

User Manual

EKI-9316P/ EKI-9312P Series

Industrial Managed 16-Port and 12-Port Full Gigabit Switch with PoE/ PoE+



Content

Chapter 1 Hardware Installation

1.1.	Introduction	2
1.2.	Key Features	2
1.2.1	EKI-9316P/ EKI-9312P.....	2
1.2.2	EKI-9316 / EKI-9312	2
1.3.	Product Models	3
1.3.1	EKI-9316P/ EKI-9312P.....	3
1.3.2	EKI-9316 / EKI-9312	3
1.4.	Specifications	4
1.4.1	EKI-9316P/ EKI-9312P.....	4
1.4.2	EKI-9316 / EKI-9312	7
1.5.	Package Contents	10
1.6.	Product Views	11
1.6.1	Front View.....	11
1.6.2	Rear View	14
1.6.3	Bottom View.....	15
1.7.	Mounting Options	15
1.7.1	DIN Rail Mounting.....	15
1.7.2	Wall Mounting (Optional Kit by Request).....	17
1.8.	Hardware Dimensions	19
1.9.	Power and Alarm Wiring	19
1.9.1	Overview	19
1.9.2	Considerations	20
1.9.3	Grounding the Device	21
1.9.4	Wiring a Relay Contact	22
1.9.5	Wiring the Power Inputs.....	23
1.9.6	Wiring the Digital Inputs	24
1.10.	Communication Port Wiring.	25
1.10.1	RJ45 Ethernet Cable Wiring	25
1.10.2	Mini-GBIC Fiber Transceivers.....	25
1.10.3	Network Device Validation	28
1.10.4	Validating Connectivity.....	28

1.10.5	Serial Console Port Wiring.....	29
1.10.6	USB Console Port Wiring.....	29
1.11.	Reset Button	30

Chapter 2 First Time Setup

2.1.	First Time Setup	32
2.1.1	Overview	32
2.1.2	Introduction	32
2.1.3	Administrative Interface Access.....	32
2.1.4	Using the Graphical (Web) Interface.....	33
2.1.5	Configuring the Switch for Network Access	33
2.1.6	Configuring the Ethernet Ports.....	34
2.2.	Web Browser Configuration.	35
2.2.1	Preparing for Web Configuration	35
2.2.2	System Login	35

Chapter 3 Management Interface

3.1.	Log In.	37
3.2.	Recommended Practices	37
3.2.1	Changing Default Password	37
3.3.	Management	38
3.3.1	System Information	38
3.3.2	System Description	39
3.3.3	IP Configuration	40
3.3.4	AAA.....	41
3.3.5	Local Password Management.....	49
3.3.6	Power over Ethernet	52
3.3.7	Email Alerts.....	57
3.3.8	SNMP	62
3.3.9	Event Manager	64
3.3.10	Trap Manager	66
3.3.11	DHCP Server	67
3.3.12	DNS	76
3.3.13	Date and Time	79
3.3.14	ISDP	84
3.3.15	LLDP.....	88

3.3.16	TACACS+	101
3.3.17	RADIUS	103
3.3.18	ARP Table	112
3.3.19	Reset Button	112
3.3.20	Login Sessions	113
3.4.	Switching	114
3.4.1	MAC Address Table.....	114
3.4.2	Interface Setting.....	122
3.4.3	Interface Statistics	128
3.4.4	Port Mirroring	139
3.4.5	VLAN Setting	142
3.4.6	QinQ	152
3.4.7	GARP.....	155
3.4.8	Port Channel.....	159
3.4.9	X-Ring Pro	162
3.4.10	Spanning Tree	165
3.4.11	Flow Control.....	174
3.5.	Multicast	174
3.5.1	IGMP Snooping	174
3.5.2	IGMP Snooping Querier.....	181
3.5.3	MLD Snooping	185
3.5.4	MLD Snooping Querier	192
3.5.5	L2 Multicast Table.....	195
3.5.6	GMRP Table	197
3.6.	Security	198
3.6.1	Denial of Service Protection.....	198
3.6.2	Port Access Control	199
3.6.3	DHCP Snooping	216
3.6.4	Protected Ports	229
3.7.	QoS	231
3.7.1	Access Control Lists	231
3.7.2	Differentiated Services.....	248
3.7.3	Class of Service	256

3.8.	Maintenance	263
3.8.1	System Resources.....	263
3.8.2	Config Save	264
3.8.3	Factory Defaults.....	264
3.8.4	Download.....	265
3.8.5	Upload	266
3.8.6	System Reset	268
3.8.7	Network Diagnostics	268

Chapter 4 Troubleshooting

4.1.	Troubleshooting.	274
------	--------------------------	-----

Federal Communication Commission Interference Statement

For further certification information, please go to www.advantech.com

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications when shielded cables are used for external wiring. We recommend the use of shielded cables. This kind of cable is available from Advantech. Please contact your local supplier for ordering information.

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

UL



Battery Information

Your Batteries

Batteries, battery packs, and accumulators should not be disposed of as unsorted household waste. Please use the public collection system to return, recycle or treat them in compliance with the local regulations.



Product Warranty (2 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out-of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

- Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any on screen messages you get when the problem occurs.
- Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
- If your product is diagnosed as defective, obtain an RMA (return merchandise authorization) number from your dealer. This allows us to process your return more quickly.
- Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
- Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Conventions



Warning signs are used to identify immediate hazards for property damage, injury or death.



CAUTION SIGNS ARE USED TO WARN AGAINST POTENTIAL HAZARDS OR TO CAUTION AGAINST UNSAFE PRACTICES.



Note signs are used to provide additional information for the device or settings.

Copyright

Copyright © 2014 Advantech Inc. All rights reserved. No part of this publication may be reproduced, adapted, stored in a retrieval system, translated into any language, or transmitted in any form or by any means without the written permission of the manufacturer.

Customer Support

Regional Service & Customization Centers

China | Kunshan
86-512-5777-5666

Taiwan | Taipei
886-2-2792-7818

Netherlands | Eindhoven
31-40-267-7000

Poland | Warsaw
48-22-33-23-730

USA | Milpitas, CA
1-408-519-3898

Worldwide Offices

Greater China

China

Toll Free 800-810-0345
Beijing 86-10-6298-4346
Shanghai 86-21-3632-1616
Shenzhen 86-755-8212-4222
Chengdu 86-28-8545-0198
Hong Kong 852-2720-5118

Taiwan

Toll Free 0800-777-111
Neihu 886-2-2792-7818
Xindian 886-2-2218-4567
Taichung 886-4-2329-0371
Kaohsiung 886-7-229-3600

Asia Pacific

Japan

Toll Free 0800-500-1055
Tokyo 81-3-6802-1021
Osaka 81-3-6802-1021

Korea

Toll Free 080-363-9494
Seoul 82-2-3663-9494

Singapore

Singapore 65-6442-1000

Malaysia

Toll Free 1800-88-1809
Kuala Lumpur 60-3-7725-4188
Penang 60-4-537-9188

Thailand

Bangkok 66-2-248-3140

India

Bangalore 1800-425-5070
Pune 1800-425-5071

Indonesia

Jakarta 62-21-751-1939

Australia

Toll Free 1300-308-531
Melbourne 61-3-9797-0100
Sydney 61-2-9476-9300

Europe

Germany

Toll Free 00800-2426-8080
Munich 49-89-12599-0
Düsseldorf 49-2103-97-855-0

France

Paris 33-1-4119-4666

Italy

Milano 39-02-9544-961

Benelux & Nordics

Breda 31-76-5233100

UK

Reading 44-0118-929-4540

Poland

Warsaw 48-22-33-23-730

Russia

Toll Free 8-800-555-01-50
Moscow 7-495-644-0364
St. Petersburg Office 7-812-332-5727

Americas

North America

Toll Free 1-888-576-9668
Cincinnati 1-513-742-8895
Milpitas 1-408-519-3898
Irvine 1-949-420-2500

Brazil

Toll Free 0800-770-5355
Saude-São Paulo 55-11-5592-5355

Mexico

Toll Free 1-800-467-2415
Mexico City 52-55-6275-2777

Safety Information

Safety Requirements

Before you begin installing the device, read through the following safety guidelines to prevent personal injury or property damage.

- Seek assistance from a trained professional installer, especially if it is your first time to install this device.
- Choose your installation site carefully, noting the location of electric power and circuit lines and ensuring that there are no obstructions.
- Do not attempt to service or open the device by yourself. Bring it to a qualified personnel or service center for repairs.
- The product was submitted and evaluated for use at the maximum ambient temperature permitted by the manufacture's specification of: 60°C

Electrostatic Discharge Requirements

Follow the steps below to protect components from electrostatic discharge:

1. Wear an ESD wrist strap when installing the device.
2. Handle the power adapter by its edge and do not touch any component or printed circuit boards.

Temperature/Humidity Requirements

Make sure to keep the temperature and humidity of the installation location at an optimal level. Very high temperatures may cause poor insulation, power leakage, mechanical property changes, and metal component corrosion. Very high temperatures will also accelerate insulation aging, which will greatly degrade reliability and even severely shorten operation life.

Under over-low humidity environments, insulation spacers may shrink, resulting in loosening of mounting screws. Extremely low humidity may also cause static electricity, which will damage the circuit.

Maintenance Requirements

Dust is a major safety hazard for this device. Dust may cause electrostatic absorption, resulting in bad contact between metal connectors or metal joints. Electrostatic absorption is faster and easier in environments with very low humidity, shortening device life and also causing communication failure.

Dust content and particle size requirements are as follows:

Table 1. Dust Content and Particle Size Requirements

Mechanical Active Substance	Content (number/m ³)
Dust Particle	≤3×10 ⁴ (no dust can be seen on desk in three days)
Dust particle diameter: ≥5μm	

Aside from dust, there should be strict limitation on air contained in the room where the device is located. Too much salt, acid and sulfide in the air will accelerate metal corrosion and aging process of certain components. There should be measures to prevent harmful gas such as SO₂, H₂S, NH₃ and Cl₂ from entering the operational environment.

Table 2. Maximum Values for Harmful Gases

Gas	Max. Value (mg/m ³)
SO ₂	0.2
H ₂ S	0.0006
NH ₃	0.05
Cl ₂	0.01

Power over Ethernet (PoE)

PoE Requirements

This product was in-door used and not connected to outside plant. The equipment is to be connected only to PoE networks without routing to the outside plant.

Warnings

- Do NOT place your device near water such as a wet basement.
- Do NOT expose your device to dust, dampness, or corrosive liquids.
- Do NOT place heavy objects on your device.
- Do NOT install, use or service your device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Make ONLY suitable connections to your device.
- Make sure all connecting cables from your device are carefully placed.
- Use ONLY an appropriate power adaptor or cord to the right supply voltage.
- Do NOT place any objects on the power adaptor or cord.
- Do NOT use your device when the power adaptor or cord is damaged as it might cause electrocution.
- Remove the power adapter or cord from the power outlet when it is damaged.
- Do NOT attempt to repair the power adapter or cord. Contact your local vendor to order a new one.
- ONLY use your device indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the ventilation slots of your device, as insufficient airflow may hard it.

About This Manual

This user manual is intended to guide professional installers in installing and configuring the EKI-9316P/ EKI-9312P (PoE/PoE+) and EKI-9316 / EKI-9312 Industrial Managed 16-Port and 12-Port Full Gigabit Switches series, and in building the infrastructure centered on it. It includes procedures to assist you in avoiding unforeseen problems.

Hardware Installation

Chapter 1

1.1. Introduction

The EKI-9316P/EKI-9312P series include EKI-9316P, EKI-9312P, EKI-9316 and EKI-9312.

1.2. Key Features

1.2.1 EKI-9316P/ EKI-9312P

- -40°C to 75°C operating temperature range
- IEEE802.3at PoE+ to supply 30W power
- IEEE802.3af PoE to supply 15.4W power
- CAT-5 cable length diagnostics function
- PoE Power management
- PoE Power input range from 46~57VDC
- Reset button for auto image/configuration upgrade
- USB port for image/configuration backup, restore and upgrade
- Redundant power inputs for higher system reliability
- STP, RSTP, MSTP and X-Ring Pro for better redundancy
- Security mechanism including SSL,SSH, 802.1X, MAC, IP filtering, RADIUS, TACACS+, VLAN for access protection

1.2.2 EKI-9316 / EKI-9312

- -40°C to 75°C operating temperature range
- CAT-5 cable length diagnostics function
- Reset button for auto image/configuration upgrade
- USB port for image/configuration backup, restore and upgrade
- Redundant power inputs for higher system reliability
- STP, RSTP, MSTP, X-Ring Pro for better redundancy
- Security mechanism including SSL,SSH, 802.1X, MAC, IP filtering, RADIUS, TACACS+, VLAN for access protection

1.3. Product Models

1.3.1 EKI-9316P/ EKI-9312P

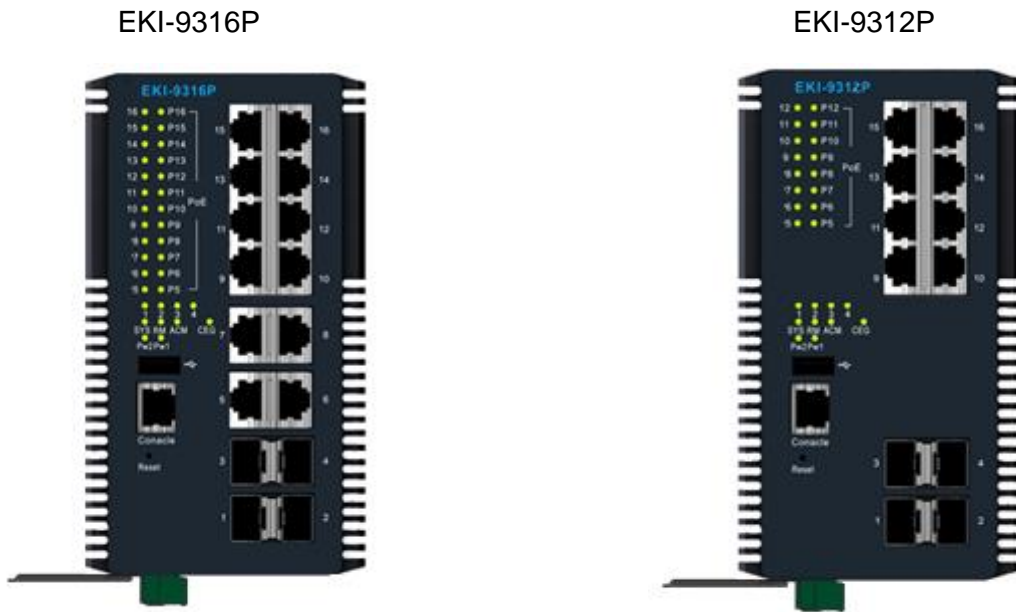


Figure 1-1. EKI-9316P/ EKI-9312P

1.3.2 EKI-9316 / EKI-9312

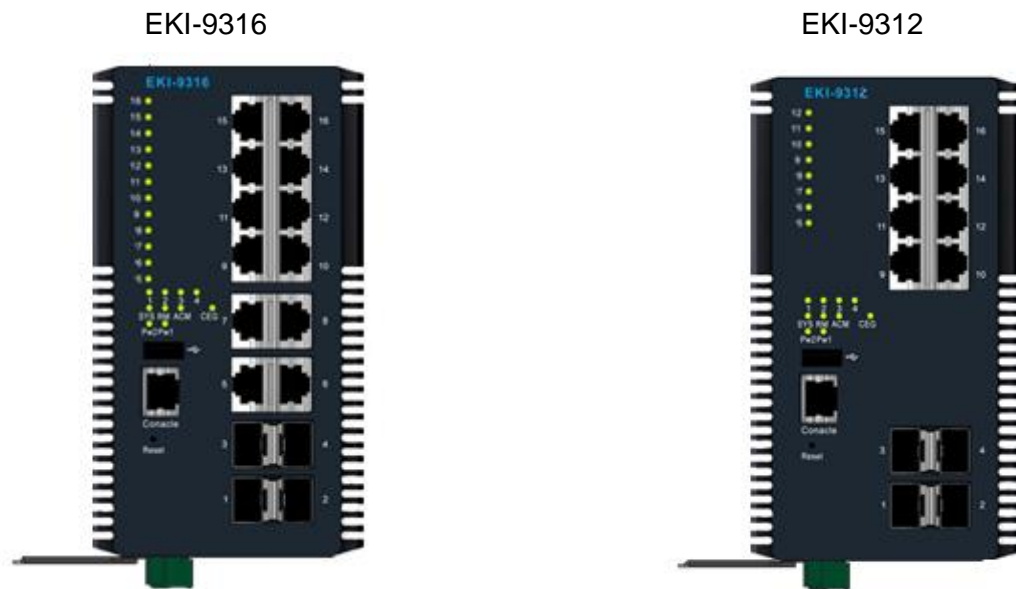


Figure 1-2. EKI-9316 / EKI-9312

1.4. Specifications

1.4.1 EKI-9316P / EKI-9312P

Table 1-1. EKI-9316P / EKI-9312P Specifications

Specifications	Description	
Interface	I/O Port	<ul style="list-style-type: none"> 8 x 10/100/1000Base-T/TX RJ-45 (P5~P12 with PoE/PoE+) 12 x 10/100/1000Base-T/TX RJ-45 (P5~P16 with PoE/PoE+) 4 x 100/1000Base-FX/X SFP (P1~P4)
	Console port	RJ-45
	F/W backup port	USB (support Transcend and ATP USB)
	PoE Pinout	V+: Pin1, 2; V-: Pin 3, 6
	Power Connector	6-pin screw Terminal Block (including relay)
Physical	Enclosure	Aluminum Shell
	Protection Class	IP30
	Installation	DIN-Rail
	Dimensions (W x H x D)	<ul style="list-style-type: none"> 86 x 165 x 125 (mm) 3.39 x 6.5 x 4.92 (inch)
LED Display	System LED	PWR1, PWR2, SYS, CFG, Alarm and R.M.
	Port LED	Link / Speed / Activity / PoE
Environment	Operating Temperature	-40°C ~ 75°C (-40°F ~ 167°F)
	Storage Temperature	-40°C ~ 85°C (-40°F ~ 185°F)
	Ambient Relative Humidity	10 ~ 95% (non-condensing)

