Supplicant MacAddress	This field displays the supplicant’s MAC address that is connected to the port. This field is not configurable. Note: This field is displayed when the port control mode of the selected port is MAC- based.

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.



Field	Description
Interface	Selects the Unit and Port to view.
Control Mode	Displays the port authorization state. The possible field values are: • 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: •ForceUnauthorized •ForceAuthorized

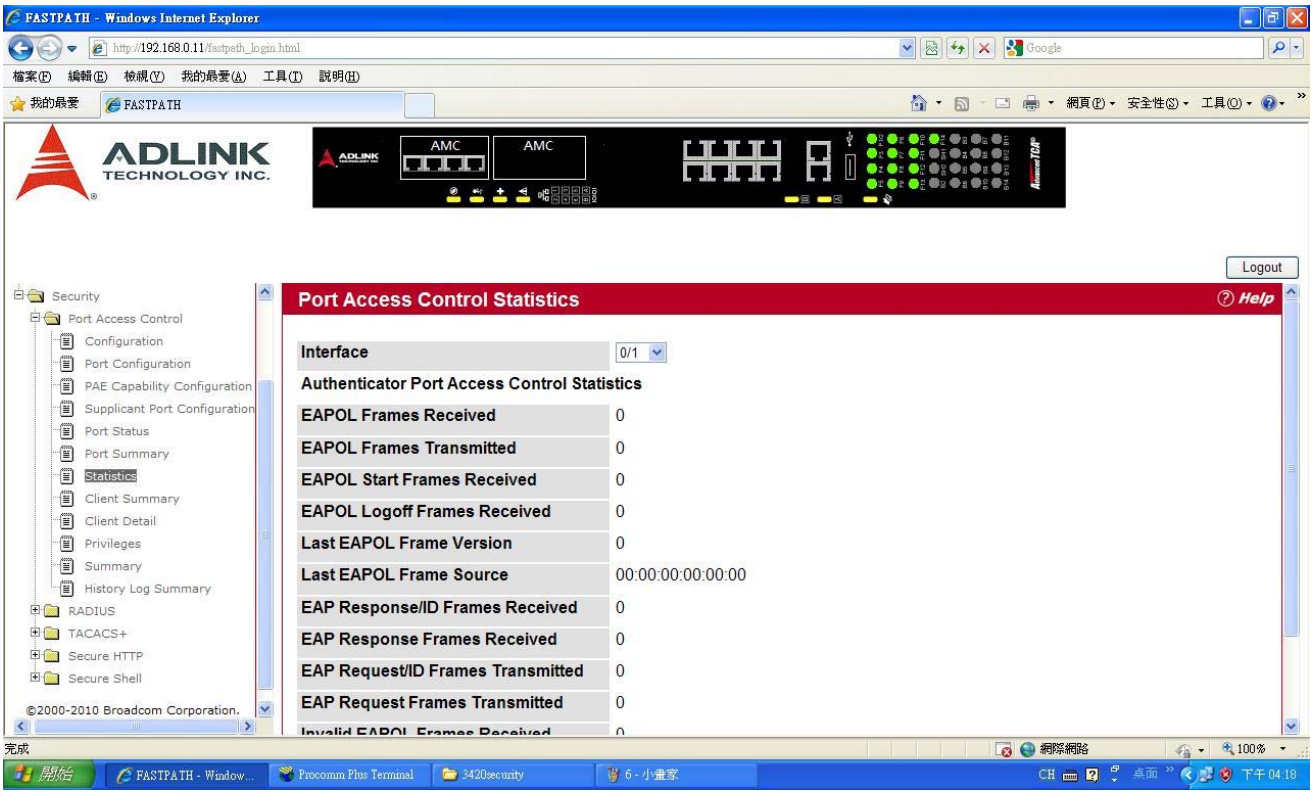
Field	Description
	•Auto •MAC-based •N/A: If the port is in detached state it cannot participate in port access control.
Reauthentication Enabled	Displays whether reauthentication is enabled on the port. This is a configurable field. The possible values are as follows: • True: Reauthentication will occur. • 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.



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	Displays the number of valid EAP Respond frames received on the

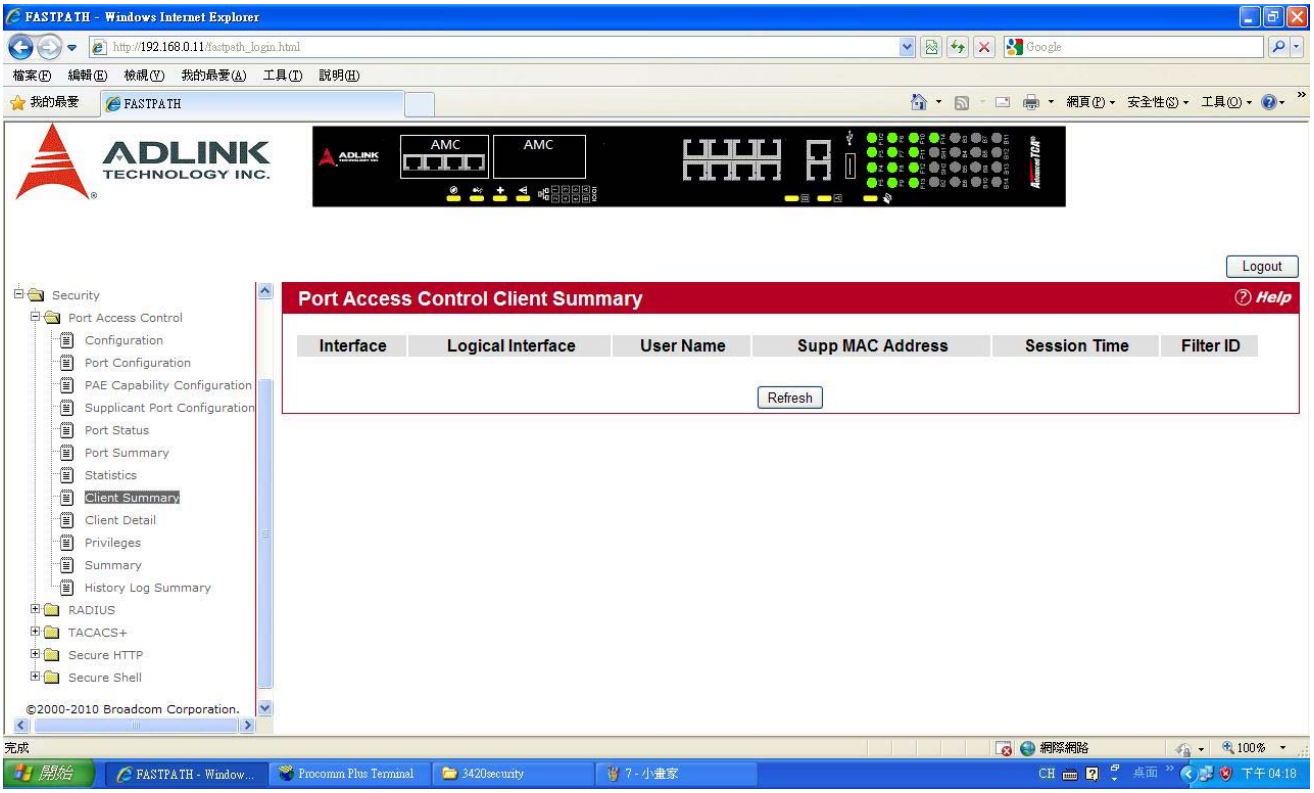
Field	Description
Received	port.
EAP Request/ID Frames Transmitted	Displays the number of EAP Requested ID frames transmitted via the port.
EAP Request Frames Transmitted	Displays the number of EAP Request frames transmitted via the port.
Invalid EAPOL Frames Received	Displays the number of unrecognized 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.



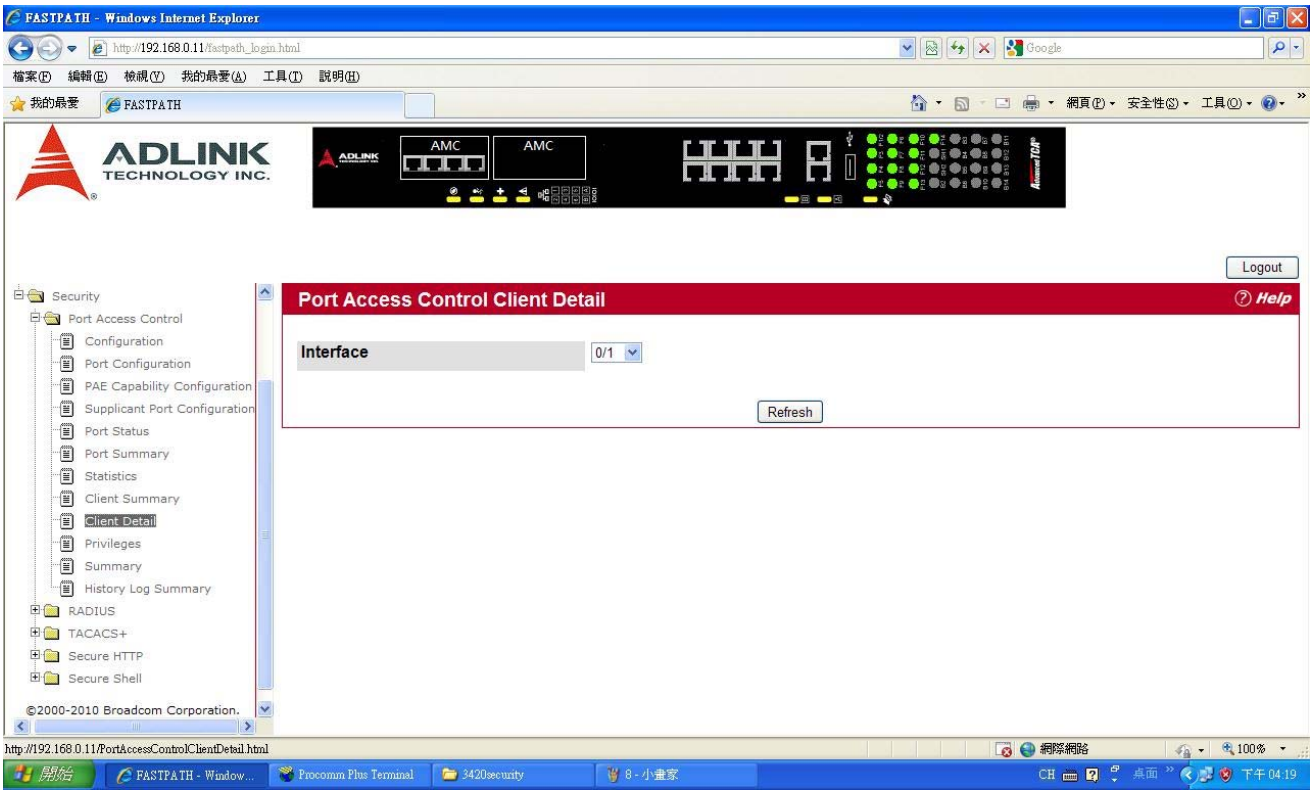
Field	Description
Interface	Displays the interface address of the supplicant device.
User Name	Displays the user name representing the supplicant device.
Supp Mac Address	Displays the supplicant device's MAC address.
Session Time	Displays the time since the supplicant logged in. The value is in seconds.
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.

Client Detail

Use the Port Access Control Client Detail page to view detail information about the supplicant device.

To access the Port Access Control Client Detail page, click Security > Port Access Control > Client Detail in the navigation menu.



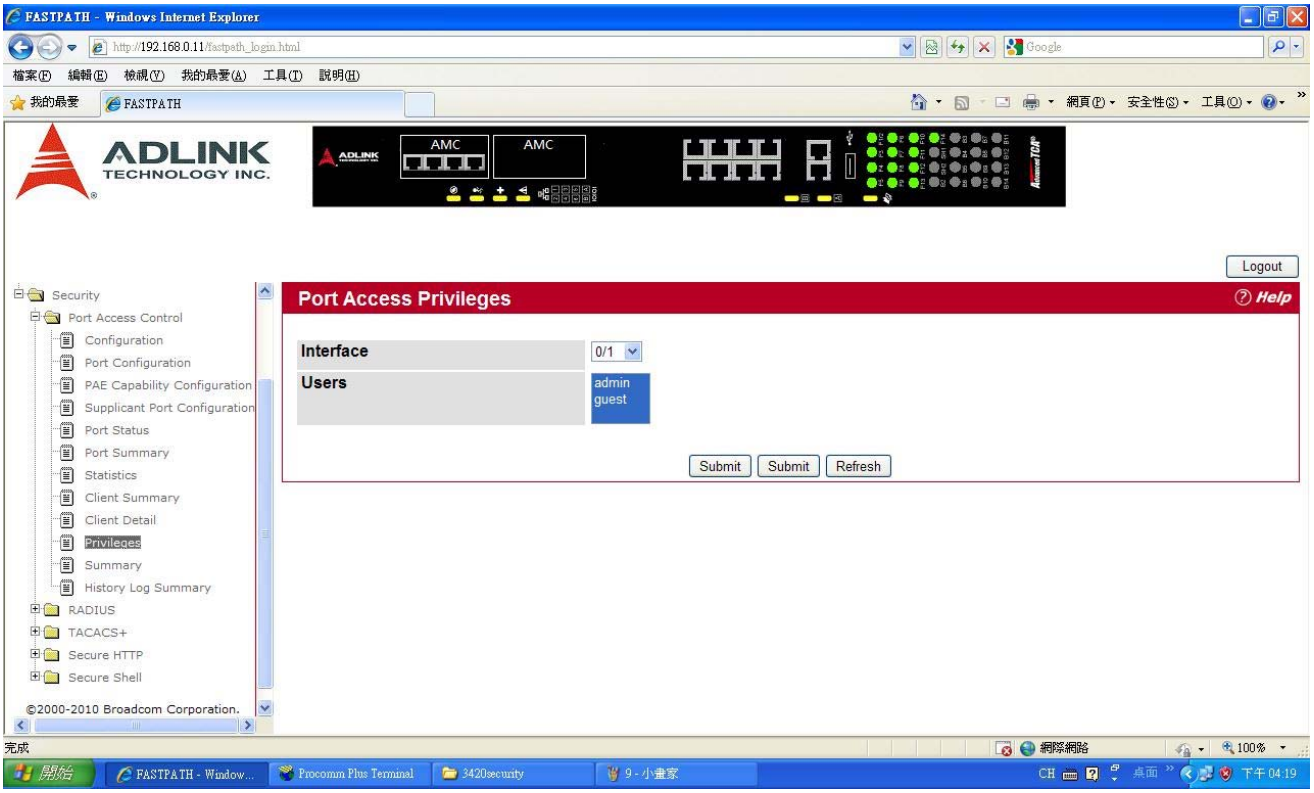
Field	Description
Interface	Displays the interface address of the supplicant device.
User Name	Displays the user name representing the supplicant device.
Supp Mac Address	Displays the supplicant device's MAC address.
Session Time	Displays the time since the supplicant logged in. The value is in seconds.
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.
VLAN Assigned	Displays the reason for the VLAN ID assigned by the authenticator to the supplicant device.
Session Timeout	Displays the session timeout set by the radius server to the supplicant device.
Termination Action	Displays the termination action set by the radius server 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 Security > Port Based Access Control > Privileges in the navigation menu.

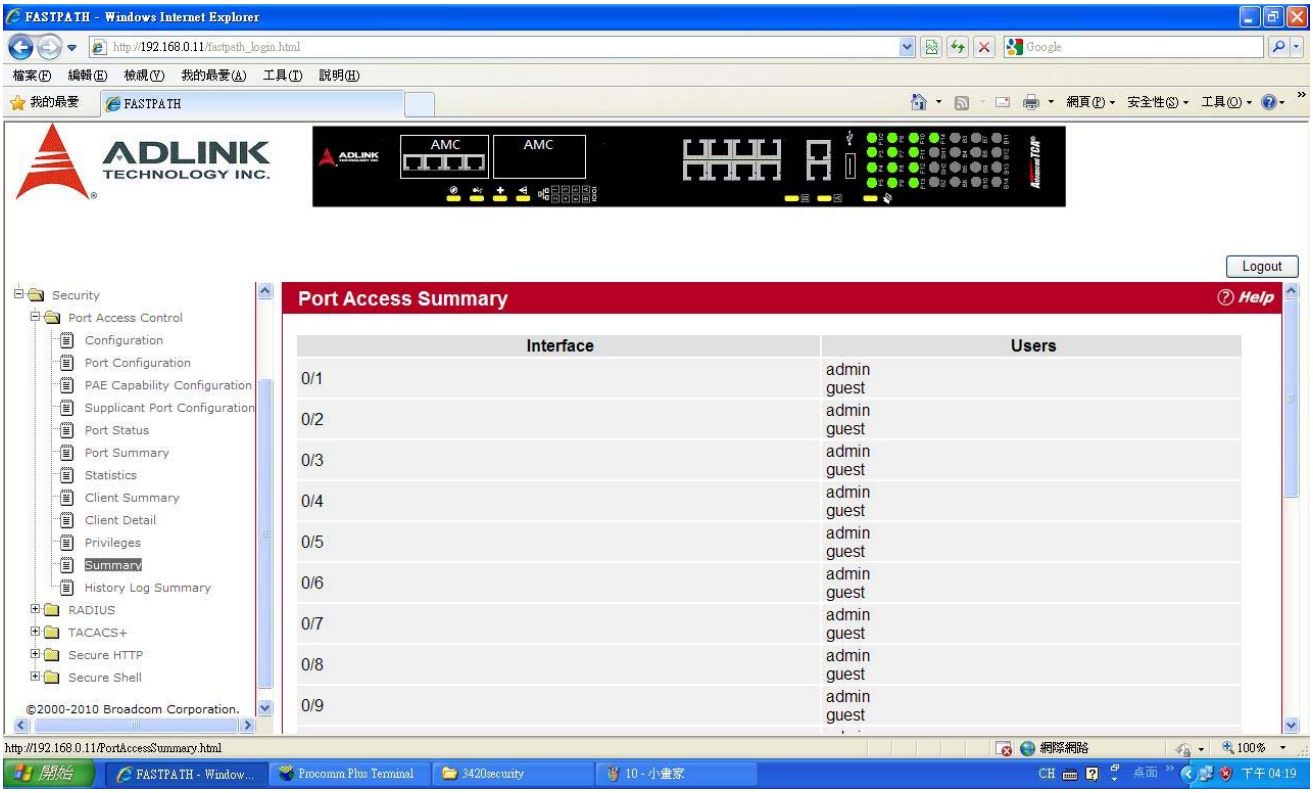


Field	Description
Interface	Selects the port to grant or deny access. To grant or deny port access privileges to a user on all ports, select All from the drop-down menu.
Users	Lists the users configured on the system. The users that are highlighted have access to the selected port. By default, all users 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.