Table 1-1. EKI-9316P / EKI-9312P Specifications (Continued)

Specifications	Description	
Switch Properties	MAC Address	16K entries
	Switching Bandwidth	<ul style="list-style-type: none">EKI-9316P: 32GbpsEKI-9312P: 24Gbps
	Packet Buffer	1.5MB
	Jumbo Frame	12KB
	Priority Queue	8
	Simultaneous VLAN	4K
	VLAN ID Range	1~4093
	Multicast Group	1024
	Max. Trunk Port/Groups	<ul style="list-style-type: none">EKI-9316P: 8/8EKI-9312P: 8/6

Table 1-1. EKI-9316P / EKI-9312P Specifications (Continued)

Specifications	Description	
Technology compliance	IEEE	802.1ab LLDP, 802.1ad provider bridging, 802.1d STP, 802.1p Ethernet priority with user provisioning and mapping, 802.1q Virtual LANs w/ port-based VLANs, 802.1s MSTP, 802.1w RSTP, 802.1x Authentication, 802.3 10BaseT, 802.3ab 1000BaseT(X), 802.3ac VLAN tagging, 802.3ad Link aggregation, 802.3af PoE, 802.3at PoE+, 802.3u 100BaseT(X), 802.3x Flow Control, 802.3z 1000BaseX
	RFC	<ul style="list-style-type: none"> • 768 User Datagram Protocol, 783 TFTP Protocol • 791 Internet Protocol, 792 Internet Control Message Protocol • 793 Transmission Control Protocol • 826 An Ethernet Address Resolution Protocol • 896 Congestion Control in IP/TCP Internetworks • 951 BOOTP, 1157 SNMP, 1321 Message-Digest Algorithm • 1034 Domain Names - Concepts and Facilities (Client Only) • 1035 Domain Names-Implementation and Specification (Client Only) • 1534 Interoperation Between BootP and DHCP • 1901 Community-based SNMPv2 • 1908 Coexistence between SNMP v1 and SNMP v2 • 2030 SNTP Version 4 for IPv4, IPv6 and OSI • 2068 HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03 • 2131 Dynamic Host Configuration Protocol • 2132 DHCP Options and BOOTP Vendor Extensions • 2866 RADIUS Accounting 2865 RADIUS client • 4251 SSH Protocol Architecture • 4253 SSH Transport Layer Protocol • 4254 SSH Connection Protocol
	SNMP MIBs	1213, 1493, 1643, 2233, 2618, 2674, 2737, 2819
Power	Power Consumption	<ul style="list-style-type: none"> • ~ 21.82 Watts (System) • EKI-9316P: ~294.22 Watts (Full loading for 6 PoE / 6 PoE+) • EKI-9312P: ~203.42 Watts (Full loading for 4 PoE / 4 PoE+)
	Power Input	48 (46 to 57 V) VDC dual inputs (>50VDC for PoE+ output recommended)

Table 1-1. EKI-9316P / EKI-9312P Specifications (Continued)

Specifications	Description	
Certifications	EMC	<ul style="list-style-type: none"> CE, FCC Class A UL60950 C1D2 EN61000-6-4; EN61000-6-2; EN61000-4-2 (ESD) Level 4 EN61000-4-3 (RS) Level 4; EN61000-4-4 (EFT) Level 4 EN61000-4-5 (Surge) Level 4; EN61000-4-6 (CS) Level 3 EN61000-4-8 (Magnetic Field) Level 4 EN50121-4
	Shock	IEC60068-2-27
	Free fall	IEC60068-2-32
	Vibration	IEC60068-2-6

1.4.2 EKI-9316 / EKI-9312

Table 1-2. EKI-9316 / EKI-9312 Specifications

Specifications	Description	
Interface	I/O Port	<ul style="list-style-type: none"> 8 x 10/100/1000Base-T/TX RJ-45 12 x 10/100/1000Base-T/TX RJ-45 4 x 100/1000Base-FX/X SFP (P1~P4)
	Console port	RJ-45
	F/W backup port	USB (support Transcend and ATP USB)
	Power Connector	6-pin screw Terminal Block (including relay)
Physical	Enclosure	Aluminum Shell
	Protection Class	IP30
	Installation	DIN-Rail
	Dimensions (W x H x D)	<ul style="list-style-type: none"> 86 x 165 x 125 (mm) 3.39 x 6.5 x 4.92 (inch)
LED Display	System LED	PWR1, PWR2, SYS, CFG, Alarm and R.M.
	Port LED	Link / Speed / Activity
Environment	Operating Temperature	-40°C ~ 75°C (-40°F ~ 167°F)
	Storage Temperature	-40°C ~ 85°C (-40°F ~ 185°F)
	Ambient Relative Humidity	10 ~ 95% (non-condensing)

Table 1-2. EKI-9316 / EKI-9312 Specifications (Continued)

Specifications	Description	
Switch Properties	MAC Address	16K entries
	Switching Bandwidth	<ul style="list-style-type: none">EKI-9316: 32GbpsEKI-9312: 24Gbps
	Packet Buffer	1.5MB
	Jumbo Frame	12KB
	Priority Queue	8
	Simultaneous VLAN	4K
	VLAN ID Range	1~4093
	Multicast Group	1024
	Max. Trunk Port/Groups	<ul style="list-style-type: none">EKI-9316: 8/8EKI-9312: 8/6

Table 1-2. EKI-9316 / EKI-9312 Specifications (Continued)

Specifications	Description	
Technology compliance	IEEE	802.1ab LLDP, 802.1ad provider bridging, 802.1d STP, 802.1p Ethernet priority with user provisioning and mapping, 802.1q Virtual LANs w/ port-based VLANs, 802.1s MSTP, 802.1w RSTP, 802.1x Authentication, 802.3 10BaseT, 802.3ab 1000BaseT(X), 802.3ac VLAN tagging, 802.3ad Link aggregation, 802.3u 100BaseT(X), 802.3x Flow Control, 802.3z 1000BaseX
	RFC	<ul style="list-style-type: none"> • 768 User Datagram Protocol, 783 TFTP Protocol • 791 Internet Protocol, 792 Internet Control Message Protocol • 793 Transmission Control Protocol • 826 An Ethernet Address Resolution Protocol • 896 Congestion Control in IP/TCP Internetworks • 951 BOOTP, 1157 SNMP, 1321 Message-Digest Algorithm • 1034 Domain Names - Concepts and Facilities (Client Only) • 1035 Domain Names-Implementation and Specification (Client Only) • 1534 Interoperation Between BootP and DHCP • 1901 Community-based SNMPv2 • 1908 Coexistence between SNMP v1 and SNMP v2 • 2030 SNTP Version 4 for IPv4, IPv6 and OSI • 2068 HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03 • 2131 Dynamic Host Configuration Protocol • 2132 DHCP Options and BOOTP Vendor Extensions • 2866 RADIUS Accounting • 2865 RADIUS client • 4251 SSH Protocol Architecture • 4253 SSH Transport Layer Protocol • 4254 SSH Connection Protocol
	SNMP MIBs	1213, 1493, 1643, 2233, 2618, 2674, 2737, 2819
Power	Power Consumption	~ 21.82 Watts (System)
	Power Input	24/48 VDC dual inputs

Table 1-2. EKI-9316 / EKI-9312 Specifications (Continued)

Specifications	Description	
Certifications	EMC	<ul style="list-style-type: none"> • CE, FCC Class A • UL60950 C1D2 • EN61000-6-4; EN61000-6-2; EN61000-4-2 (ESD) Level 4 • EN61000-4-3 (RS) Level 4; EN61000-4-4 (EFT) Level 4 • EN61000-4-5 (Surge) Level 4; EN61000-4-6 (CS) Level 3 • EN61000-4-8 (Magnetic Field) Level 4 • EN50121-4
	Shock	IEC60068-2-27
	Free fall	IEC60068-2-32
	Vibration	IEC60068-2-6

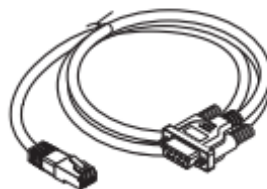
1.5. Package Contents



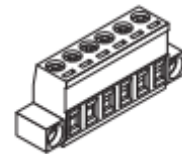
The switch is shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative for assistance.



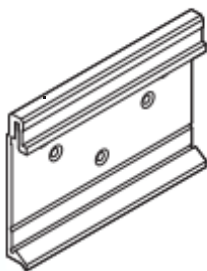
EKI-9316P / EKI-sEKI-9312P Series



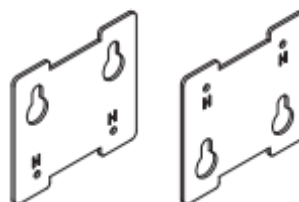
RS232 to RJ45 console port cable



Terminal block



DIN-Rail mounting plate
(attached to the rear panel of the switch)



Wall mounting kit

1.6. Product Views

1.6.1 Front View

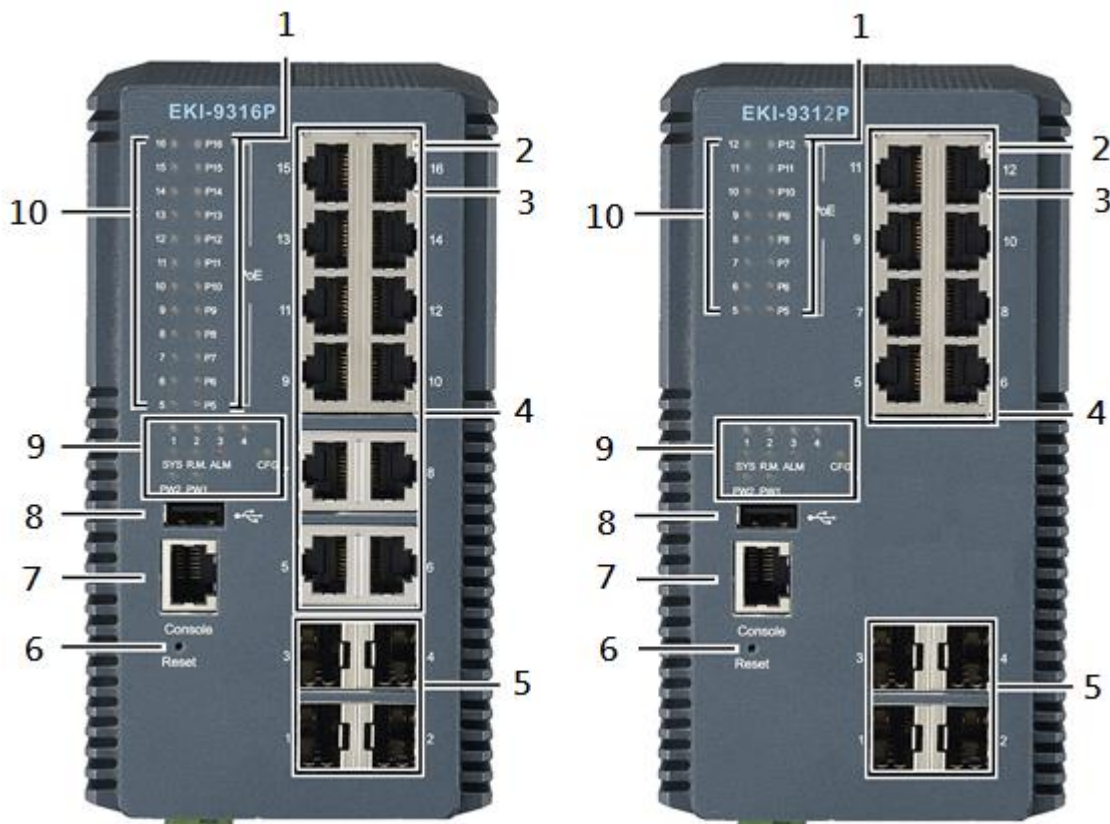


Figure 1-3. Front View

Table 1-3. Front View

No.	Item	Description
1	PoE LED (EKI-9316P / EKI-9312P only)	See Activity and PoE LED Panel on page 13
2	ETH port LED	10/100BaseT/TX LED indicator
3	ETH port LED	10/100/1000BaseT/TX LED indicator
4	ETH port LED	Twelve 10/100/1000Base-T/TX RJ45 (PoE/PoE+) ports (P5 to P16)
5	SFP slots	Four 100/1000Base-FX/X SFP ports (P1 to P4)
6	Reset button	Button allows for system soft reset or factory default reset
7	Console serial port	Console cable port to COM port (DB9 male) on computer to RS232 managed switch (RJ45 female)
8	USB 2.0	USB console port for image/configuration backup, restore and upgrading
9	System LED panel	See System LED Panel on page 12 for further details
10	Activity LED	See Activity and PoE LED Panel on page 13 for further details

System LED Panel

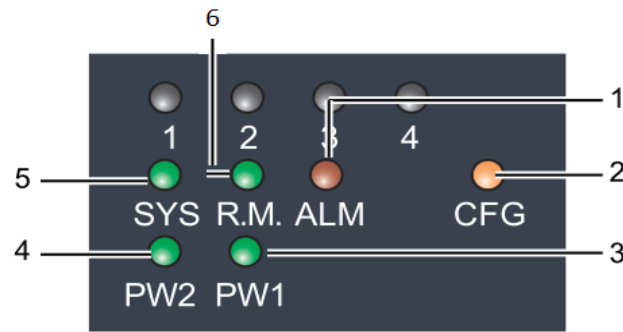


Figure 1-4. System LED Panel

Table 1-4. System LED Panel

No.	LED Name	LED Color	Description
1	ALM LED	Solid red	Defined major policies are detected
		Blinking red	Defined minor policies are detected
		Off	Powered off or system is operating normally
2	CFG LED	Solid amber	Normal status, no fault detected
		Blinking amber	Setting change detected but not saved for execution
		Off	Powered off or system is operating normally
3	PW1 LED	Solid green	Powered up
		Off	Powered down or not installed
4	PW2 LED	Solid green	Powered up
		Off	Powered down or not installed
5	SYS LED	Solid green	System is operating normally
		Off	System is powered down / system crash / operation initiating
6	R.M. LED	Solid green	Worked as Ring master
		Off	Normal status

Activity and PoE LED Panel

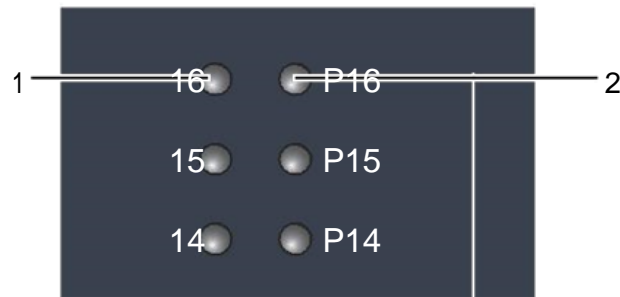


Figure 1-5. Activity and PoE LED Panel

Table 1-5. Activity and PoE LED Panel

No.	LED Name	LED Color	Description
1	Link / Status / Speed	Solid green	Secure 1000Mbps connection (Only for Gigabit Ethernet port)
		Blinking green	Data transmission rate of 1000Mbps (Only for Gigabit Ethernet port)
		Off	No connection detected or system is powered down
		Solid amber	Secure 10/100Mbps connection (100Mbps for SFP port)
		Blinking amber	Data transmission rate of 10/100Mbps (100Mbps for SFP port)
2	PoE (EKI-9316P / EKI-9312P only)	Solid green	Connected to a power distribution device
		Off	No power distribution device detected

1.6.2 Rear View

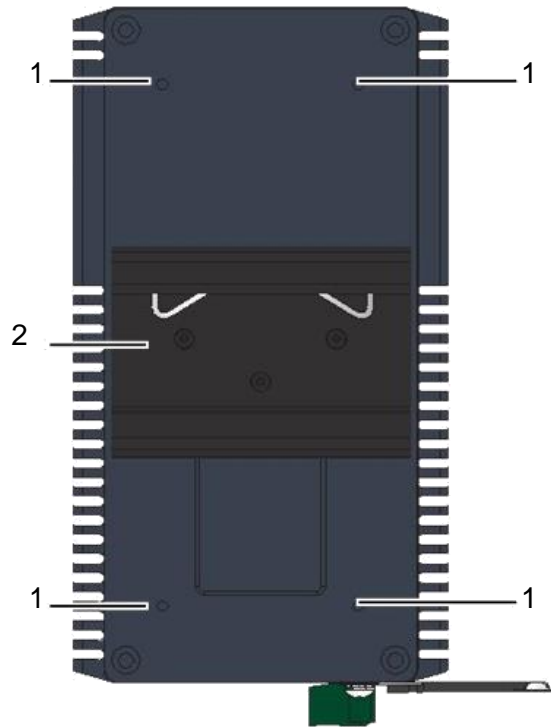


Figure 1-6. Rear View

Table 1-6. Rear View

No.	Item	Description
1	Wall mounting holes	Screw holes (x4) used in the installation of a wall mounting plate
2	DIN-Rail mounting plate	Mounting plate used for the installation to a standard DIN rail

1.6.3 Bottom View

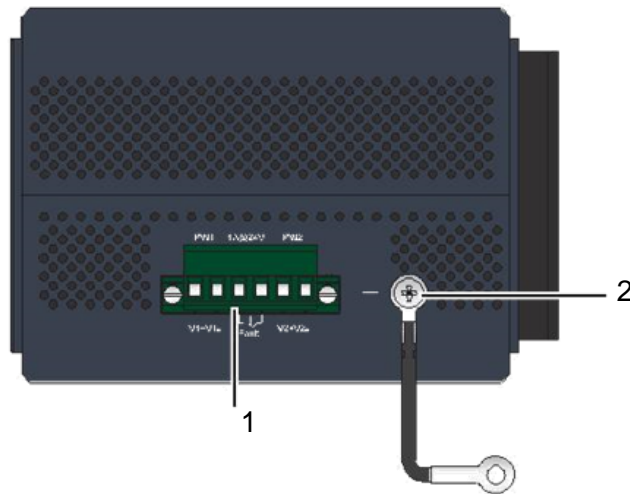


Figure 1-7. Bottom View

Table 1-7. Bottom View

No.	Item	Description
1	Terminal block	Connect cabling for power and alarm wiring
2	Ground terminal	Screw terminal used to ground chassis

1.7. Mounting Options

1.7.1 DIN Rail Mounting

The DIN rail mount option is the quickest installation option. Additionally, it optimizes the use of rail space.

The metal DIN rail kit is secured to the rear of the switch. The device can be mounted onto a standard (corrosion-free mounting rail is advisable) 35mm (1.37") x 75 mm (3") height DIN rail. The devices can be mounted vertically or horizontally. Refer to the following guidelines for further information.



When installing, make sure to allow for enough space to properly install the cabling.

Installing the DIN-Rail Mounting Kit

- Insert the top back of the mounting bracket over the DIN rail.
- Push the bottom of the switch towards the DIN rail until it snaps into place.

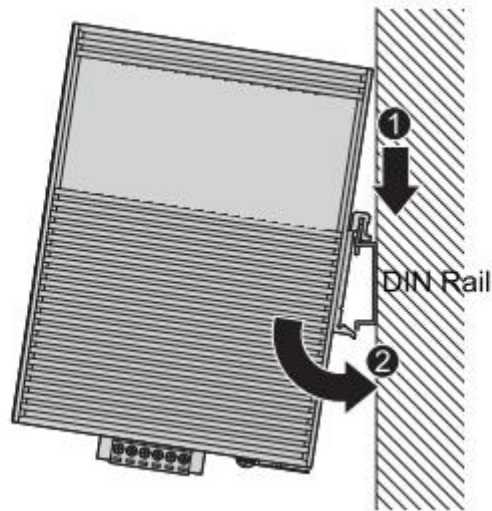


Figure 1-8. Installing the DIN-Rail Mounting Kit

Removing the DIN-Rail Mounting Kit

1. Push the switch down to free the bottom of the plate from the DIN rail.
2. Rotate the bottom of the device towards you and away from the DIN rail.
3. Once the bottom is clear of the DIN rail, lift the device straight up to unhook it from the DIN rail.

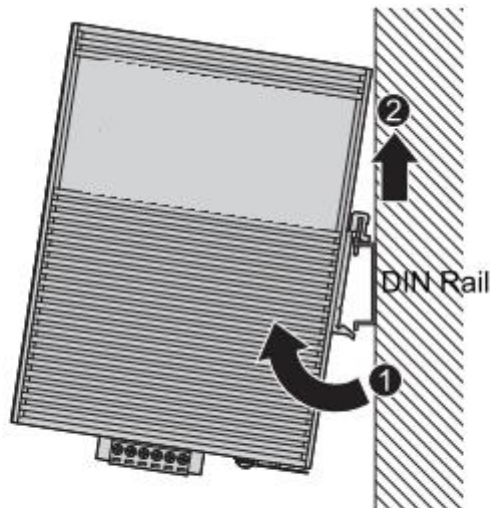


Figure 1-9. Removing the DIN-Rail

1.7.2 Wall Mounting (Optional Kit by Request)

The wall mounting option provides better shock and vibration resistance than the DIN rail vertical mount.



When installing, make sure to allow for enough space to properly install the cabling.

Before the device can be mounted on a wall, you will need to remove the DIN rail plate.

1. Rotate the device to the rear side and locate the DIN mounting plate.
2. Remove the screws securing the DIN mounting plate to the rear panel of the switch.
3. Remove the DIN mounting plate. Store the DIN mounting plate and provided screws for later use.
4. Align the wall mounting plates on the top and bottom of the rear side. The screw holes on the device and the mounting plates must be aligned, see the following illustration.
5. Secure the wall mount plates with M3 screws, see the following figure.

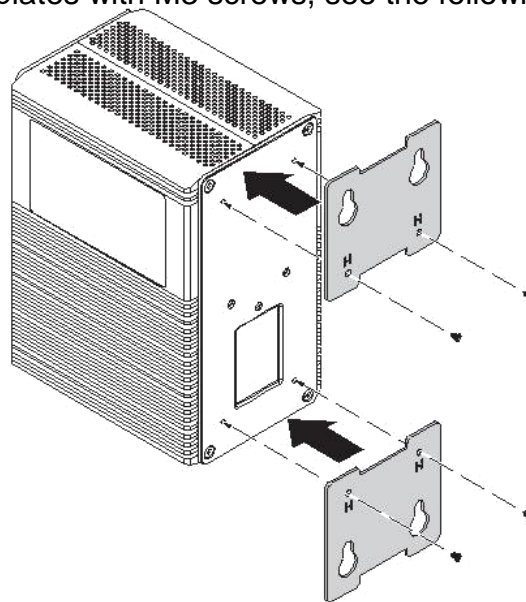


Figure 1-10. Installing Wall Mount Plates

Once the wall mounting plates are secure on the device, you will need to attach the wall screws (x4).

6. Locate the installation site and place the switch against the wall, making sure it is the final installation location.
7. Use the wall mount plates as a guide to mark the locations of the screw holes.
8. Drill four holes over the four marked locations on the wall, keeping in mind that the holes must accommodate wall sinks in addition to the screws.
9. Insert the wall sinks into the walls.

10. Insert the screws into the wall sinks. Leave a 6mm gap between the wall and the screw head to allow for wall mount plate insertion.



Figure 1-11. Securing Wall Mounting Screws



- Make sure the screws dimensions are suitable for use with the wall mounting plate.
- Do not completely tighten the screws into the wall. A final adjustment may be needed before fully securing the wall mounting plates on the wall.

11. Align the wall mount plate over the screws on the wall.
12. Install the wall mount plate on the screws and slide it down to lock in place, see the following figure.

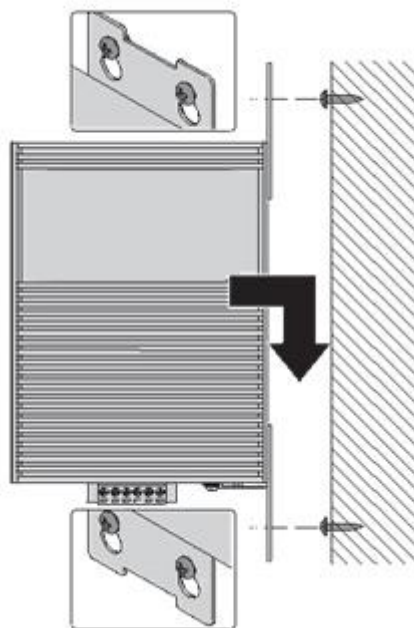


Figure 1-12. Wall Mount Installation

13. Once the device is installed on the wall, tighten the screws to secure the device.

1.8. Hardware Dimensions

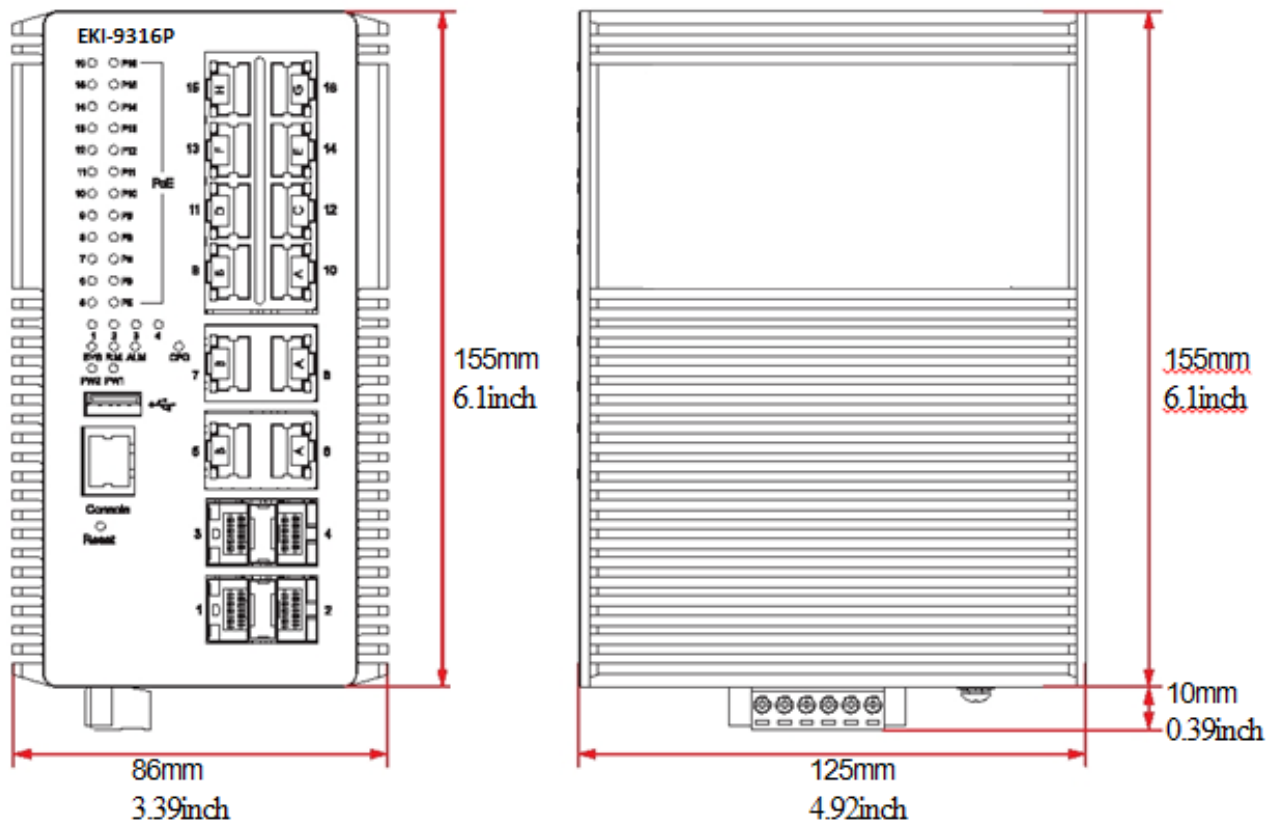


Figure 1-13. Hardware Dimensions

1.9. Power and Alarm Wiring

1.9.1 Overview



POWER DOWN AND DISCONNECT THE POWER CORD BEFORE SERVICING OR WIRING THE SWITCH.



Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch device.



Disconnect the power cord before installation or cable wiring.

The switches can be powered by using the same DC source used to power other devices. A DC voltage range of 10 to 30 VDC (3.0W) must be applied between the V1+ terminal and the V1- terminal (PW1), see the following illustrations. A Class 2 power supply is required to maintain a UL60950 panel listing. The chassis ground screw terminal should be tied to the panel or chassis ground. A redundant power configuration is supported through a secondary power supply unit to reduce network down time as a result of power loss.

EKI-9316 / EKI-9312 supports 24 and 48 VDC and EKI-9316P / EKI-9312P supports 48 VDC (for PoE) and 50 VDC (for PoE+). For PoE sourcing (PSE) operation, a power range of 46 to 57 VDC is necessary. Make sure the 48 VDC supply is rated at 15.4W per PoE port and the 50 VDC supply is rated at 30W per PoE+ port. Dual power inputs are supported and allow you to connect a backup power source.

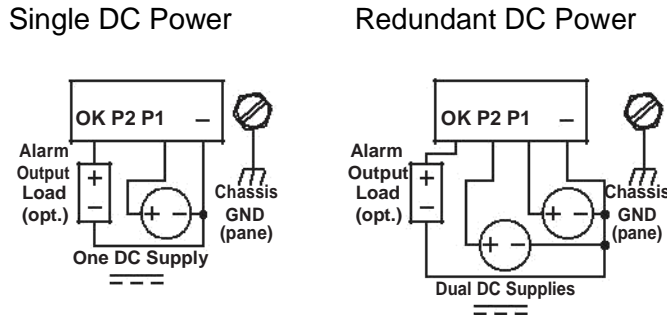


Figure 1-14. Power Wiring for Managed Switches

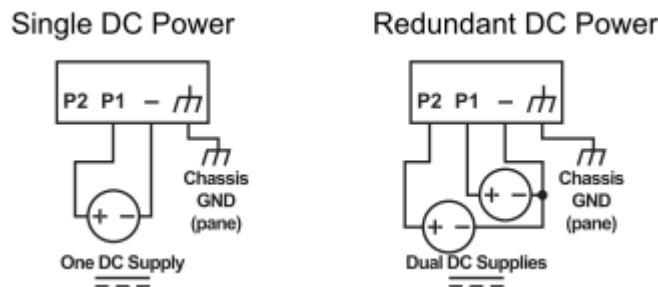


Figure 1-15. Power Wiring for Unmanaged Switches

1.9.2 Considerations


Take into consideration the following guidelines before wiring the device:


- Screws should not be overly tightened, max. torque value: 5 lb-in [0.57 Nm].
- Wire sizes: between 24 AWG and 12 AWG.
- Turn off the power to the switch.
- Calculate the maximum possible current for each power and common wire. Make sure the power draw is within limits of local electrical code regulations.
- For best practices, route wiring for power and devices on separate paths.
- Do not bundle together wiring with similar electrical characteristics.
- Make sure to separate input and output wiring.
- Label all wiring and cabling to the various devices for more effective management and servicing.
- Unscrew and remove the terminal block to prevent a short circuit to the device.