Port Access Summary

Use the Port Access Control Summary page to view a summary of which users are allowed access to the physical ports on the system.

To access the Port Based Access Control Summary page, click Security > Port Based Access Control > Summary in the navigation menu.



Field	Description
Interface	Lists the physical ports on the system.
Users	Lists the users that are allowed 802.1x access to the port. If a username is configured on the system and does not appear in the Users column for a port, the user is denied access to the port.

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

5.24 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 to Switch Access
- Access Control Port (802.1x)

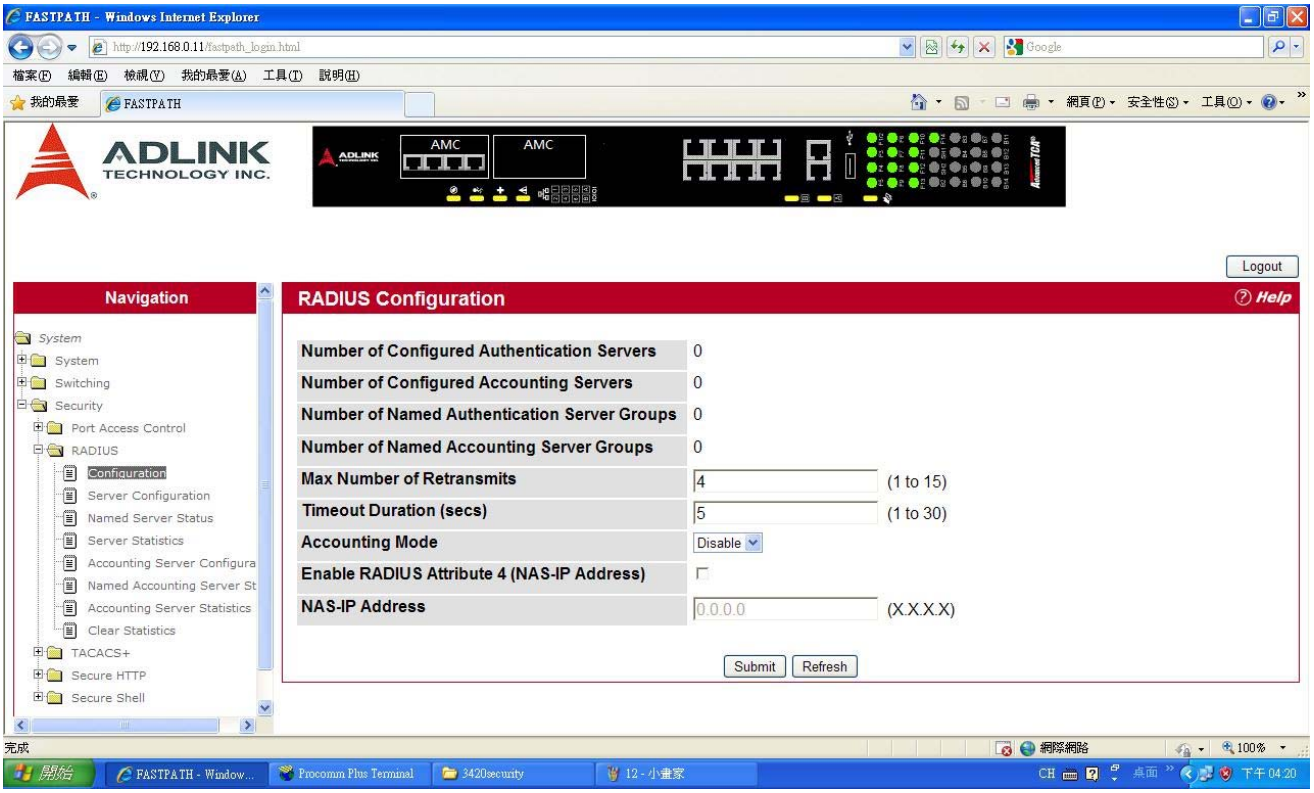
The RADIUS folder contains links to the following pages that help you view and configure system RADIUS settings:

- RADIUS Configuration
- Server Configuration
- Server Statistics
- Accounting Server Configuration
- Accounting Server Statistics
- Clear Statistics

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 Security > RADIUS > Configuration in the navigation menu.



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.
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.
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.

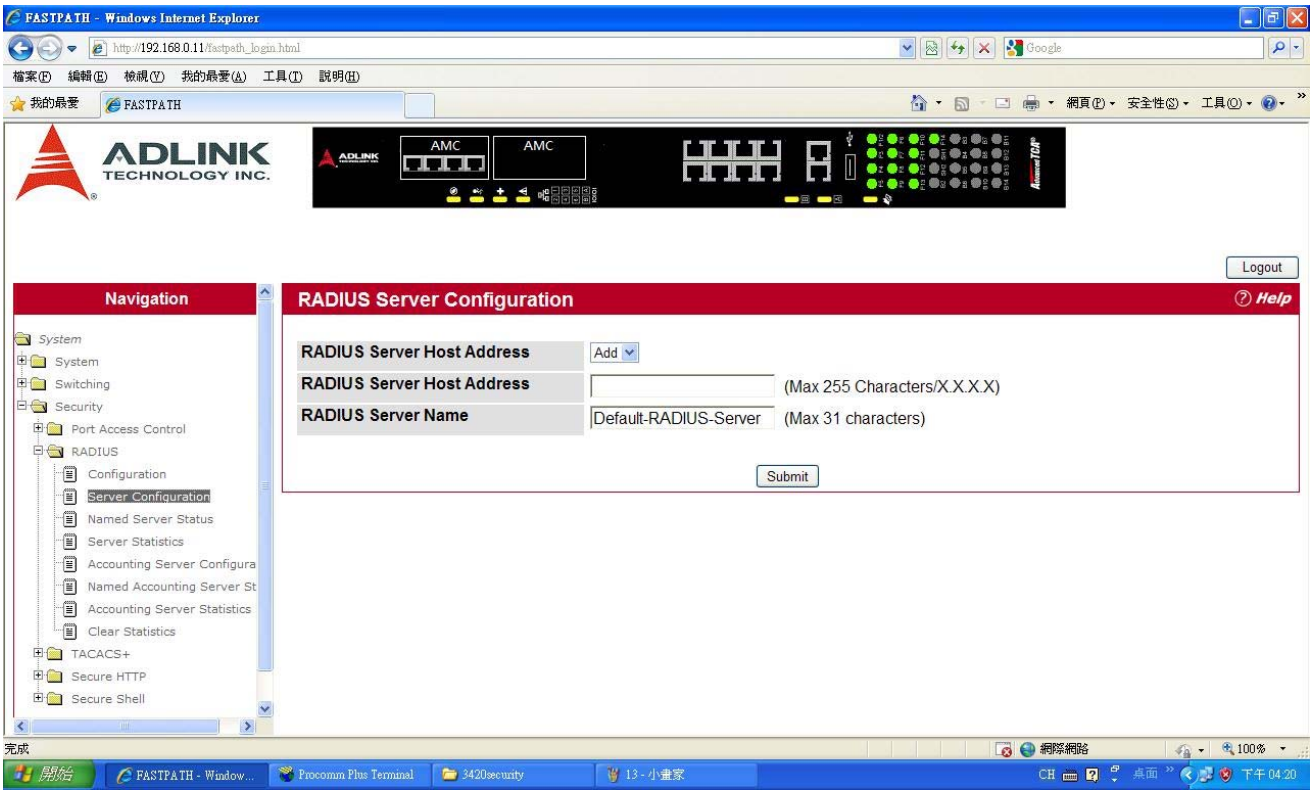
Use the buttons at the bottom of the page to perform the following actions:

- 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.

Server Configuration

From the 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 Security > RADIUS > 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, the fields described in the following table are available.



Field	Description
RADIUS Server Host Address	To configure a new RADIUS server, select the Add option from the menu. To view or configure a RADIUS server that is already configured on the system, select its IP address from the menu.
Host Address	Enter the IP address of the RADIUS server to add. This field is only available when Add is selected in the RADIUS Server Host Address field.
RADIUS Server Name	Enter the name of the RADIUS 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 Authentication servers. RADIUS clients can use RADIUS servers with the same name as backups for each other.

After you enter the RADIUS server information, click Submit to apply the changes to the system. The page refreshes, and additional RADIUS server configuration fields appear.

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. After you add a RADIUS server, use the Server Configuration page to configure the server settings.

If you select Add from the RADIUS Server Host Address field, the page refreshes and several of the configuration options are hidden.

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 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. If the primary server is not

Field	Description
	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. 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:

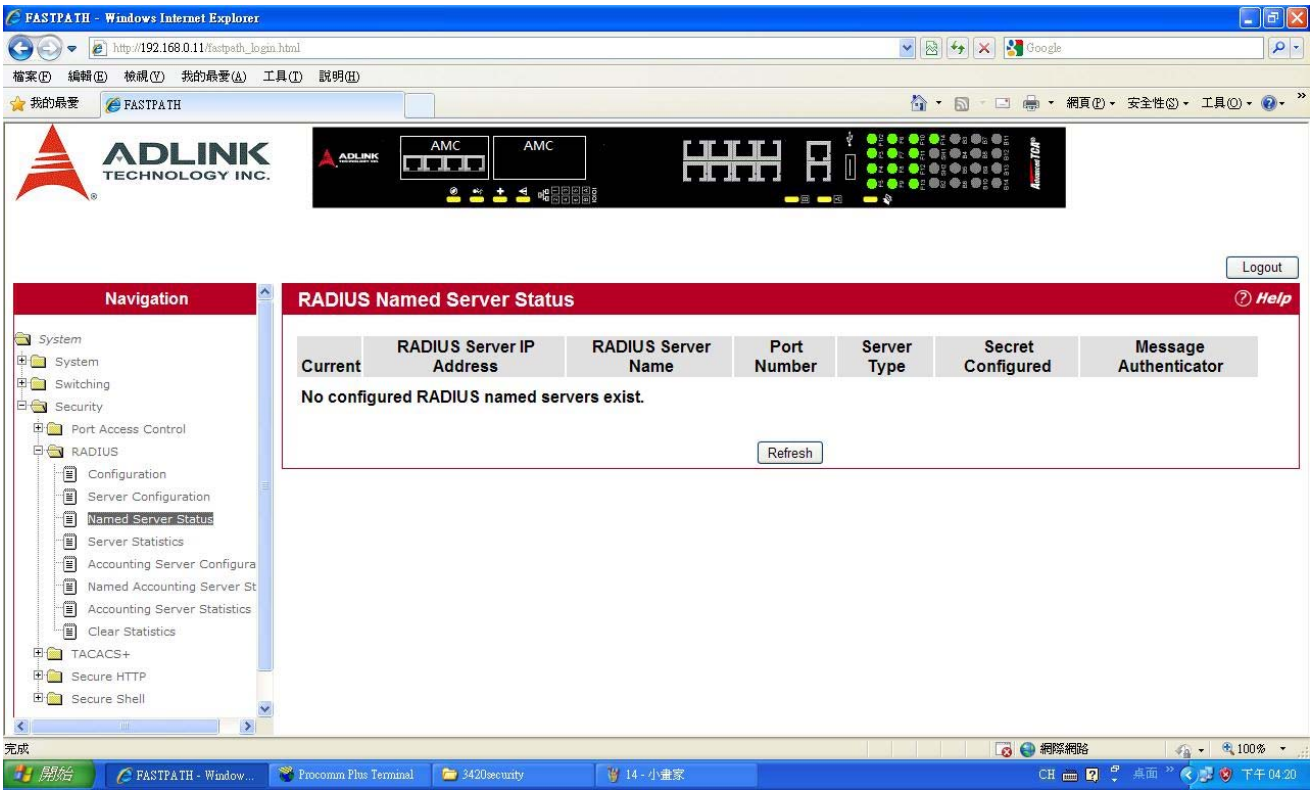
- If you make changes to the page, click Submit to apply the changes to the system.

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.

Named Server Status Information

The RADIUS Named Server Status page shows summary information about the RADIUS servers configured on the system.



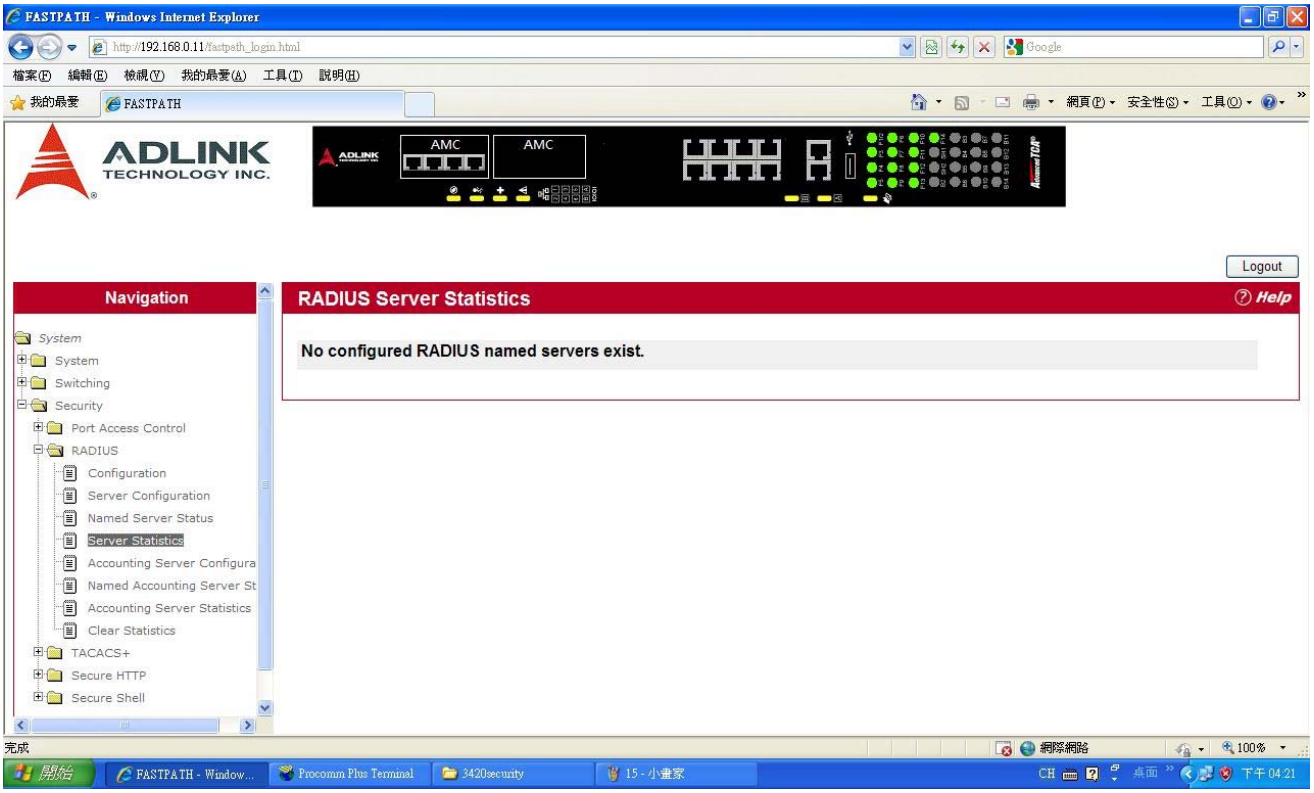
Field	Description
Current	An asterisk (*) in the column Indicates that the server is the current server for the authentication server group. If no asterisk is present, the server is a backup server. If more than one RADIUS server is configured with the same name, the switch selects one of the servers 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.

Server Statistics

Use the RADIUS Server Statistics page to view statistical information for each RADIUS server configured on the system.

To access the RADIUS Server Statistics page, click Security > RADIUS > Server Statistics in the navigation menu.



Field	Description
RADIUS Server Host Address	Use the drop-down menu to select the IP address of the RADIUS server for which to display statistics.
Round Trip Time (secs)	The time interval, in hundredths of a second, between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from this RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.