Routing communications and power wiring through the same conduit may cause signal interference. To avoid interference and signal degradation, route power and communications wires through separate conduits.


1.9.3 Grounding the Device

 Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch device.

 Before connecting the device properly ground the device. Lack of a proper grounding setup may result in a safety risk and could be hazardous.

 Do not service equipment or cables during periods of lightning activity.

 Do not service any components unless qualified and authorized to do so.

 Do not block air ventilation holes.

Electromagnetic Interference (EMI) affects the transmission performance of a device. By properly grounding the device to earth ground through a drain wire, you can setup the best possible noise immunity and emissions.

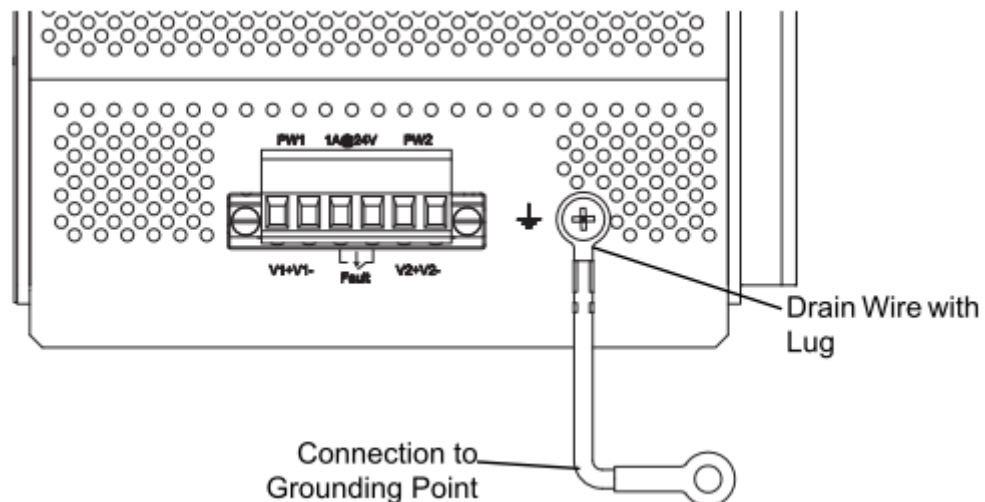



Figure 1-16. Grounding Connection

By connecting the ground terminal by drain wire to earth ground the switch and chassis can be ground.

 *Before applying power to the grounded switch, it is advisable to use a volt meter to ensure there is no voltage difference between the power supply's negative output terminal and the grounding point on the switch.*

1.9.4 Wiring a Relay Contact

The following section details the wiring of the relay output. The terminal block on the EKI-9316P / EKI-9312P is wired and then installed onto the terminal receptor located on the EKI-9316P / EKI-9312P.

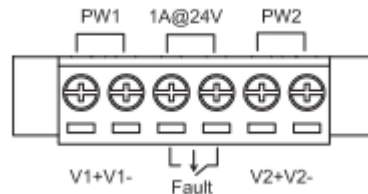


Figure 1-17. Terminal Receptor: Relay Contact

The terminal receptor includes a total of six pins: two for PWR1, two for PWR2 and two for a Fault circuit.

The fault circuit is designed for triggering alarm outputs. In normal conditions the output is on and does not trigger an event. When the condition changes the output is turned off and the alarm condition is triggered.

Alarm conditions can be setup for the following:

- Authentication failure
- X-Ring Pro failure
- Port link state change
- Firmware upgrade or failure
- PoE state change or overload

For further details about setting up an event policy see Event Policy Configuration on page 64.

1.9.5 Wiring the Power Inputs



Do not disconnect modules or cabling unless the power is first switched off. The device only supports the voltage outlined in the type plate. Do not use any other power components except those specifically designated for the switch device.



POWER DOWN AND DISCONNECT THE POWER CORD BEFORE SERVICING OR WIRING THE SWITCH.

There are two power inputs for normal and redundant power configurations. The power input 2 is used for wiring a redundant power configuration. See the following for terminal block connector views.

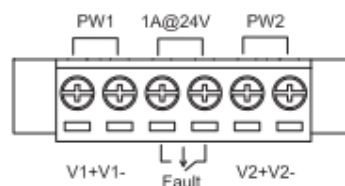


Figure 1-18. Terminal Receptor: Power Input Contacts

To wire the power inputs:

Make sure the power is not connected to the switch or the power converter before proceeding.

1. Loosen the screws securing terminal block to the terminal block receptor.
2. Remove the terminal block from the switch.

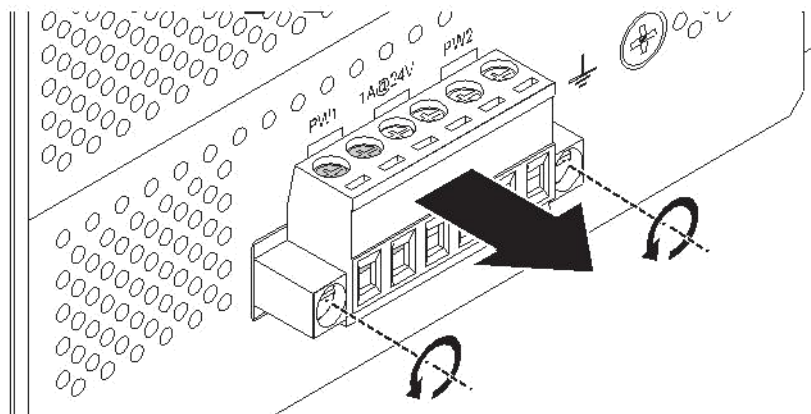


Figure 1-19. Removing a Terminal Block

3. Insert a small flat-bladed screwdriver in the V1+/V1- wire-clamp screws, and loosen the screws.
4. Insert the negative/positive DC wires into the V+/V- terminals of PW1. If setting up power redundancy, connect PW2 in the same manner.

5. Tighten the wire-clamp screws to secure the DC wires in place.

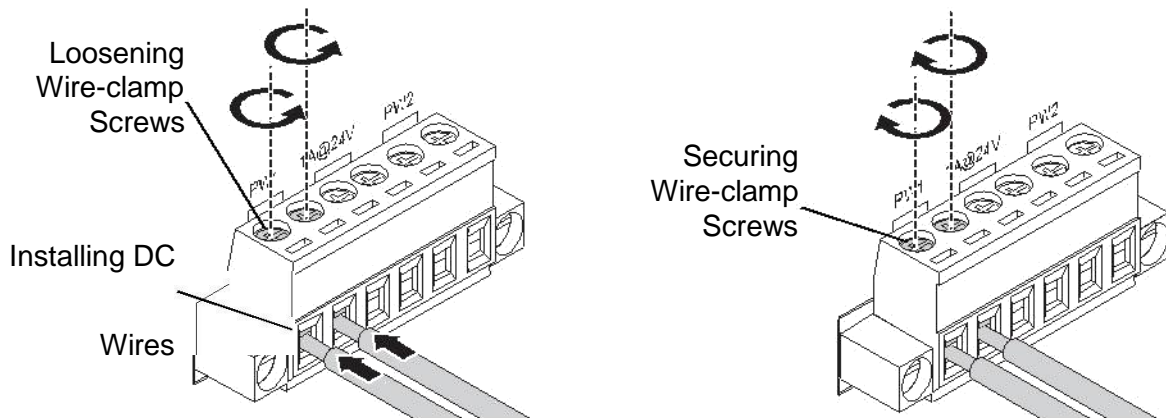


Figure 1-20. Installing DC Wires in a Terminal Block

6. Align the terminal block over the terminal block receptor on the switch.
7. Insert the terminal block and press it in until it is flush with the terminal block receptor.
8. Tighten the screws on the terminal block to secure it to the terminal block receptor. If there is no gap between the terminal block and the terminal receptor, the terminal block is seated correctly.

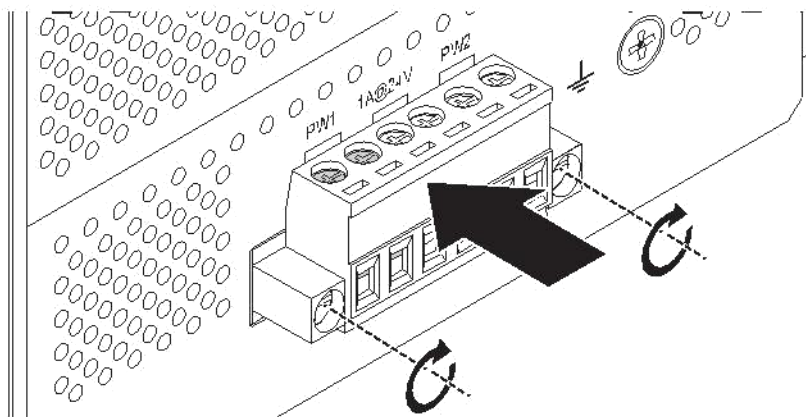


Figure 1-21. Securing a Terminal Block to a Receptor

1.9.6 Wiring the Digital Inputs

The EKI series has one set of digital input (DI). The DI consists of two contacts of the 6-pin terminal block connector on the switch's bottom panel, which are used for the two DC inputs. The top and front views of one of the terminal block connectors are shown as follows.

1. Insert the negative (ground)/positive DI wires into the V1- and Ground terminals.
2. Use a small flat-blade screwdriver to tighten the wire-clamp screws.
3. Insert the plastic terminal block connector prongs into the terminal block receptor, which is located on the bottom panel of the device.

1.10. Communication Port Wiring

The EKI-9316P / EKI-9312P are industrial Ethernet switches provide connections to standard Ethernet devices. There are three types of communication ports the switches: RJ45 Ethernet ports, fiber optic Ethernet ports, and a USB console port for management options.

1.10.1 RJ45 Ethernet Cable Wiring

For RJ45 connectors, data-quality, twisted pair cabling (rated CAT5 or better) is recommended. The connector bodies on the RJ45 Ethernet ports are metallic and connected to the GND terminal. For best performance, use shielded cabling. Shielded cabling may be used to provide further protection.

Table 1-8. RJ45 Ethernet Wiring for Reference

Straight-thru Cable Wiring		Cross-over Cable Wiring	
Pin 1	Pin 1	Pin 1	Pin 3
Pin 2	Pin 2	Pin 2	Pin 6
Pin 3	Pin 3	Pin 3	Pin 1
Pin 6	Pin 6	Pin 6	Pin 2

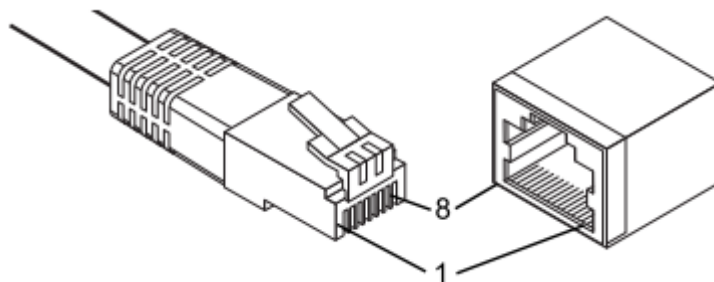


Figure 1-22. Ethernet Plug & Connector Pin Position

Maximum cable length: 100 meters (328 ft.) for 10/100/1000BaseT.

1.10.2 Mini-GBIC Fiber Transceivers

Up to four fiber optic ports are available (dependent on model) for use in the switch. Refer to the technical specifications for details.

The Gigabit Ethernet ports on the switch are 100/1000BaseSFP Fiber ports, which require using the 100M or 1G mini-GBIC fiber transceivers to work properly. Advantech provides completed transceiver models for different distance requirement.

The concept behind the LC port and cable is quite straightforward. Suppose that you are connecting devices I and II; contrary to electrical signals, optical signals do not require a circuit in order to transmit data. Consequently, one of the optical lines is used to transmit data from device I to device II, and the other optical line is used transmit data from device II to device I, for full-duplex transmission.

Remember to connect the Tx (transmit) port of device I to the Rx (receive) port of device II, and the Rx (receive) port of device I to the Tx (transmit) port of device II. If you make your own cable, we suggest labeling the two sides of the same line with the same letter (A-to-A and B-to-B, as shown below, or A1-to-A2 and B1-to-B2).



This is a Class 1 Laser/LED product. To avoid causing serious damage to your eyes, do not stare directly into the Laser Beam.

Installing a Transceiver

To connect the fiber transceiver and LC cable, use the following guidelines:

1. Remove the dust plug from the fiber optic slot chosen for the SFP transceiver.

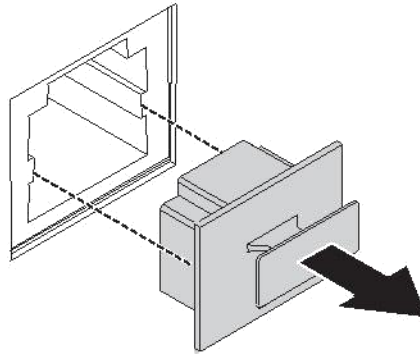


Figure 1-23. Removing the Dust Plug from an SFP Slot



Do not remove the dust plug from the SFP slot if you are not installing the transceiver at this time. The dust plug protects hardware from dust contamination.

2. Position the SFP transceiver with the handle on top, see the following figure.
3. Locate the triangular marking in the slot and align it with the bottom of the transceiver.
4. Insert the SFP transceiver into the slot until it clicks into place.

5. Make sure the module is seated correctly before sliding the module into the slot. A click sounds when it is locked in place.

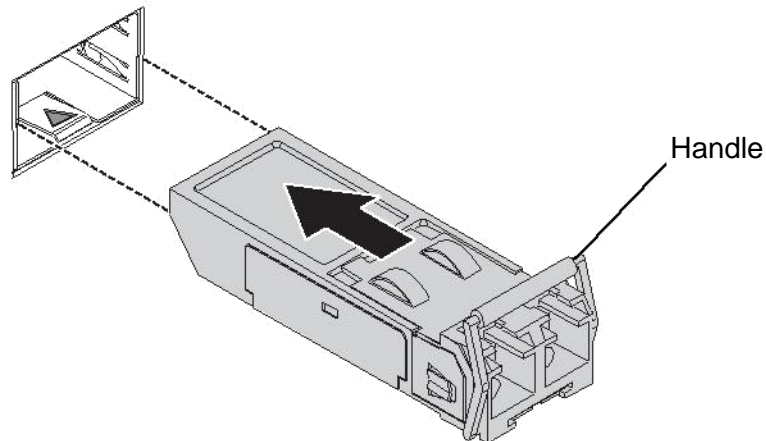


Figure 1-24. Installing an SFP Transceiver



If you are attaching fiber optic cables to the transceiver, continue with the following step. Otherwise, repeat the previous steps to install the remaining SFP transceivers in the device.

6. Remove the protective plug from the SFP transceiver.



Do not remove the dust plug from the transceiver if you are not installing the fiber optic cable at this time. The dust plug protects hardware from dust contamination.