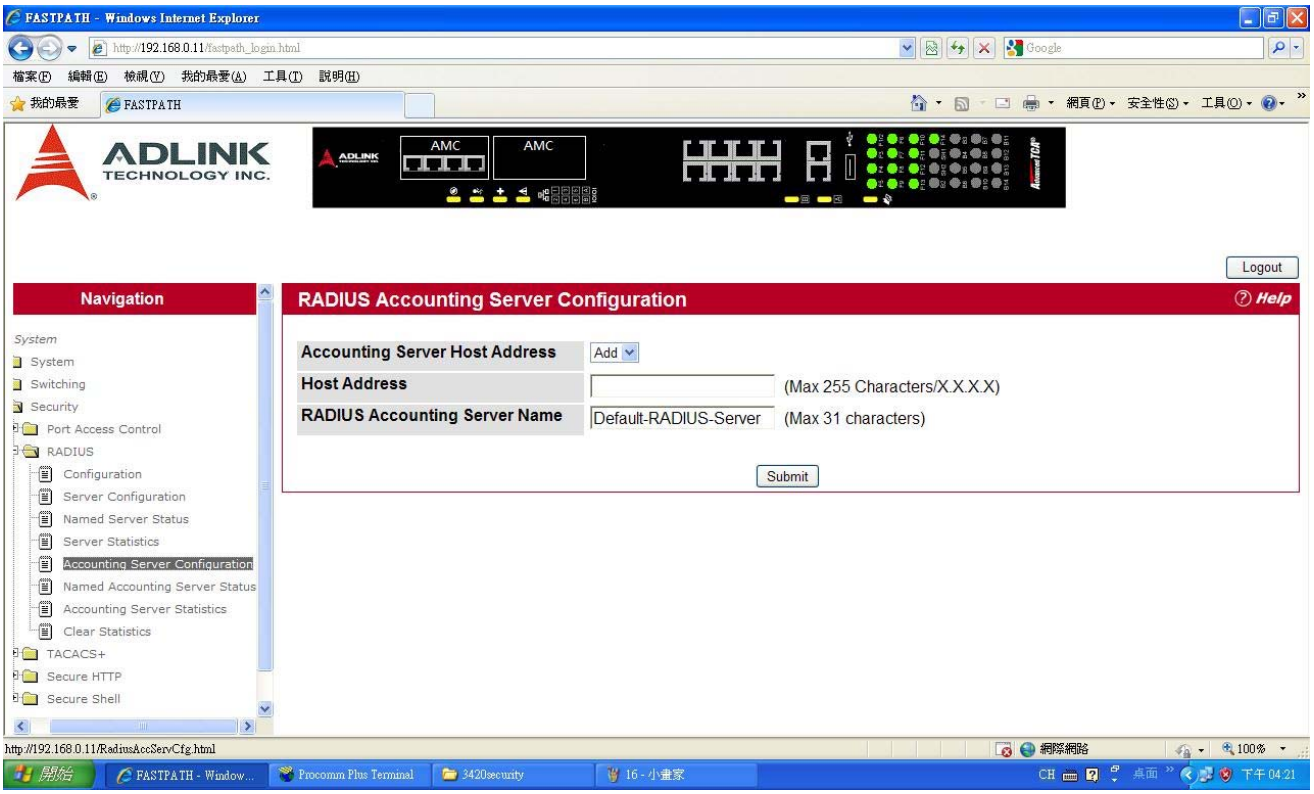
Field	Description
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access- responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

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

Accounting Server Configuration

From the 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, the fields described in the following table are available.



Field	Description
Accounting Server Host Address	To configure a new RADIUS accounting server, select the Add option from the menu. To view or configure an accounting server that is already configured on the system, select its IP address from the menu.
Host Address	Enter the IP address of the RADIUS accounting server to add. This field is only available when Add is selected in the Accounting Server Host Address field.
RADIUS Accounting Server Name	Enter a name for 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.

After you enter the RADIUS accounting server information, click Submit to apply the changes to the system. The page refreshes, and additional accounting server 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. After you add an accounting server, use the Accounting Server Configuration page to configure the server settings.

If you select Add from the Accounting Server Host Address field, the page refreshes and several of the configuration options are hidden.

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:

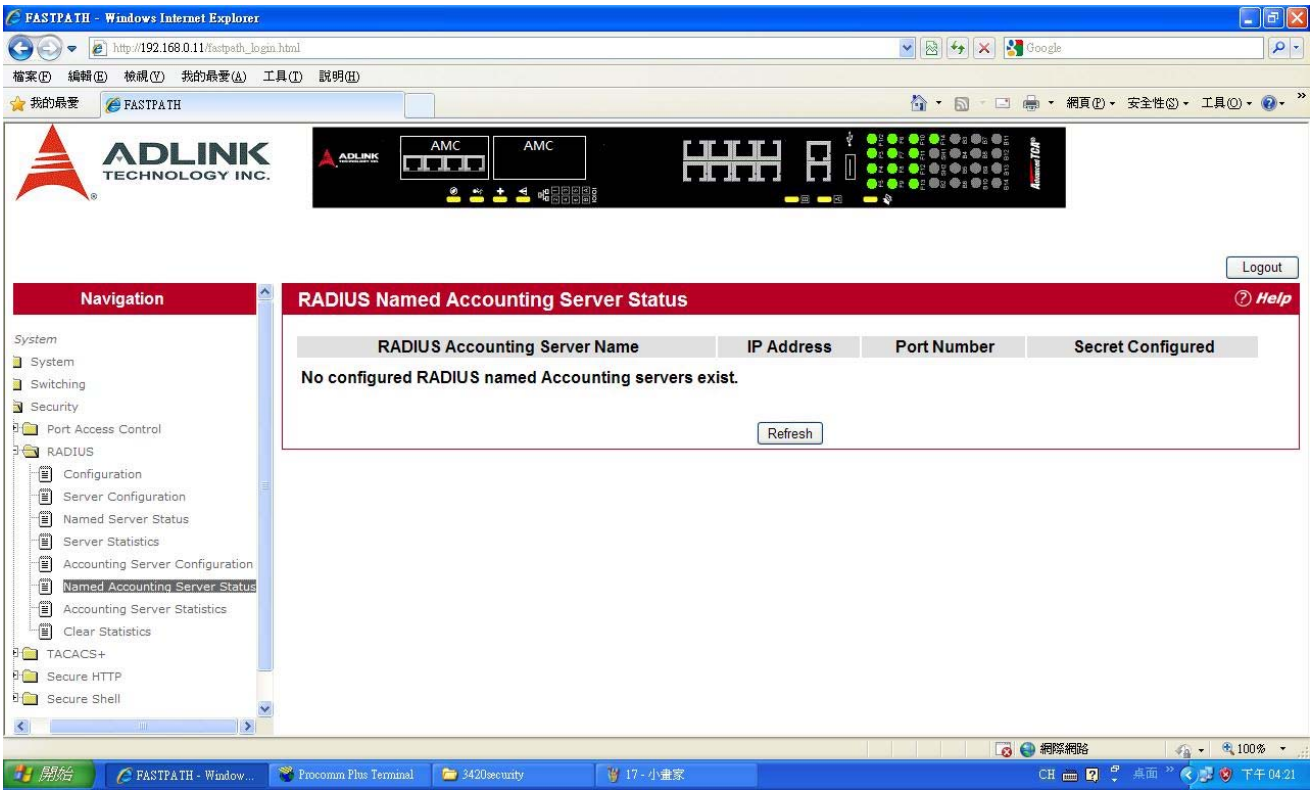
- If you make changes to the page, click Submit to apply the changes to the system.

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.

Named Accounting Server Status

The RADIUS Named Accounting Server Status page shows summary information about the accounting servers configured on the system.