7. Insert the fiber cable into the transceiver. The connector snaps into place and locks.

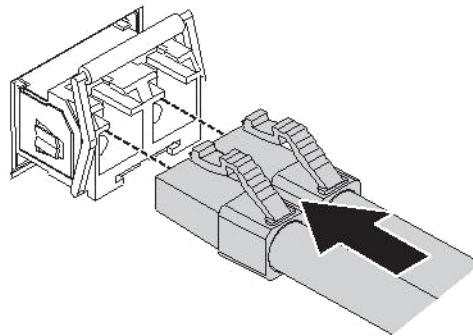


Figure 1-25. Attaching a Fiber Optic Cable to a Transceiver

8. Repeat the previous procedures to install any additional SFP transceivers in the switch. The fiber port is now setup.

Removing an Transceiver

To disconnect an LC connector, use the following guidelines:

1. Press down and hold the locking clips on the upper side of the optic cable.
2. Pull the optic cable out to release it from the transceiver.

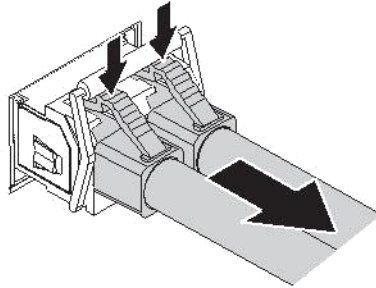


Figure 1-26. Removing a Fiber Optic Cable to a Transceiver

3. Hold the handle on the transceiver and pull the transceiver out of the slot.

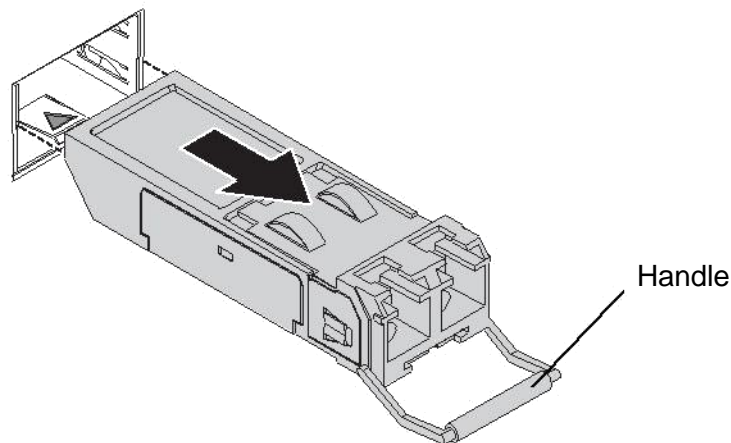


Figure 1-27. Removing an SFP Transceiver



Replace the dust plug on the slot if you are not installing a transceiver. The dust plug protects hardware from dust contamination.

1.10.3 Network Device Validation

Advantech industrial Ethernet switches support 10/100BaseT or 10/100/1000BaseT on the RJ45 (copper) ports and 100BaseFX or gigabit Ethernet on the fiber optic ports. Make sure the devices are connected to the corresponding ports for proper operation.

1.10.4 Validating Connectivity

It is important to ensure all devices are connected correctly to the switch. Once all Ethernet and fiber cabling is connected, inspect the LED corresponding to connected cable. The LED displays a solid or blinking light. Any LED that is off signifies a connectivity issue. Inspect the port connection and the associated networked device. For further LED information see System LED Panel on page 12 and Activity and PoE LED Panel on page 13.

1.10.5 Serial Console Port Wiring

The industrial switch supports a secondary means of management. By connecting the RJ45 to RS232 serial cable between a COM port on your PC (9-pin D-sub female) and the switch's RJ45 (RJ45) port, a wired connection for management can be established.

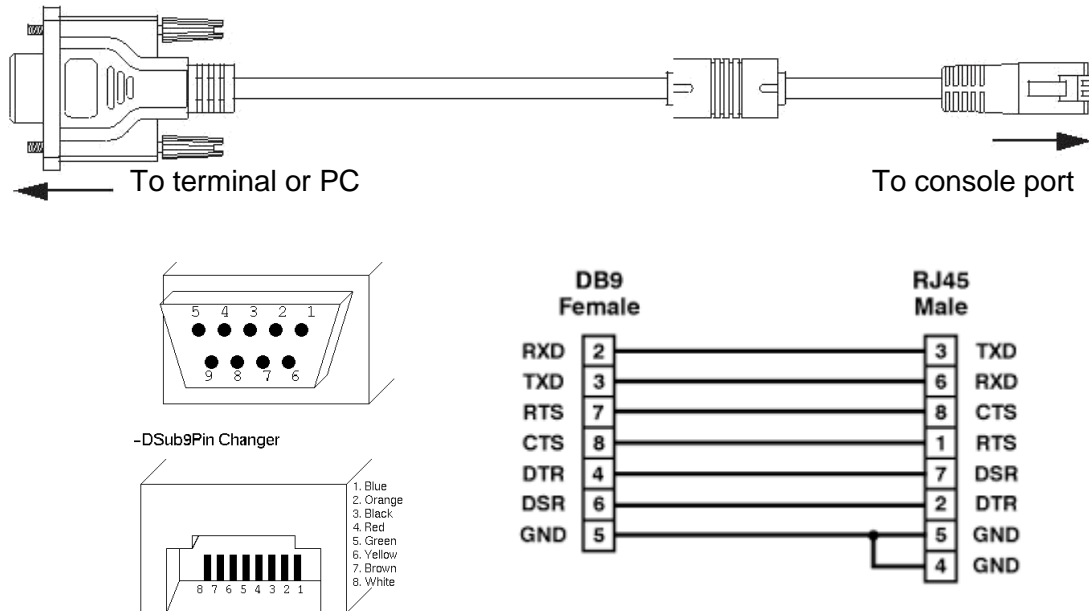


Figure 1-28. Serial Console Cable

1.10.6 USB Console Port Wiring

In addition to the serial console option, the industrial switch supports a USB port for management. A standard A-type-USB cable is used to connect the switch. Connect the USB cable to the USB port on the PC and the switch.

USB Storage Port

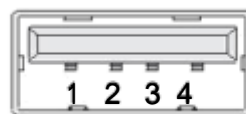


Figure 1-29.

Table 1-9. USB Port

PIN	Description
1	VCC (+5V)
2	D- (Data -)
3	D+ (Data+)
4	GND (Ground)

1.11. Reset Button

Reset configuration to factory default:

Press and hold Reset button for 2 seconds.

System reboot:

Press and hold Reset button for 5 seconds.



Do NOT power off the Ethernet switch when loading default settings.

First Time Setup

Chapter 2

2.1. First Time Setup

2.1.1 Overview

The Industrial Ethernet Managed Switch is a configurable device that facilitates the interconnection of Ethernet devices on an Ethernet network. This includes computers, operator interfaces, I/O, controllers, RTUs, PLCs, other switches/hubs or any device that supports the standard IEEE 802.3 protocol.

This switch has all the capabilities of a store and forward Ethernet switch plus advanced management features such as SNMP, RSTP and port mirroring. This manual details how to configure the various management parameters in this easy to use switch.

2.1.2 Introduction

To take full advantage of all the features and resources available from the switch, it must be configured for your network.

The switch implements Rapid Spanning Tree Protocol (RSTP) and Simple Network Management Protocol (SNMP) to provide most of the services offered by the switch. Rapid Spanning Tree Protocol allows managed switches to communicate with each other to ensure that there exists only one active route between each pair of network nodes and provides automatic failover to the next available redundant route. A brief explanation of how RSTP works is given in the Spanning Tree section.

The switch is capable of communicating with other SNMP capable devices on the network to exchange management information. This statistical/derived information from the network is saved in the Management Information Base (MIB) of the switch. The MIB is divided into several different information storage groups. These groups will be elaborated in detail in the Management and SNMP information section of this document. The switch implements Internet Group Management Protocol (IGMP) to optimize the flow of multicast traffic on your network.

The switch supports both port-based and tag-based Virtual LANs for flexible integration with VLAN-aware networks with support for VLAN-unaware devices.

2.1.3 Administrative Interface Access

There are several administrative interfaces to the switch:

1. A graphical web interface accessible via the switch's built-in web server. Both http and secure https with SSL are supported.



This is the recommended method for managing the switch.

2. A terminal interface via the RS232/USB port or over the network using telnet or Secure Shell (SSH).
3. An SNMP interface can be used to read/write many settings.
4. Command Line Interface (CLI) can be used to read/write most settings. Initial setup must be done using an Ethernet connection (recommended) or the serial port.

2.1.4 Using the Graphical (Web) Interface

The graphical interface is provided via a web server in the switch and can be accessed via a web browser such as Opera, Mozilla, or Internet Explorer.



JavaScript must be supported and enabled in your browser for the graphical interface to work correctly.

HTTP and HTTPS (secure HTTP) are supported for access to the web server. By default, both protocols are enabled. Either or both may be disabled to secure the switch. (See the Remote Access Security topic in this section.)

To access the graphical interface, enter a URL like HTTP://192.168.1.1 in your browser's address bar. Replace “http” with “https” to use secure http and replace “192.168.1.1” with your switch's IP address if you've changed it from the factory default.

The web server in the switch uses a signed security certificate. When you access the server via https, you may see a warning dialog indicating that the certificate was signed by an unknown authority. This is expected and to avoid this message in the future you can choose to install the certificate on your computer.



This manual describes and depicts the web user interface in detail. The terminal interface is not specifically shown but is basically the same.

2.1.5 Configuring the Switch for Network Access

To control and monitor the switch via the network, it must be configured with basic network settings, including an IP address and subnet mask. Refer to the quick start guide in Section 1 for how to initially access your switch.

To configure the switch for network access, select [Add Menu Address Here] to reach the System Settings menu. The settings in this menu control the switch's general network configuration.

- DHCP Enabled/Disabled: The switch can automatically obtain an IP address from a server using the Dynamic Host Configuration Protocol (DHCP). This can speed up initial set up, as the network administrator does not have to find an open IP address.
- IP Address and subnet mask configuration: The IP address for the switch can be changed to a user-defined address along with a customized subnet mask to separate subnets.



Advanced users can set the IP address to 0.0.0.0 to disable the use of an IP address for additional security. However, any features requiring an IP address (i.e., web interface, etc.) will no longer be available.

- Default Gateway Selection: A Gateway Address is chosen to be the address of a router that connects two different networks. This can be an IP address or a Fully Qualified Domain Name (FQDN) such as “domainname.org”.

- NTP Server: The IP address or domain name of an NTP (Network Time Protocol) server from which the switch may retrieve the current time at startup. Please note that using a domain name requires that at least one domain name server be configured.

2.1.6 Configuring the Ethernet Ports

The switch comes with default port settings that should allow you to connect to the Ethernet Ports without any necessary configuration. Should there be a need to change the name of the ports, negotiation settings or flow control settings, you can do this in the Port Configuration menu. Access this menu by selecting Setup from the Main menu, and then selecting Main Settings.

- Port Name: Each port in the managed switch can be identified with a custom name. Specify a name for each port here.
- Admin: Ports can be enabled or disabled in the managed switch. For ports that are disabled, they are virtually non-existent (not visible in terms of switch operation or spanning tree algorithm). Choose to enable or disable a port by selecting Enabled or Disabled, respectively.
- Negotiation: All copper ports and gigabit fiber ports in the managed switch are capable of auto-negotiation such that the fastest bandwidth is selected. Choose to enable auto-negotiation or use fixed settings. 100Mbps Fiber ports are Fixed speed only.
- Speed/Duplex/Flow Control: The managed switch accepts three local area network Ethernet Standards. The first standard, 10BASE-T, runs 10Mbps with twisted pair Ethernet cable between network interfaces. The second local area network standard is 100BASE-T, which runs at 100Mbps over the same twisted pair Ethernet cable. Lastly, there is 100BASE-F, which enables fast Ethernet (100Mbps) over fiber.

These options are available:

- 10h–10 Mbps, Half Duplex
- 10f –10 Mbps, Full Duplex
- 100h–100 Mbps, Half Duplex
- 100f –100 Mbps, Full Duplex
- 1000f–1000 Mbps, Full Duplex

On managed switches with gigabit combination ports, those ports will have two rows, a standard row of check boxes and a row labeled “SFP” with radio buttons. The SFP setting independently sets the speed at which a transceiver will operate if one is plugged in. Other-wise, the switch will use the fixed Ethernet port and the corresponding settings for it.



When 100f is selected for the SFP of a gigabit combination port, the corresponding fixed Ethernet jack will be disabled unless it is changed back to 1000F.

2.2. Web Browser Configuration

The switch has an HTML based user interface embedded in the flash memory. The interface offers an easy to use means to manage basic and advanced switch functions. The interface allows for local or remote switch configuration anywhere on the network.

The interface is designed for use with [Internet Explorer (6.0), Chrome, Firefox].

2.2.1 Preparing for Web Configuration

The interface requires the installation and connection of the switch to the existing network. A PC also connected to the network is required to connect to the switch and access the interface through a web browser. The required networking information is provided as follows:

- IP address: 192.168.1.1
- Subnet mask: 255.255.255.0
- Default gateway: 0.0.0.0
- User name: admin
- Password: admin

2.2.2 System Login

Once the switch is installed and connected, power on the switch. The following information guides you through the logging in process.

1. Launch your web browser on the PC.
2. In the browser's address bar, type the switch's default IP address (192.168.1.1).
The login screen displays.
3. Enter the user default name and password (admin / admin).
4. Click **OK** on the login screen to log in.
The main interface displays.

Management Interface

Chapter 3

3.1. Log In

To access the log in window, connect the device to the network, see “Communication Port Wiring” on page 25 and open a browser window.

Enter the default user name and password (admin/admin) to log into the management interface. You can change the default password after you have successfully logged in.



Figure 3-1. Login Screen

3.2. Recommended Practices

3.2.1 Changing Default Password

In keeping with good management and security practices, it is recommended that you change the default password as soon as the device is functioning and setup correctly. The following details the necessary steps to change the default password.

To change the password:

1. Navigate to **Management > Local Password Management > User Accounts**.
2. From the User drop-down menu, select the admin (default) account.
3. In the User Name field, enter a new user name for this account. It is not necessary to change the user name, however, a change in the default settings increases the security settings.
4. In the password field, type in the new password. Re-type the same password in the Confirm Password field.

5. Click **Submit** to change the current account settings.

User Accounts Configuration

User	admin ▾
User Name	admin (1 to 32 alphanumeric characters)
Password	(8 to 64 Characters)
Confirm Password	(8 to 64 Characters)
Access Level	Read-Write ▾
Lockout Status	False
Password Override-Complexity-Check	Disable ▾
Password Expiration Date	

SNMP v3 User Configuration

SNMP v3 Access Mode	Read-Write ▾
Authentication Protocol	None ▾
Configure Encryption	<input type="checkbox"/>
Encryption Protocol	None ▾
Encryption Key	(8 to 64 characters)

Submit Delete

Figure 3-2. Changing Default Password

After saving all the desired settings, perform a system save (**Maintenance > Config Save**). The changes are saved and retained even after a reboot.

3.3. Management

3.3.1 System Information

The System Information page displays information about the switch and network settings. To access this page, click **Management > System Information**.

System Information

System Description	Industrial Managed 16-port Full Gigabit PoE/PoE+ Switch, v1.0.0, Linux 2.6.34.10																																			
Machine Type	Industrial Managed 16-port Full Gigabit PoE/PoE+ Switch																																			
Machine Model	EKI-7756FP																																			
Serial Number	AKS0073027																																			
Manufacturer	Advan Tech																																			
Burned In MAC Address	0C:00:C9:75:15:FF																																			
Number Of MAC Address	0																																			
Software Version	v1.0.0																																			
Build Version	k7.C0.27																																			
Build Time	Wed Apr 22 11:09:09 CST 2014																																			
Operating System	Linux 2.6.34.10																																			
Hardware Monitor	<p>Hardware Status: Normal Last Update: 1939-Jul-30, 01:45:48</p> <table border="1"> <thead> <tr> <th>Temperature (C)</th> <th>Last</th> <th>Average</th> <th>Minimum</th> <th>Maximum</th> </tr> </thead> <tbody> <tr> <td>CPU</td> <td>33.125</td> <td>33.069</td> <td>27.813</td> <td>33.125</td> </tr> <tr> <td>SWITCH</td> <td>38.188</td> <td>38.128</td> <td>29.750</td> <td>38.188</td> </tr> <tr> <td>PHY1</td> <td>41.938</td> <td>41.889</td> <td>34.563</td> <td>42.000</td> </tr> <tr> <td>PHY2</td> <td>44.563</td> <td>44.514</td> <td>35.100</td> <td>44.563</td> </tr> <tr> <td>Sys Power</td> <td>38.688</td> <td>38.591</td> <td>29.563</td> <td>38.688</td> </tr> <tr> <td>PrF_Power</td> <td>36.625</td> <td>36.711</td> <td>29.313</td> <td>38.313</td> </tr> </tbody> </table>	Temperature (C)	Last	Average	Minimum	Maximum	CPU	33.125	33.069	27.813	33.125	SWITCH	38.188	38.128	29.750	38.188	PHY1	41.938	41.889	34.563	42.000	PHY2	44.563	44.514	35.100	44.563	Sys Power	38.688	38.591	29.563	38.688	PrF_Power	36.625	36.711	29.313	38.313
Temperature (C)	Last	Average	Minimum	Maximum																																
CPU	33.125	33.069	27.813	33.125																																
SWITCH	38.188	38.128	29.750	38.188																																
PHY1	41.938	41.889	34.563	42.000																																
PHY2	44.563	44.514	35.100	44.563																																
Sys Power	38.688	38.591	29.563	38.688																																
PrF_Power	36.625	36.711	29.313	38.313																																

Refresh

Figure 3-3. Management > System Information

The following table describes the items in the previous menu.