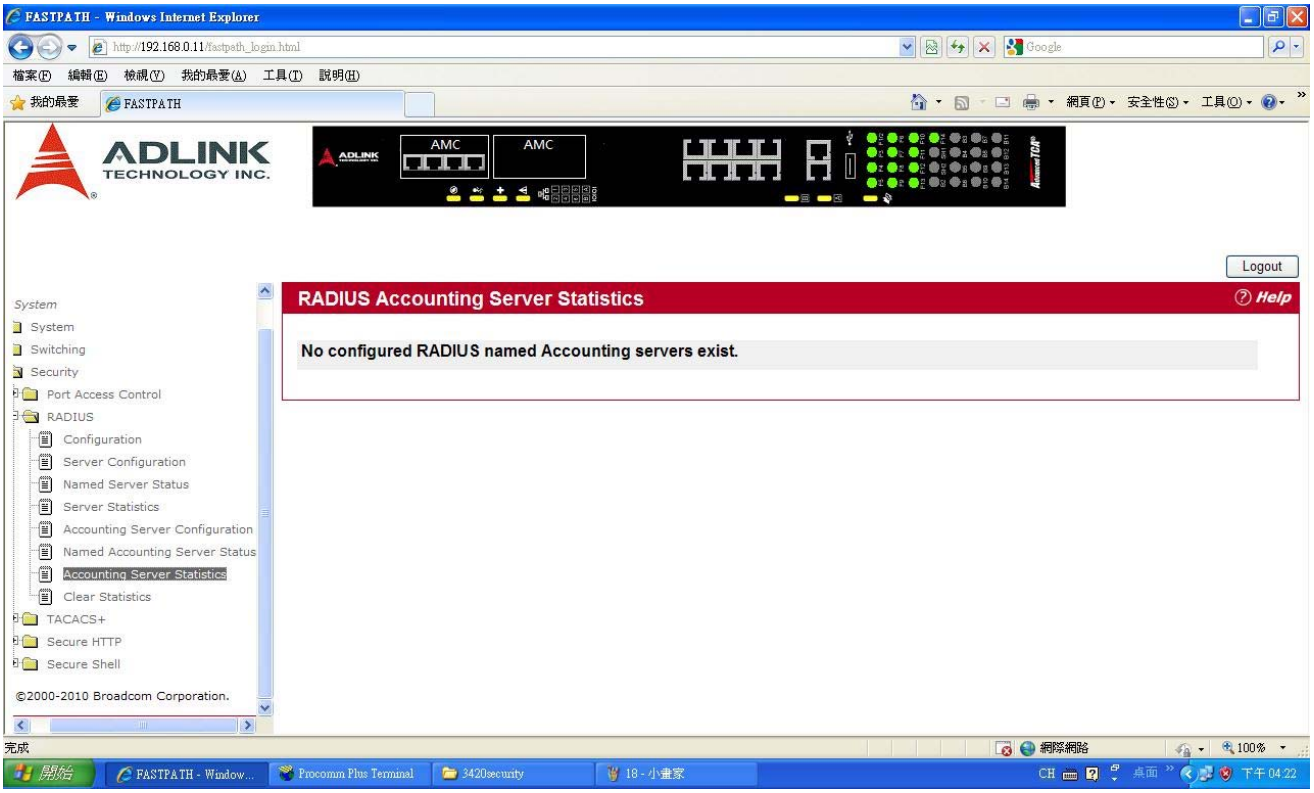
Field	Description
RADIUS Accounting Server Name	Shows the RADIUS accounting server name. Multiple RADIUS accounting servers can have the same name. In this case, RADIUS clients can use RADIUS servers with the same name as backups for each other.
IP Address	Shows the IP address of the RADIUS server.
Port 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.

Accounting Server Statistics

Use the RADIUS Accounting Server Statistics page to view statistical information for each RADIUS server configured on the system.

To access the RADIUS Accounting Server Statistics page, click Security > RADIUS > Accounting Server Statistics in the navigation menu.



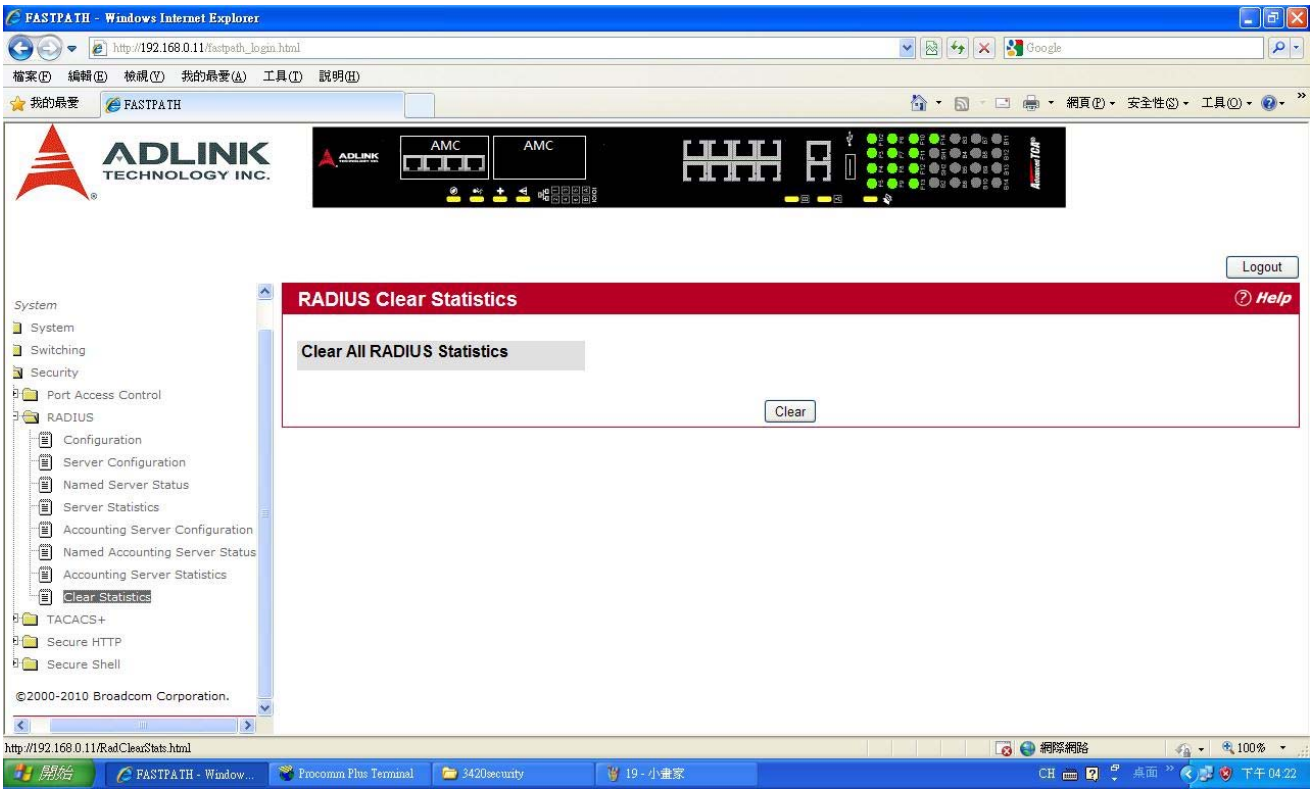
Field	Description
Accounting Server Host Address	Use the drop-down menu to select the IP address of the RADIUS accounting server for which to display statistics.
Round Trip Time (secs)	Displays the time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Accounting Requests	The number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.
Accounting Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this server.
Accounting Responses	Displays the number of RADIUS packets received on the accounting port from this server.
Malformed Access Responses	Displays the number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	Displays the number of RADIUS Accounting-Response packets that

Field	Description
	contained invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

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 Security > RADIUS > Clear Statistics in the navigation menu.



To clear all statistics for the RADIUS authentication and accounting server, click Clear.

5.25 TACACS+ Settings

FASTPATH® software 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.

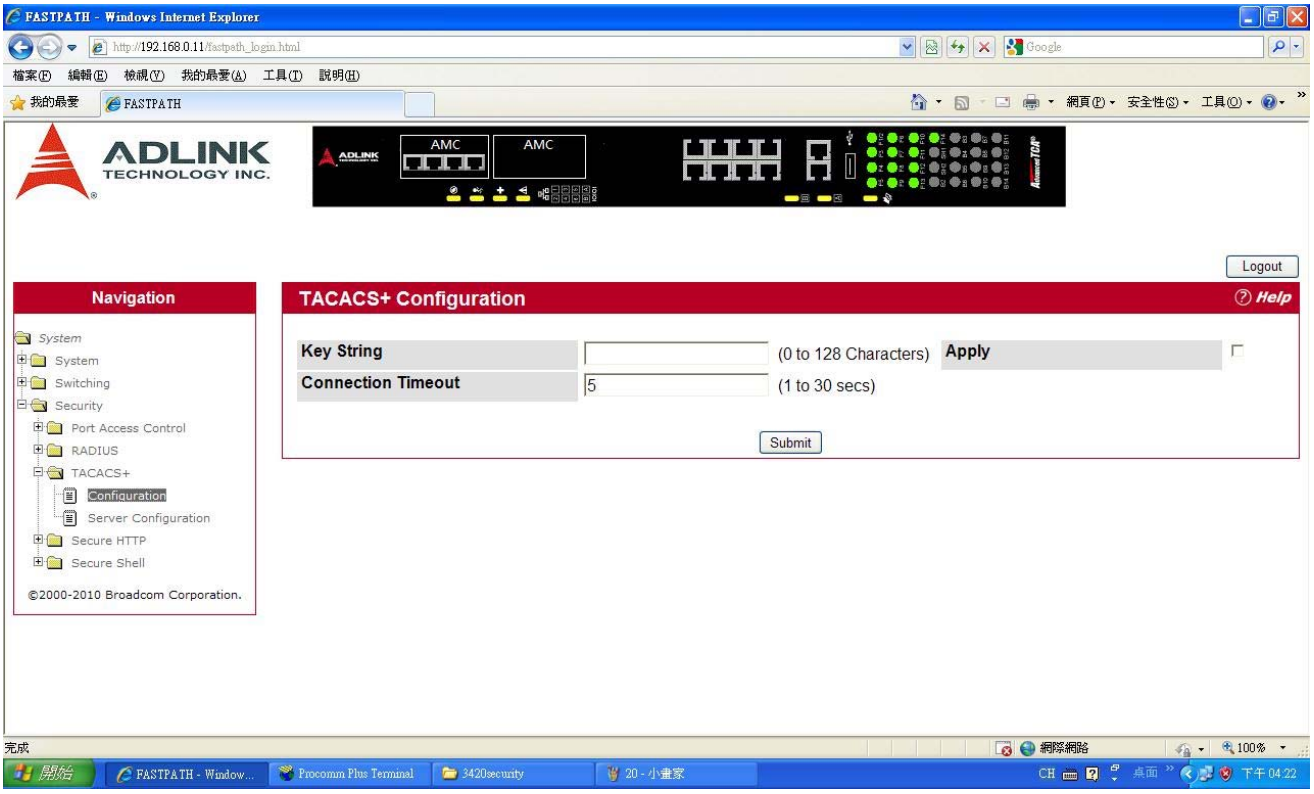
The TACACS+ folder contains links to the following web pages:

- TACACS+ Configuration
- TACACS+ Server Configuration

TACACS+ Configuration

The TACACS+ Configuration page contains the TACACS+ settings for communication between the switch and the TACACS+ server you configure. the inband management port.