Table 3-1. Management > System Information

Item	Description
System Description	Displays the product name of the switch.
Machine Type	Displays the machine type of the switch.
Machine Model	Displays the model name of the switch.
Serial Number	Displays the serial number of the switch.
Manufacturer	Displays the manufacturer of the switch.
Burned In MAC Address	Displays the burned-in universally administered MAC address of the switch.
Number Of MAC Address	Displays number of burned-in universally administered MAC address of the switch.
Software Version	Displays the software version as follows: release, version, and maintenance number.
Build Version	Displays the build version of the switch.
Build Time	Displays the build time of the switch.
Operating System	Displays the operating system currently running of the switch.
Hardware Monitor	Displays the hardware status of the switch.
Refresh	Click Refresh to update the screen.

3.3.2 System Description

The System Description page displays basic information about the system. To access this page, click **Management > System Description**.

System Description

Industrial Managed 16-port Full Gigabit PoE/PoE+ Switch, v1.0.0, Linux 2.6.34.10

System Name	<input type="text" value="EKI-7756FHPI"/> (0 to 255 alphanumeric characters)
System Location	<input type="text"/> (0 to 255 alphanumeric characters)
System Contact	<input type="text"/> (0 to 255 alphanumeric characters)
IP Address	192.168.1.1
System Object ID	1.3.6.1.4.1.10297.2.6.7756
System Up Time	0 days, 0 hours, 11 mins 45 secs
Current SNTP Synchronized Time	Not Synchronized

Figure 3-4. Management > System Description

The following table describes the items in the previous menu.

Table 3-2. Management > System Description

Item	Description
System Description	Displays the product name of the switch.
System Name	Enter the system name: up to 255 alphanumeric characters. The default is blank.
System Location	Enter the location: up to 255 alphanumeric characters. The default is blank.
System Contact	Enter the contact person: up to 255 alphanumeric characters. The default is blank.
IP Address	Displays the assigned IP address of the switch.
System Object ID	Displays the base object ID of the switch.
System Up Time	Displays the time since the last switch reboot.
Current SNTP Synchronized Time	Displays currently synchronized SNTP time in UTC.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

3.3.3 IP Configuration

The network interface is the logical interface used for in-band connectivity with the switch via any of the front panel ports of the switch. To access the switch over a network, users must first configure the IP address, subnet mask, and default gateway. To access this page, click **Management > IP Configuration**.

Network Connectivity Configuration

Interface Status Up

IPv4

Network Configuration Protocol None ▾

IP Address

Subnet Mask

Default Gateway

Burned In MAC Address 00:D0:C9:75:16:FF

Management VLAN ID

Figure 3-5. Management > IP Configuration

The following table describes the items in the previous menu.

Table 3-3. Management > IP Configuration

Item	Description
Interface Status	Displays the link status.
IPv4	
Network Configuration Protocol	Click the drop-down menu to specify a protocol after power-up. The default is None.
IP Address	Enter a value to specify the IP address of the interface. The default is 192.168.1.1
Subnet Mask	Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
Default Gateway	Enter a value to specify the default gateway for the IP interface. The default is 0.0.0.0
Burned In MAC Address	Displays the burned in MAC address of the switch.
Management VLAN ID	Enter a value (between 1 to 4093) to specify a management VLAN ID of the switch. The default is 1. And it's only available for administrator.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Renew DHCP IPv4 Address	Click Renew DHCP IPv4 Address to renew a IPv4 address from DHCP server.

3.3.4 AAA

Authentication Configuration

The Authentication Configuration allows users to configure authentication lists. To access this page, click **Management > AAA > Authentication Configuration**.

Authentication List Configuration

Access Mode Login ▾

Authentication List default_list ▾

Method 1 LOCAL ▾

Method 2 Undefined ▾ (Previous methods must be configured before this one)

Method 3 Undefined ▾ (Previous methods must be configured before this one)

Method 4 Undefined ▾ (Previous methods must be configured before this one)

Method 5 Undefined ▾ (Previous methods must be configured before this one)

Delete Submit

Figure 3-6. Management > AAA > Authentication Configuration

The following table describes the items in the previous menu.

Table 3-4. Management > AAA > Authentication Configuration

Parameter	Description
Access Mode	Click the drop-down menu to specify login list or enable list. The default is default-List for all newly created user.
Authentication List	Click the drop-down menu to select the authentication list. Select "Create" to define a new list and the default is undefined.
Authentication List Name	Enter the list name (up to 12 characters) to create a new list.
Method 1	Click the drop-down menu to select the authentication method order. The first method has first priority. If the method times out, the following method is selected. The method options are: <ul style="list-style-type: none"> • Undefined - the authentication method is unspecified (this may not be assigned as the first method) • Enable - uses the enable password for authentication • Line - uses the Line password for authentication • Local - the user's locally stored ID and password are used for authentication. This method is only visible and applicable for login authentication method. • None - no authentication is used • Radius - the user's ID and password will be authenticated using the RADIUS server instead of locally • Deny - the user gets rejected to get access to the privileged mode. This method is only visible and applicable for enable authentication method • Tacacs+ - the user's ID and password will be authenticated using the TACACS+ server
Method 2	Click the drop-down menu to select the authentication method order.
Method 3	Click the drop-down menu to select the authentication method order.
Method 4	Click the drop-down menu to select the authentication method order.
Method 5	Click the drop-down menu to select the authentication method order.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected authentication list. If the selected list is assigned to any user, the Delete process will fail. To save the values across a power cycle perform a system save.

Authentication Status

The Authentication Status page displays a summary of the Login Authentication List, Enable Authentication List, and Login and Enable Method Lists for Console, Telnet, and SSH.

To access this page, click **Management > AAA > Authentication Status**.

Authentication List Summary

Login Authentication List	Login Method List	Remove
defaultList:	LOCAL	<input type="checkbox"/>
networkList	LOCAL	<input type="checkbox"/>

Enable Authentication List	Enable Method List	Remove
enableList	ENABLE,NONE	<input type="checkbox"/>

Console	
Login Method List	defaultList
Enable Method List	enableList

Telnet	
Login Method List	networkList
Enable Method List	enableList

SSH	
Login Method List	networkList
Enable Method List	enableList

HTTPS	Local
HTTP	Local
SSH	Local

Figure 3-7. Management > AAA > Authentication Status

The following table describes the items in the previous menu.

Table 3-5. Management > AAA > Authentication Status

Parameter	Description
Authentication List	Displays all the authentication profiles.
Method List	<p>Displays all the authentication methods.</p> <p>The method options are:</p> <ul style="list-style-type: none"> • 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. This method is only visible and applicable for login authentication method. • 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. • Deny - the user gets rejected to get access to the privileged mode. This method is only visible and applicable for enable authentication method.

Table 3-5. Management > AAA > Authentication Status (Continued)

Parameter	Description
Remove	<ol style="list-style-type: none"> 1. Select the authentication profile to remove. 2. Click Submit to remove the profile.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Refresh	Click Refresh to update the screen.



The same fields are displayed in case of **Enable Authentication List Table**.



The Authentication Lists and Authentication Methods configured for each List of **Console, Telnet, SSH, HTTPS, HTTP and DOT1X** are displayed respectively.

Authentication Preference

The Authentication Preference page allows users to configure the Login and Enable lists for the console, telnet, and SSH. Users can also assign an authentication method for Secure HTTP, HTTP, and Dot1x. To access this page, click **Management > AAA > Authentication Preference**.

Select Authentication List

Console			
Login	defaultList ▼	Enable	enableList: ▼
Telnet			
Login	networkList ▼	Enable	enableList: ▼
SSH			
Login	networkList ▼	Enable	enableList: ▼
Secure HTTP			
Method 1	LOCAL ▼		
Method 2	Undefined ▼	(Previous methods must be configured before this one)	
Method 3	Undefined ▼	(Previous methods must be configured before this one)	
Method 4	Undefined ▼	(Previous methods must be configured before this one)	
HTTP			
Method 1	LOCAL ▼		
Method 2	Undefined ▼	(Previous methods must be configured before this one)	
Method 3	Undefined ▼	(Previous methods must be configured before this one)	
Method 4	Undefined ▼	(Previous methods must be configured before this one)	
Dot1x			
Method	Undefined ▼		

Submit

Figure 3-8. Management > AAA > Authentication Preference

The following table describes the items in the previous menu.

Table 3-6. Management > AAA > Authentication Preference

Parameter	Description
Console	Click the drop-down menu to verify console users' profiles. <ul style="list-style-type: none"> • Login or Enable - Specify the login list and enable list which will be used to validate switch or port access for the users associated with the list.
Telnet	Click the drop-down menu to verify Telnet users' profiles. <ul style="list-style-type: none"> • Login or Enable - Specify the login list and enable list which will be used to validate switch or port access for the users associated with the list.
Secure Telnet (SSH)	Click the drop-down menu to verify Secure Shell (SSH) users profiles. <ul style="list-style-type: none"> • Login or Enable - Specify the login list and enable list which will be used to validate switch or port access for the users associated with the list.
HTTP and Secure HTTP	Click the drop-down menu to select an authentication method for HTTP access and secure HTTP access. <ul style="list-style-type: none"> • Method 1 -Click the drop-down menu to select the authentication method order. The first method has first priority. If the method times out, the following method is selected. The method options are: <ul style="list-style-type: none"> • Undefined - the authentication method is disabled (this may not be assigned as the first method). • 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. • Method 2 - Click the drop-down menu to select the authentication method order. • Method 3 - Click the drop-down menu to select the authentication method order. • Method 4 - Click the drop-down menu to select the authentication method order.

Table 3-6. Management > AAA > Authentication Preference (Continued)

Parameter	Description
Dot1x	<p>Click the drop-down menu to select an authentication method to verify the Dof1x access.</p> <ul style="list-style-type: none"> Method - Click the drop-down menu to select a method. The method options are: <ul style="list-style-type: none"> Undefined - the authentication method is disabled. IAS - the user's ID and password in Internal Authentication Server Database will be used 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.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

Accounting Configuration

Accounting Configuration allows the users to record information about clients who were successfully authenticated and allowed access to the network. To access this page, click **Management > AAA > Accounting Configuration**.

Accounting List Configuration

The screenshot shows the 'Accounting List Configuration' page. It contains the following fields and options:

- Accounting Type:** EXEC
- Accounting List:** dfltExecList
- Record Type:** STARTSTOP
- Method 1:** Tacacs+
- Method 2:** Undefined (Previous methods must be configured before this one)

Buttons: Delete, Submit

Figure 3-9. Management > AAA > Accounting Configuration

The following table describes the items in the previous menu.

Table 3-7. Management > AAA > Accounting Configuration

Parameter	Description
Accounting Type	<p>Click the drop-down menu to select an accounting type.</p> <ul style="list-style-type: none"> EXEC - Account login and logout time for a user session. COMMANDS - Account executed commands for a user.
Accounting List	Click the drop-down menu to select an accounting list you want to configure. Select "Create" to define a new list and the default is undefined.
Accounting List Name	Enter the accounting list name: up to 12 characters.

Table 3-7. Management > AAA > Accounting Configuration (Continued)

Parameter	Description
Record Type	Click the drop-down menu to select a record type. <ul style="list-style-type: none"> StartStop - Account when the start and end of an user session or executed commands. StopOnly - Account when the end of an user session or executed commands.
Method 1	Click the drop-down menu to select a method. The method options are: <ul style="list-style-type: none"> Undefined - the accounting method is unspecified (this cannot be assigned as a method). RADIUS - Accounting messages will be sent to a RADIUS server. Tacacs+ - Accounting messages will be sent to a Tacacs+ server.
Method 2	Click the drop-down menu to select the authentication method order.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected accounting list. If the selected list is assigned to any line, the Delete process will fail. You can use this button only when you have Read/Write access. To save the values across a power cycle perform a system save.

Accounting Status

The Accounting Status page displays the summary of the current method list selected for the switch. To access this page, click **Management > AAA > Accounting Status**.

Accounting List Summary

Exec Accounting List	Exec Method List	Remove
dfltExecList	TACACS+	<input type="checkbox"/>
Commands Accounting List	Commands Method List	Remove
dfltCmdList	TACACS+	<input type="checkbox"/>
Console		
Exec Method List	None	
Commands Method List	None	
Telnet		
Exec Method List	None	
Commands Method List	None	
SSH		
Exec Method List	None	
Commands Method List	None	

Submit Refresh

Figure 3-10. Management > AAA > Accounting Status

The following table describes the items in the previous menu.

Table 3-8. Management > AAA > Accounting Status

Parameter	Description
Accounting List	Displays the all accounting profiles.
Methods List	Displays the accounting methods. <ul style="list-style-type: none"> Radius - RADIUS is used to account user exec sessions and user executed commands. TACACS+ - TACACS+ is used to account user exec sessions and user executed commands.
Remove	Check the checkbox to remove the accounting profile.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Refresh	Click Refresh to update the screen.



The same fields are displayed in case of **Commands Accounting List Table**.



The Exec and Command Accounting Method Lists configured for each List of **Con-sole, Telnet and SSH** are displayed respectively.

Accounting Preference

The Accounting Preference page allows users to configure the console, telnet, and SSH commands. To access this page, click **Management > AAA > Accounting Preference**.

Select Accounting List

Console	
Exec <input type="text" value="None"/>	Commands <input type="text" value="None"/>
Telnet	
Exec <input type="text" value="None"/>	Commands <input type="text" value="None"/>
SSH	
Exec <input type="text" value="None"/>	Commands <input type="text" value="None"/>
<input type="button" value="Submit"/>	

Figure 3-11. Management > AAA > Accounting Preference

The following table describes the items in the previous menu.

Table 3-9. Management > AAA > Accounting Preference

Parameter	Description
Console	Click the drop-down menu to specify the profile. Accounting profiles used to account console users activity. <ul style="list-style-type: none"> Exec or Commands - Specify the Exec list and Commands list which will be used to account for user activity associated with the list.
Telnet	Click the drop-down menu to specify the profile. Accounting profiles used to account Telnet users. <ul style="list-style-type: none"> Exec or Commands - Specify the Exec list and Commands list which will be used to account for user activity associated with the list.
Secure Telnet (SSH)	Click the drop-down menu to specify the profile. Accounting profiles used to account SSH users. <ul style="list-style-type: none"> Exec or Commands - Specify the Exec list and Commands list which will be used to account for user activity associated with the list.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

3.3.5 Local Password Management

User Accounts

The User Accounts Configuration page allows users to personalize accounts, set up a new user name and password, access level, and SNMP v3 user configuration information. To access this page, click **Management > Local Password Management > User Accounts**.

User Accounts Configuration

User

User Name: (.. to 32 alphanumeric characters)

Password: (8 to 54 Characters)

Confirm Password: (8 to 54 Characters)

Access Level:

Lockout Status:

Password Override-Complexity-Check:

Password Expiration Date:

SNMP v3 User Configuration

SNMP v3 Access Mode:

Authentication Protocol:

Configure Encryption:

Encryption Protocol:

Encryption Key: (8 to 64 characters)

Figure 3-12. Management > Local Password Management > User Accounts

The following table describes the items in the previous menu.