To display the TACACS+ Configuration page, click Security > TACACS+ > Configuration in the navigation menu.



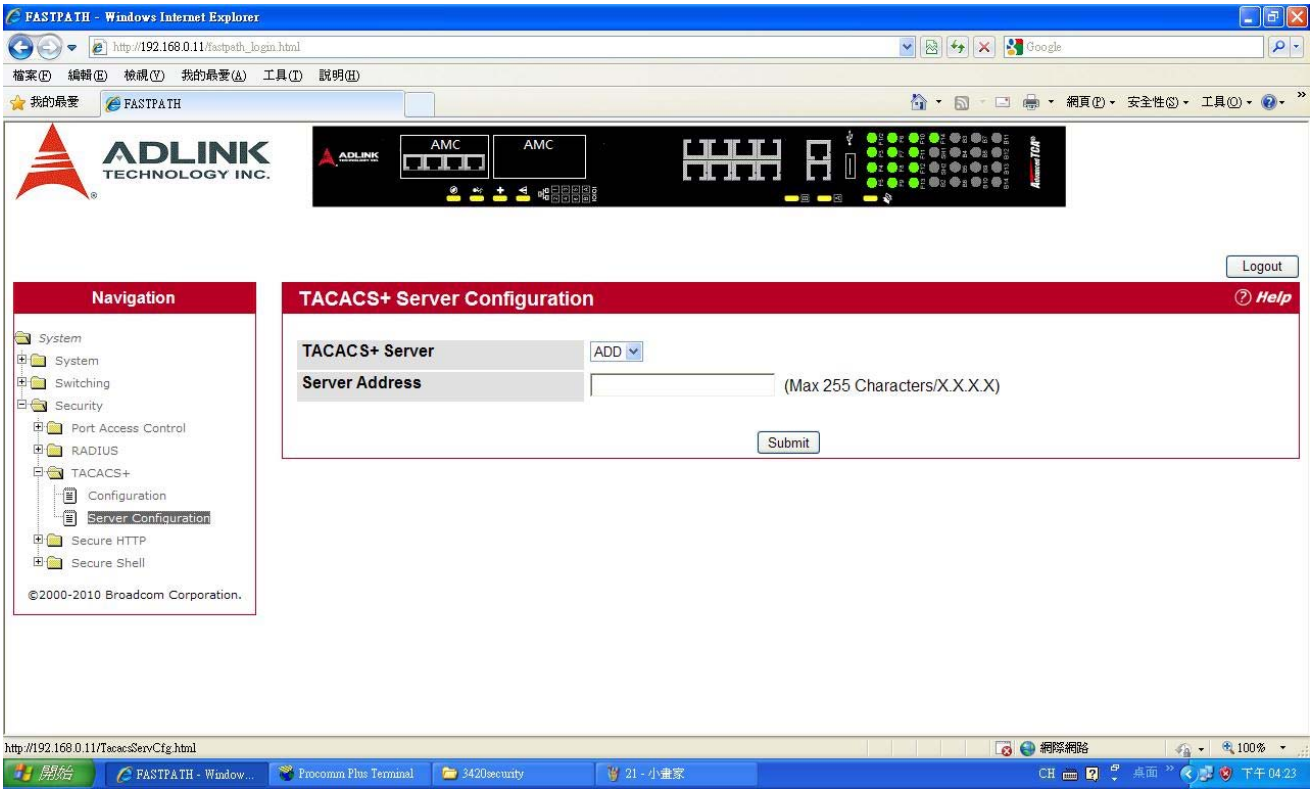
Field	Description
Key String	Specifies the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The valid range is 0-128 characters. The key must match the key configured on the TACACS+ server.
Connection Timeout	The maximum number of seconds allowed 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 Security > TACACS+ > Server Configuration in the navigation menu.



After you add one or more TACACS+ servers, additional fields appear on the RADIUS Accounting Server Configuration page.

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 RADIUS servers are configured on the system, the Add option is also available. Select Add to configure additional RADIUS servers.
IP Address	Enter the IP address of the RADIUS accounting server to add. This field is only available when Add is selected in the RADIUS Server IP Address 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.

Field	Description
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.

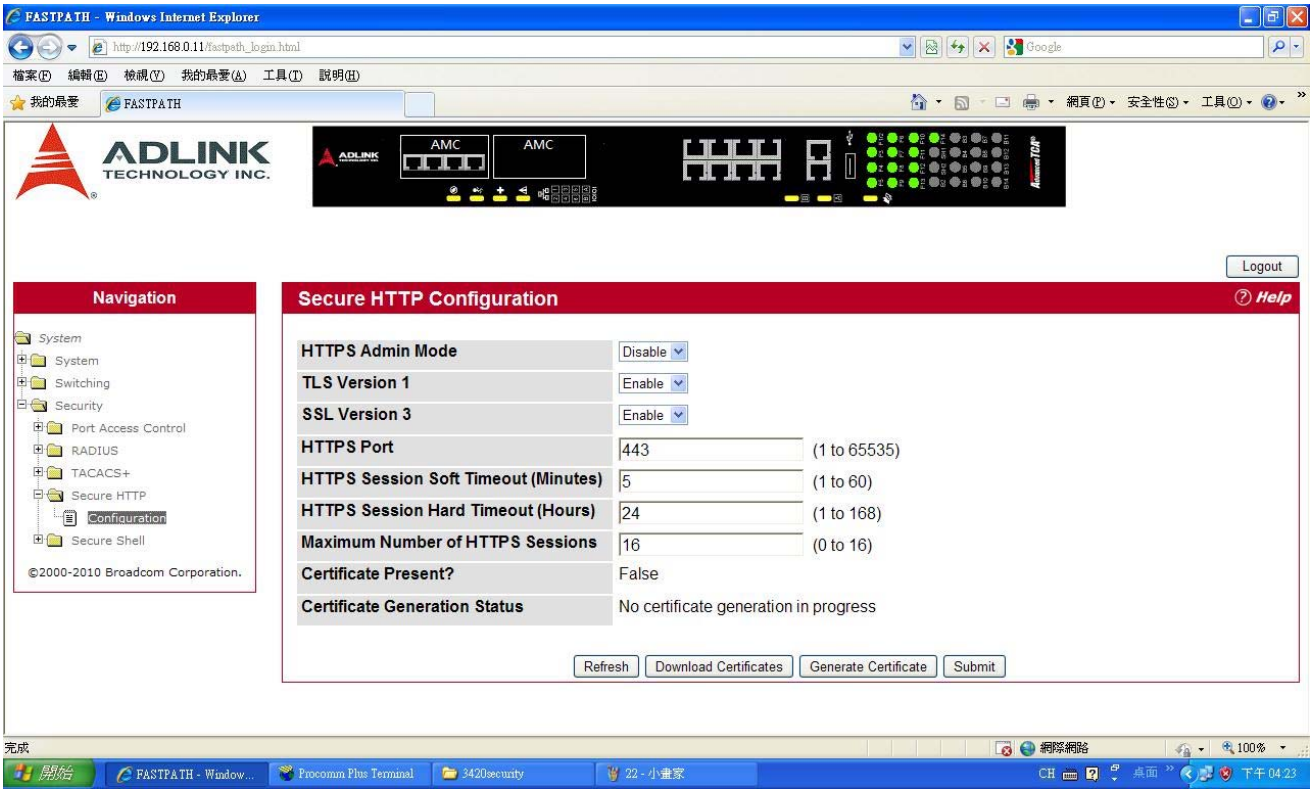
5.26 Secure HTTP

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.

Secure HTTP Configuration

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 Security > Secure HTTP > Configuration in the navigation menu.



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.

Field	Description
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 Number	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.
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 switch can 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 Certificates.

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

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 Security > Secure HTTP > Configuration in the navigation menu.