Table 3-10. Management > Local Password Management > User Accounts

Parameter	Description
User	Click the drop-down menu to configure an existing account or to create a new one. Up to support five "Read-Only" accounts.
User Name	Displays the account name or enter a name for new account. Up to 32 alphanumeric characters (not case sensitive) and also the dash ('-') and underscore ('_') are available. Default is not valid for account name.
Password	Enter a new password or change password (between 8 to 64 characters) for the account. It only shows asterisks (*) or dots (.) based on the web browser. The special character as following are available (except " and ?). ~ ` ! @ # \$ % ^ & * () _ - + = [] { } \ : ; ' < > . , /
Confirm Password	Enter the password to verify. It only shows asterisks (*) or dots (.) based on the web browser.
Access Level	Click the drop-down menu to select the user access level. The lowest access level is "Read-Only", and "Read-Write" is the highest. Only the user has "Read-Write" level can suspend a user's access.
Lockout Status	Displays the user account is locked due to excessive login attempts.
Password Override-Complexity Check	Click the drop-down menu to enable or disable override complexity check. The default is Disable.
Password Expiration Date	Displays the expiration date of the password.
SNMP v3 User Configuration	
SNMP v3 Access Mode	Displays the SNMP v3 access privileges. Only the admin account has "Read-Write" access, and other accounts have "Read-Only" access.
Authentication Protocol	Click the drop-down menu to select a SNMP v3 authentication protocol for the selected user account. Specify a password (8 characters) for authentication protocol is MD5 or SHA.
Configure Encryption	Check the checkbox to allow modifying encryption protocol and encryption key.
Encryption Protocol	Click the drop-down menu to select a SNMP v3 encryption protocol. Select None and ignore the Encryption Key.
Encryption Key	Enter a key (between 8 to 64 characters) to be a SNMP v3 encryption key.
Add	Click Add to create a new user account.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete a selected user account. To save the values across a power cycle perform a system save. "Read-Write" user accounts are not deletable.

Line Password

The Line Password function allows you to configure the Telnet access password. Select the line mode type from the following screen before setting up the access password.

To access this page, click **Management > Local Password Management > Line Password**.

Line Password Configuration

Figure 3-13. Management > Local Password Management > Line Password

The following table describes the items in the previous menu.

Table 3-11. Management > Local Password Management > Line Password

Parameter	Description
Line Mode	Click the drop-down menu to select the line mode.
Line Password (8-64 characters)	Enter the password (between 8 to 64 characters) for accessing the device via console, telnet, or source telnet. It only shows asterisks (*) or dots (.) based on the web browser.
Confirm Password (8-64 characters)	Enter the password to verify. It only shows asterisks (*) or dots (.) based on the web browser.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

Enable Password

The Enable Password Configuration allows users to assign a password for accessing the device via console, telnet, or secure telnet. To access this page, click **Management > Local Password Management > Enable Password**.

Enable Password Configuration

Figure 3-14. Management > Local Password Management > Enable Password

The following table describes the items in the previous menu.

Table 3-12. Management > Local Password Management > Enable Password

Parameter	Description
Enable Password (8-64 characters)	Enter the password (between 8 to 64 characters) for accessing the device via console, telnet, or source telnet. It only shows asterisks (*) or dots (.) based on the web browser.
Confirm Enable Password (8-64 characters)	Enter the password to verify. It only shows asterisks (*) or dots (.) based on the web browser.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

3.3.6 Power over Ethernet

Global Configuration and Status

Users can enable or disable the Admin Mode through the drop down menu, and configure power and temperature settings. To access this page, click **Management > Power over Ethernet > Global Configuration and Status**.

PoE Global Configuration and Status

Admin Mode	Enable
Power Budget (1/10 Watts)	3024 (342 to 3J24)
Power Consumption (Watts)	0.1
Power Usage Alarm Threshold (%)	99 (1 to 99)
Cumulative Power Consumption (Kilo-Watts/Hour)	0.00000
Current Measured (mA)	0
Voltage Guard Threshold (1/10 V)	620 (530 to 020)
Power Supply Voltage (V)	47.4
Temperature Guard Threshold (Celsius)	150 (63 to 155)
PoE Temperature (Celsius)	50
Fault Indication	None

Submit Refresh

Figure 3-15. Management > Power over Ethernet > Global Configuration and Status

The following table describes the items in the previous menu.

Table 3-13. Management > Power over Ethernet > Global Configuration and Status

Parameter	Description
Admin Mode	Click the drop-down menu to enable or disable the admin mode. The default is Enable.
Power Budget (1/10 Watts)	Enter a value [between 342 to 342 x (maximum of copper PoE port) to specify PSE maximal supplying power. The unit is 0.1 watt.
Power Consumption (Watts)	Displays the power consumption of PSE's total real-time power consumption. It's the summary of all PSE ports.
Power Usage Alarm Threshold (%)	Enter a power usage alarm threshold (between 1 to 99). The default is 99.
Cumulative Power Consumption (Kilo-Watts/Hour)	Displays the cumulative PSE total power consumption. It's the summary of all PSE ports. The unit is KWH (kilowatt hour).
Current Measured (mA)	Displays the total real-time output current of PSE. It's the summary of all PSE ports. The unit is mA.
Voltage Guard Threshold (1/10V)	Enter a value (between 500 to 620) to specify the PSE over-load guard voltage. The unit is 0.1 voltage. The default is 620.
Power Supply Voltage (V)	Displays the input voltage of power supply units. The unit is voltage.
Temperature Guard Threshold (Celsius)	Enter a value (between 60 to 155) to specifies PSE over-heat guard temperature. The unit is celsius. The default is 150.
PoE Temperature (Celsius)	Displays the PSE operation temperature. The unit is celsius.
Fault Indication	<p>Displays the PSE global fault indication.</p> <ul style="list-style-type: none"> ● None - Specifies PSE detects no error condition. ● Power-Absent - Specifies absence of PSE input power. ● Abnormal-Voltage - Specifies the measured PSE input voltage exceeds guard threshold. ● Over-Heat - Specifies the measured PSE temperature exceeds guard threshold. ● Other-Fault - Specifies PSE detects fault condition which not listed in selection.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Refresh	Click Refresh to update the screen.

Interface Configuration and Status

Users can enable or disable the Admin Mode through the drop down menu, and configure the Power Budget, Power Priority, and Power Pairs. To access this page, click **Management > Power over Ethernet > Interface Configuration and Status**.

PoE Interface Configuration and Status

Interface	ge0/5
Admin Mode	Enable
Power Budget (1/10 Watts)	342 (154 to 342)
Power Priority	Low
Power Pairs	Signal

Interface	Admin Mode	Power Budget	Power Priority	Power Pairs	Power Class	Power Consumption	Cumulative Power Consumption	Current Consumption	Detection Status	Fault Status
ge0/5	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/6	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/7	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/8	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/9	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/10	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/11	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/12	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/13	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/14	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/15	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None
ge0/16	Enable	34.2 Watts	Low	Signal	N/A	0.0 Watts	0.000000 KWH	0 mA	Searching	None

Submit Refresh

Figure 3-16. Management > Power over Ethernet > Interface Configuration and Status The following table describes the items in the previous menu.

Table 3-14. Management > Power over Ethernet > Interface Configuration and Status

Parameter	Description
Interface	Click the drop-down menu to select a PSE port to apply the settings.
Admin Mode	Click the drop-down menu to enable or disable PSE function of the port. The default is "Enable".
Power Budget (1/10 Watts)	Enter a value (between 150 to 342) to specify the maximum of PSE supply power. The default is 342.
Power Priority	Click the drop-down menu to select the power-on priority of PSE port.
Power Pairs	Click the drop-down menu to select the power-carrying pairs. <ul style="list-style-type: none"> • Signal - Supply PD power via 1/2 and 3/6 wire pairs. • Spare - Supply PD power via 4/5 and 7/8 wire pairs.

Table 3-14. Management > Power over Ethernet > Interface Configuration and Status (Continued)

Parameter	Description
Power Class	Displays the PD power classify level. <ul style="list-style-type: none"> ● N/A - Specifies the PSE port is not delivering power. ● Class-0 - Specifies PSE port power class level-0 is selected. The maximal output power in PSE side is 30 Watts. ● Class-1 - Specifies PSE port power class level-1 is selected. The maximal output power in PSE side is 4 Watts. ● Class-2 - Specifies PSE port power class level-2 is selected. The maximal output power in PSE side is 7 Watts. ● Class-3 - Specifies PSE port power class level-3 is selected. The maximal output power in PSE side is 15.4 Watts. ● Class-4 - Specifies PSE port power class level-4 is selected. The maximal output power in PSE side is 30 Watts.
Power Consumption	Displays the power consumption of PSE port. The unit is watt.
Cumulative Power Consumption	Displays the power consumption summary of PSE port. The unit is KWH (kilowatt hour).
Current Consumption	Displays the current consumption summary of PSE port. The unit is mA.
Detection Status	Displays the operation status of PSE port. <ul style="list-style-type: none"> ● Disabled - Specifies PSE port is not delivering power. ● Searching - Specifies PSE port is trying to detect the connection of PD. ● Delivering-Power - Specifies PSE port is delivering power to PD. ● Test - Specifies PSE port IS under test. ● Fault - Specifies PSE port operation fault defined in IEEE 802.3af and 802.3at. ● Other Fault - Specifies PSE port operation fault other than those defined in IEEE 802.3af and 802.3at.
Fault Status	Displays the fault indication of PSE port. <ul style="list-style-type: none"> ● None - Specifies PSE port detects no error condition. ● Short-Circuit - Specifies PSE port detects short circuit in PD loop. ● Over-Load - Specifies PSE port detects lover-load in PD loop. ● Power-Denied - Specifies PSE port denies PD power class request. ● Startup-Failure - Specifies PSE port operation fault defined in IEEE 802.3af and 802.3at. ● Other-Fault - Specifies PSE port fault other than those defined in IEEE 802.3af and 802.3at.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Refresh	Click Refresh to update the screen.

Interface Statistics

The Interface Statistics displays information for each interface. To access this page, click **Management > Power over Ethernet > Interface Statistics**.

PoE Interface Statistics

Interface	MPS Absent	Invalid Signature	Power Denied	Over Load	Short Circuit
ge0/5	0	0	0	0	0
ge0/6	0	0	0	0	0
ge0/7	0	0	0	0	0
ge0/8	0	146	0	0	0
ge0/9	0	0	0	0	0
ge0/10	0	0	0	0	0
ge0/11	0	0	0	0	0
ge0/12	0	0	0	0	0
ge0/13	0	0	0	0	0
ge0/14	0	0	0	0	0
ge0/15	0	0	0	0	0
ge0/16	0	0	0	0	0

Figure 3-17. Management > Power over Ethernet > Interface Statistics

The following table describes the items in the previous menu.

Table 3-15. Management > Power over Ethernet > Interface Statistics

Parameter	Description
Interface	Click the drop-down menu to select a PSE port to clean the PSE statistic counters.
MPS Absent	Displays the count of power-on PD has no longer requested power.
Invalid Signature	Displays the count of invalid MPS (maintenance power signature).
Power Denied	Displays the count of PD request power has been denied.
Over Load	Displays the count of delivering power exceeds PSE port power budget.
Short Circuit	Displays the count of the PSE detects a short circuit in PD loops.
Clean Counter	Click Clean Counter to clean all PSE counter of the selected PSE port,
Refresh	Click Refresh to update the screen.

3.3.7 Email Alerts

Email Alert Global Configuration

The Email Alert Global Configuration page allows users to configure email alert settings. To access this page, click **Management > Email Alerts > Email Alert Global Configuration**.

Email Alert Global Configuration

Figure 3-18. Management > Email Alerts > Email Alert Global

Configuration The following table describes the items in the previous menu.

Table 3-16. Management > Email Alerts > Email Alert Global Configuration

Parameter	Description
Admin Mode	Click the drop-down menu to enable or disable email alerts to SMTP server.
From Address	Enter an email address (up to 255 characters) to send email alerts.
Log Duration	Enter a value (between 30 to 1440 minutes) to send message to SMTP server. The default is 30.
Urgent Messages Severity	Click the drop-down menu to select the severity level for urgent log messages. The default is Alert. The level options are: <ul style="list-style-type: none"> ● Emergency - Indicates system is unusable. It is the highest level of severity. ● Alert - Indicates action must be taken immediately. ● Critical - Indicates critical conditions. ● Error - Indicates error conditions. ● Warning - Indicates warning conditions. ● Notice - Indicates normal but significant conditions. ● Info - Indicates informational messages. ● Debug - Indicates debug-level messages.

Table 3-16. Management > Email Alerts > Email Alert Global Configuration (Continued)

Parameter	Description
Non Urgent Messages Severity	<p>Click the drop-down menu to select the severity level for non-urgent log messages. The default is Warning.</p> <p>The level options are:</p> <ul style="list-style-type: none"> • Emergency - Indicates system is unusable. It is the highest level of severity. • Alert - Indicates action must be taken immediately. • Critical - Indicates critical conditions. • Error - Indicates error conditions. • Warning - Indicates warning conditions. • Notice - Indicates normal but significant conditions. • Info - Indicates informational messages. • Debug - Indicates debug-level messages.
Traps Severity	<p>Click the drop-down menu to select the severity level for trap log messages. The default is Info.</p> <p>The level options are:</p> <ul style="list-style-type: none"> • Emergency - Indicates system is unusable. It is the highest level of severity. • Alert - Indicates action must be taken immediately. • Critical - Indicates critical conditions. • Error - Indicates error conditions. • Warning - Indicates warning conditions. • Notice - Indicates normal but significant conditions. • Info - Indicates informational messages. • Debug - Indicates debug-level messages.
Test Message Type	Click the drop-down menu to select the message type for testing email alert.
Test Message Body	Click the drop-down menu to select the message body for testing email alert.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Test	Click Test to send a logging email for testing.
Refresh	Click Refresh to update the screen.

Email Alert Mail Server Configuration

The Email Alert Mail Server Configuration page allows users to configure mail server settings. To access this page, click **Management > Email Alerts > Email Alert Mail Server Configuration**.

Email Alert Mail Server Configuration

Figure 3-19. Management > Email Alerts > Email Alert Mail Server Configuration The following table describes the items in the previous menu.

Table 3-17. Management > Email Alerts > Email Alert Mail Server Configuration

Parameter	Description
Mail Server Address	Enter an mail server address (up to 255 characters). NOTE: In this version, only supports one mail server configuration.
Mail Server Security	Click the drop-down menu to configure the mail server security.
Mail Server User Name	Enter an user name of the mail server (up to 16 characters).
Mail Server Password	Enter the password of the user (up to 16 characters).
Mail Server Port	Enter a value to configure the mail server port.
Remove	Check the checkboxes to select the mail servers need to be delete.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected row.
Refresh	Click Refresh to update the screen.

Email Alert Statistics

The Email Alert Statistics displays a summary of the emails sent, received, and the time that has lapsed since the last email sent. To access this page, click **Management > Email Alerts > Email Alert Mail Statistics**.

Email Alert Statistics

Number of Emails Sent	0
Number of Emails Failed	0
Time Since Last Email Sent	0 days, 0 hours, 0 mins 0 secs

Figure 3-20. Management > Email Alerts > Email Alert Mail

Statistics The following table describes the items in the previous menu.

Table 3-18. Management > Email Alerts > Email Alert Mail Statistics

Parameter	Description
Number of Emails Sent	Displays the number of sent emails since last reset.
Number of Emails Failed	Displays the number of failed emails since last reset.
Time Since Last Email Sent	Displays the time elapse since the latest email sent succeed.
Clear Counters	Click Clear Counters to clear the counters.
Refresh	Click Refresh to update the screen.

Email Alert Subject Configuration

Users can configure alert settings for urgent emails based on the email subject. To access this page, click **Management > Email Alerts > Email Alert Subject Configuration**.