7. To enable the HTTPS admin mode, select Enable from the HTTPS Admin Mode field, and then click Submit.

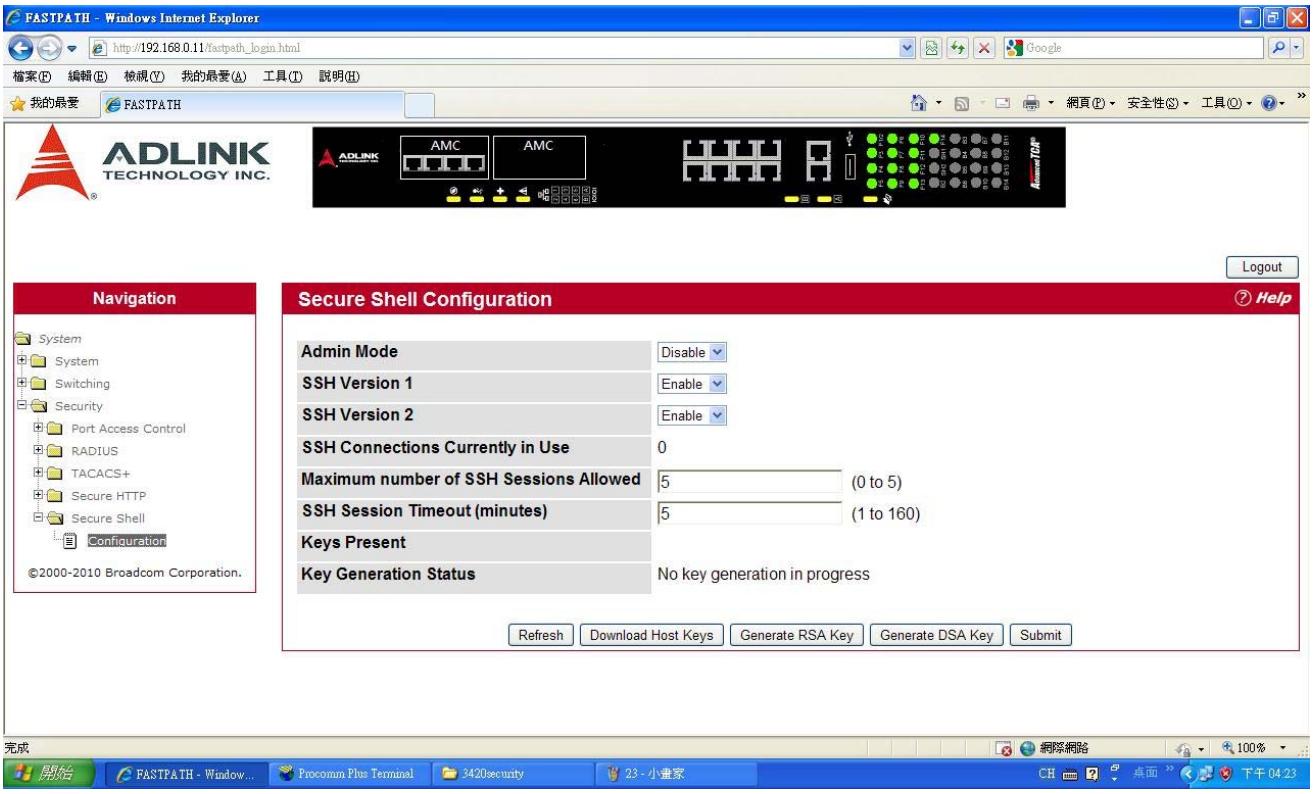
Secure Shell

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 Security > Secure Shell > Configuration in the navigation menu.



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. Setting this value to disable shuts down the SSH port. If the admin mode is set to disable, then all existing SSH connections remain connected until timed-out or logged out, but new SSH connections cannot be established. 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).
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.

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" in previous **SECURE HTTP CONFIGURATION** section. 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).

Safety Instructions

1. Read these safety instructions carefully.
2. Keep this user's manual for future reference.
3. Read the specifications section of this manual for detailed information on the operating environment of this equipment.
4. When installing/mounting or uninstalling/removing equipment, turn off power and unplug any power cords/cables.
5. To avoid electrical shock and/or damage to equipment:
    a. Keep equipment away from water or liquid sources;
    b. Keep equipment away from high heat or high humidity;
    c. Keep equipment properly ventilated (do not block or cover ventilation openings);
    d. Make sure to use recommended voltage and power source settings;
    e. Always install and operate equipment near an easily accessible electrical socket-outlet;
    f. Secure the power cord (do not place any object on/over the power cord);
    g. Only install/attach and operate equipment on stable surfaces and/or recommended mountings; and,
    h. If the equipment will not be used for long periods of time, turn off and unplug the equipment from its power source.
6. Never attempt to fix the equipment. Equipment should only be serviced by qualified personnel.
7. Equipment must be serviced by authorized technicians when:
    a. The power cord or plug is damaged;
    b. Liquid has penetrated the equipment;
    c. It has been exposed to high humidity/moisture;
    d. It is not functioning or does not function according to the user's manual;
    e. It has been dropped and/or damaged; and/or,
    f. It has an obvious sign of breakage.
8. The equipment can be operated at an ambient temperature of 55°C.

A Lithium-type battery may be provided for uninterrupted, backup or emergency power.

Warning! – Risk of explosion if battery is replaced with one of an incorrect type. Dispose of used batteries appropriately.

Getting Service

Contact us should you require any service or assistance.

ADLINK Technology, Inc.
Address: 9F, No.166 Jian Yi Road, Zhonghe District
New Taipei City 235, Taiwan
新北市中和區建一路 166 號 9 樓
Tel: +886-2-8226-5877
Fax: +886-2-8226-5717
Email: service@adlinktech.com

Ampro ADLINK Technology, Inc.
Address: 5215 Hellyer Avenue, #110, San Jose, CA 95138, USA
Tel: +1-408-360-0200
Toll Free: +1-800-966-5200 (USA only)
Fax: +1-408-360-0222
Email: info@adlinktech.com

ADLINK Technology (China) Co., Ltd.
Address: 上海市浦东新区张江高科技园区芳春路 300 号 (201203)
300 Fang Chun Rd., Zhangjiang Hi-Tech Park,
Pudong New Area, Shanghai, 201203 China
Tel: +86-21-5132-8988
Fax: +86-21-5132-3588
Email: market@adlinktech.com

ADLINK Technology Beijing
Address: 北京市海淀区上地东路 1 号盈创动力大厦 E 座 801 室(100085)
Rm. 801, Power Creative E, No. 1, B/D
Shang Di East Rd., Beijing, 100085 China
Tel: +86-10-5885-8666
Fax: +86-10-5885-8625
Email: market@adlinktech.com

ADLINK Technology Shenzhen
Address: 深圳市南山区科技园南区高新南七道 数字技术园 A1 栋 2 楼 C 区 (518057)
2F, C Block, Bldg. A1, Cyber-Tech Zone, Gao Xin Ave. Sec. 7,
High-Tech Industrial Park S., Shenzhen, 518054 China
Tel: +86-755-2643-4858
Fax: +86-755-2664-6353
Email: market@adlinktech.com

LiPPERT ADLINK Technology GmbH
Address: Hans-Thoma-Strasse 11, D-68163, Mannheim, Germany
Tel: +49-621-43214-0
Fax: +49-621 43214-30
Email: emea@adlinktech.com

ADLINK Technology, Inc. (French Liaison Office)
Address: 15 rue Emile Baudot, 91300 Massy CEDEX, France
Tel: +33 (0) 1 60 12 35 66
Fax: +33 (0) 1 60 12 35 66
Email: france@adlinktech.com

ADLINK Technology Japan Corporation
Address: 〒101-0045 東京都千代田区神田鍛冶町 3-7-4
神田 374 ビル 4F
KANDA374 Bldg. 4F, 3-7-4 Kanda Kajicho,
Chiyoda-ku, Tokyo 101-0045, Japan
Tel: +81-3-4455-3722
Fax: +81-3-5209-6013
Email: japan@adlinktech.com

ADLINK Technology, Inc. (Korean Liaison Office)
Address: 서울시 서초구 서초동 1675-12 모인터빌딩 8 층
8F Mointer B/D,1675-12, Seocho-Dong, Seocho-Gu,
Seoul 137-070, Korea
Tel: +82-2-2057-0565
Fax: +82-2-2057-0563
Email: korea@adlinktech.com

ADLINK Technology Singapore Pte. Ltd.
Address: 84 Genting Lane #07-02A, Cityneon Design Centre,
Singapore 349584
Tel: +65-6844-2261
Fax: +65-6844-2263
Email: singapore@adlinktech.com

ADLINK Technology Singapore Pte. Ltd. (Indian Liaison Office)
Address: 1st Floor, #50-56 (Between 16th/17th Cross) Margosa Plaza,
Margosa Main Road, Malleswaram, Bangalore-560055, India
Tel: +91-80-65605817, +91-80-42246107
Fax: +91-80-23464606
Email: india@adlinktech.com