Email Alert Subject Configuration

Message Type	<input type="text" value="Urgent"/>
Email Subject	<input type="text" value="Urgent Log Messages"/> (1 to 255 Alphanumeric Characters)

Message Type	Email Subject	Remove
Urgent	Urgent Log Messages	<input type="checkbox"/>
Non-Urgent	Non-Urgent Log Messages	<input type="checkbox"/>

Figure 3-21. Management > Email Alerts > Email Alert Subject Configuration

The following table describes the items in the previous menu.

Table 3-19. Management > Email Alerts > Email Alert Subject Configuration

Parameter	Description
Message Type	Click the drop-down menu to configure the logging email alert message type.
Email Subject	Enter the subject (up to 255 alphanumeric characters) to configure the logging email alert subject.
Remove	Check the checkboxes to select the email alerts need to be delete.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected row.
Refresh	Click Refresh to update the screen.

Email Alert To Address Configuration

Users can configure the email address to where emails will be sent based on the message type. To access this page, click **Management > Email Alerts > Email Alert To Address Configuration**.

Email Alert To Address Configuration

Figure 3-22. Management > Email Alerts > Email Alert To Address

Configuration The following table describes the items in the previous menu.

Table 3-20. Management > Email Alerts > Email Alert To Address Configuration

Parameter	Description
Message Type	Click the drop-down menu to select the message type.
To Address	Enter the address (up to 255 characters) to send the logging email alert. Support up to 5 addresses per message type.
Remove	Check the checkboxes to select the addresses need to be delete.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected row.
Refresh	Click Refresh to update the screen.

3.3.8 SNMP

Configuration

The SNMP Community Configuration page allows users to configure community string status and access mode. It also displays the settings for each community string status. To access this page, click **Management > SNMP > Configuration**.

SNMP Community Configuration

Community	public ▼
Client IP Address	0.0.0.0
Client IP Mask	0.0.0.0
Access Mode	Read-Only ▼
Status	Enable ▼

Community	Client IP Address	Client IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read-Only	Enable
private	0.0.0.0	0.0.0.0	Read-Write	Enable

Figure 3-23. Management > SNMP > Configuration

The following table describes the items in the previous menu.

Table 3-21. Management > SNMP > Configuration

Parameter	Description
Community	Click the drop-down menu to select a community name or select Create to create a new one (up to 16 characters).
Client IP Address	Enter the client IP address to allow SNMP clients using the community to access the device. NOTE: Access available for any IP addresses if IP address or IP mask is 0.0.0.0.
Client IP Mask	Enter the client IP mask to allow SNMP clients using the community to access the device. NOTE: Allow to access for only one IP if IP mask is 255.255.255.255.
Access Mode	Click the drop-down menu to specify the access level.
Status	Click the drop-down menu to enable or disable community.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected community.

Trap Server Configuration

The SNMP Trap Server Configuration page allows users to configure SNMP trap receiver settings. To access this page, click **Management > SNMP > Trap Server Configuration**.

SNMP Trap Receiver Configuration

SNMP Trap Name	Create ▾
SNMP Trap Name	<input type="text"/> (0 to 16 characters)
SNMP Version	SNMP v1 ▾
Protocol	IPv4 ▾
IP Address	<input type="text"/>
Status	Enable ▾

SNMP Trap Name	SNMP Version	IP Address	Status
----------------	--------------	------------	--------

Figure 3-24. Management > SNMP > Trap Server Configuration

The following table describes the items in the previous menu.

Table 3-22. Management > SNMP > Trap Server Configuration

Parameter	Description
SNMP Trap Name	Click the drop-down menu to select a SNMP trap name or select Create to create a new one (up to 16 characters and case sensitive).
SNMP Version	Click the drop-down menu to select a SNMP version. The version options are: <ul style="list-style-type: none"> • SNMP v1 - Uses SNMP v1 to send traps to the receiver. • SNMP v2 - Uses SNMP v2 to send traps to the receiver.
Protocol	Click the drop-down menu to select a protocol for the SNMP trap receiver configuration. The options are: <ul style="list-style-type: none"> • IPv4 - Choose IPv4 to enter the address in IPv4 format.
IP Address	Enter the IP address to the selected protocol.
Status	Click the drop-down menu to enable or disable receiver's status. <ul style="list-style-type: none"> • Enable - Send traps to the receiver. • Disable - Do not send traps to the receiver.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected trap name.

3.3.9 Event Manager

Event Policy Configuration

The Event Policy Configuration page allows users to configure settings for event policies. To access this page, click **Management > Event Manager > Event Policy Configuration**.

Event Policy Configuration

The screenshot shows a configuration form with the following fields and options:

- Event Policy: default
- Cold Start: Disable
- Warm Start: Disable
- Authentication Fail: Disable
- X-Ring+ Critical: Enable
- Link State Change: List of interfaces (None, ge0/1, ge0/2, ge0/3, ge0/4, ge0/5, ge0/6, ge0/7)
- Config Change: Disable
- Firmware Upgrade: Enable
- Firmware Upgrade Fail: Enable
- PoE Port State Change: Disable
- PoE Power Overload: Disable

Buttons: Submit, Delete

Policy Name	Notification Events
default	X-Ring+ critical

Figure 3-25. Management > Event Manager > Event Policy Configuration

The following table describes the items in the previous menu.

Table 3-23. Management > Event Manager > Event Policy Configuration

Parameter	Description
Event Policy	Click the drop-down menu to select a event policy or select Create to create a new one (up to 31 characters).
Cold Start	Click the drop-down menu to enable or disable cold start event.
Warm Start	Click the drop-down menu to enable or disable warm start event.
Authentication Fail	Click the drop-down menu to enable or disable SNMP authentication fail event.
X-Ring Pro Critical	Click the drop-down menu to enable or disable X-Ring pro critical event.
Link State Change	Select the option from the Link State Change.
Config Change	Click the drop-down menu to enable or disable configuration change event.
Firmware Upgrade	Click the drop-down menu to enable or disable firmware upgrade event.
Firmware Upgrade Fail	Click the drop-down menu to enable or disable firmware upgrade fail event.
PoE Port State Change	Click the drop-down menu to enable or disable PoE port power state change event.

Table 3-23. Management > Event Manager > Event Policy Configuration (Continued)

Parameter	Description
PoE Power Overload	Click the drop-down menu to enable or disable the PoE global power overload event.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected policy name.

Event Manager Configuration

The Event Manager Configuration page allows users to configure logging, traps, alerts and alarm settings for events. To access this page, click **Management > Event Manager > Event Manager Configuration**.

Event Manager Configuration

Logging	default ▾
Traps	default ▾
Alert Mail	default ▾
Alarm Relay	default ▾
Alarm LED	default ▾

Submit

Figure 3-26. Management > Event Manager > Event Manager Configuration The following table describes the items in the previous menu.

Table 3-24. Management > Event Manager > Event Manager Configuration

Parameter	Description
Logging	Click the drop-down menu to select a policy for notify through logging.
Traps	Click the drop-down menu to select a policy for notify through SNMP trap.
Alert Mail	Click the drop-down menu to select a policy for notify through alert mail.
Alarm Relay	Click the drop-down menu to select a policy for notify through alert relay.
Alarm LED	Click the drop-down menu to select a policy for notify alarm LED.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

3.3.10 Trap Manager

Trap Flags

The Trap Flags page allows users to configure trap flag settings. To access this page, click **Management > Trap Manager > Trap Flags**.

Trap Flags

Authentication	Enable ▾
Link Up/Down	Enable ▾
Multiple Users	Enable ▾
Spanning Tree	Enable ▾
ACL Traps	Disable ▾

Figure 3-27. Management > Trap Manager > Trap Flags

The following table describes the items in the previous menu.

Table 3-25. Management > Trap Manager > Trap Flags

Parameter	Description
Authentication	Click the drop-down menu to enable or disable activation of authentication failure traps. The default is Enable.
Link Up/Down	Click the drop-down menu to enable or disable activation of link status traps. The default is Enable.
Multiple Users	Click the drop-down menu to enable or disable activation of multiple user traps. The default is Enable.
Spanning Tree	Click the drop-down menu to enable or disable activation of spanning tree traps. The default is Enable.
ACL Traps	Click the drop-down menu to enable or disable activation of ACL traps. The default is Disable.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

Trap Logs

Trap Logs displays the entries in the trap log. To access this page, click **Management > Trap Manager > Trap Logs**.

Trap Logs

Number of Traps Since Last Reset	0
Trap Log Capacity	256
Number of Traps Since Log Last Viewed	0

Log	System Up Time	Trap
-----	----------------	------

Figure 3-28. Management > Trap Manager > Trap Logs

The following table describes the items in the previous menu.

Table 3-26. Management > Trap Manager > Trap Logs

Parameter	Description
Number of Traps Since Last Reset	Displays the number of traps generated since the trap log entries were last cleared.
Trap Log Capacity	Displays the maximum number of traps stored in the log. If exceed, the entries overwrite the oldest one.
Number of Traps Since Log Last Viewed	Displays the number of traps have occurred since the traps were last displayed. The counter will be cleared if the traps are displayed.
Log	Displays the sequence number of the trap.
System Up Time	Displays the trap occurred time since reboot the switch at the last time as follows: days, hours, minutes and seconds.
Trap	Displays the identified information of the trap.
Clear Log	Click Clear Log to clear all entries in the log.

3.3.11 DHCP Server

Global Configuration

The Global Configuration page allows users to configure the global settings for DHCP servers, add, and delete excluded addresses. To access this page, click **Management > DHCP Server > Global Configuration**.

DHCP Server Global Configuration

Admin Mode	<input type="text" value="Disable"/>
Ping Packet Count	<input type="text" value="2"/> (0, 2 to 10)
Conflict Logging Mode	<input type="text" value="Enable"/>
Bootp Automatic Mode	<input type="text" value="Disable"/>
Add Excluded Addresses	
From	<input type="text" value="0.0.0.0"/>
To	<input type="text" value="0.0.0.0"/> (a.b.c.d to Exclude address range or 0.0.0.0 to exclude single address)
Delete Excluded Addresses	
<input type="text" value="Delete"/>	<input type="text" value="From"/> <input type="text" value="To"/>
<input type="button" value="Submit"/> <input type="button" value="Delete"/>	

Figure 3-29. Management > DHCP Server > Global Configuration

The following table describes the items in the previous menu.

Table 3-27. Management > DHCP Server > Global Configuration

Parameter	Description
Admin Mode	Click the drop-down menu to enable or disable DHCP service. The default is Disable.
Ping Packet Count	Enter the number (0 or between 2 to 10) of packets a server sends to a pool address to check. The default is 2. 0 means disable the function.
Conflict Logging Mode	Click the drop-down menu to enable or disable conflict logging on a DHCP server. The default is Enable.
Bootp Automatic Mode	Click the drop-down menu to enable or disable Bootp for dynamic pools. The default is Disable.
Add Excluded Addresses	
From	Enter an IP address user want to exclude a range of addresses.
To	Enter an IP address user want to exclude a range of addresses. To exclude a single address, enter the same IP address as in From or enter 0.0.0.0.
Delete Excluded Addresses	
Delete	Check the checkboxes to select the ranges need to be delete.
From	Enter an IP address user want to exclude a range of addresses.
To	Enter an IP address user want to exclude a range of addresses. To exclude a single address, enter the same IP address as in From or enter 0.0.0.0.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected row.

Pool Configuration

The Pool Configuration page allows users to configure settings for existing pools, as well as create new pools. To access this page, click **Management > DHCP Server > Pool Configuration**.

DHCP Server Pool Configuration

The screenshot shows the DHCP Server Pool Configuration interface. It includes the following fields and controls:

- Pool Name:** A dropdown menu with '1' selected.
- Type of Binding:** A dropdown menu with 'Unallocated' selected.
- Lease time:** A dropdown menu with 'Specified Duration' selected.
- Days:** A text input field containing '1', with a range indicator '(1 to 59)'.
- Hours:** A text input field containing '0', with a range indicator '(0 to 23)'.
- Minutes:** A text input field containing '0', with a range indicator '(0 to 59)'.
- Default Router Addresses:** Five text input fields, each containing '0.0.0.0'.

Figure 3-30. Management > DHCP Server > Pool Configuration

The following table describes the items in the previous menu.

Table 3-28. Management > DHCP Server > Pool Configuration

Parameter	Description
Pool Name	Click the drop-down menu to select a pool name or select Create to create a new one (up to 31 characters). It is available when user has "Read-Write" level.
Type of Binding	<p>Click the drop-down menu to select a type of binding for the pool.</p> <ul style="list-style-type: none"> ● Unallocated ● Automatic - The following fields are available when Type of Binding is Automatic. <ul style="list-style-type: none"> ● Network Number - Enter the IP subnet address for an automatic DHCP pool. ● Network Mask - Enter the IP mask address for an automatic DHCP pool. ● Prefix Length - Enter the prefix length (between 0 to 32) for an automatic DHCP pool. Configure one of Network Mask or Prefix Length. ● Prefix Length Option Enable - Check the checkbox to configure the Network Number using Prefix Length or Network Mask. ● Manual - The following fields are available when Type of Binding is Manual. <ul style="list-style-type: none"> ● Client Name - Enter the client name (between 1 to 31 characters) for DHCP manual pool. ● Hardware Address - Enter the MAC address of the hardware platform of the DHCP client. ● Hardware Address Type - Enter the protocol of the hardware platform of the DHCP client. The default is Ethernet. ● Client ID - Enter the client ID for DHCP manual Pool. In some systems, such as Microsoft DHCP clients, client ID is necessary, not hardware address. ● Host Number - Enter the IP host address for a manual binding to a DHCP client. Host can be set if at least one of Client ID or Hardware Address is specified. ● Host Mask - Enter the IP mask address for a manual binding to a DHCP client. ● Prefix Length - Enter the prefix length (between 0 to 32) for an automatic DHCP pool. Configure one of Host Mask or Prefix Length. ● Prefix Length Option Enable - Check the checkbox to configure the Host Number using Prefix Length or Host Mask.
Lease Time	Click the drop-down menu to select a lease time. The default is Specified Duration.
Days	Enter a number of days (between 0 to 59) of a lease period. It is available when Lease Time is Specified Duration. The default is 1.
Hours	Enter a number of hours (between 0 to 23) of a lease period. It is available when Lease Time is Specified Duration. The default is 0.
Minutes	Enter a number of minutes (between 0 to 59) of a lease period. It is available when Lease Time is Specified Duration. The default is 0.

Table 3-28. Management > DHCP Server > Pool Configuration (Continued)

Parameter	Description
Default Router Addresses	Enter the list of default router addresses (up to 8).
DNS Server Addresses	Enter the list of DNS server addresses for the pool (up to 8).
NetBIOS Name Server Addresses	Enter the list of NetBIOS name server addresses for the pool (up to 8).
NetBIOS Node Type	Click the drop-down menu to select the NetBIOS node type for DHCP clients. <ul style="list-style-type: none"> • b-node Broadcast • p-node Peer-to-Peer • m-node Mixed • h-node Hybrid
Next Server Address	Enter the next server address for the pool.
Domain Name	Enter the domain name (up to 255 characters) for a DHCP client.
Bootfile	Enter the name of the default boot image (up to 128 characters) for a DHCP client.
Add Option	Check the checkbox to configure the DHCP server options.
OptionCode	Enter the DHCP option code (between 1 to 254).
ASCII Value	Enter the NVT ASCII character string.
Hex Value	Enter the hexadecimal data (2 bytes or 4 hexadecimal digits). Separate each bytes by a colon or a space.
IP Address Value	Enter the option IP addresses (up to 8).
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the pool. It is available for "Read-Write" level.

Static Port Binding Configuration

The DHCP Static Port Binding Configuration page allows users to configure the IP address and IP mask for each interface. To access this page, click **Management > DHCP Server > Static Port Binding Configuration**.

DHCP Static Port Binding Configuration

Interface	<input type="text" value="ge0/1"/>	<input type="button" value="Delete"/>
IP Address	<input type="text" value="n.n.n.n"/>	
IP Mask	<input type="text" value="0.0.0.0"/>	

Interface	IP Address	IP Mask
ge0/1	0.0.0.0	0.0.0.0
ge0/2	0.0.0.0	0.0.0.0
ge0/3	0.0.0.0	0.0.0.0
ge0/4	0.0.0.0	0.0.0.0
ge0/5	0.0.0.0	0.0.0.0
ge0/6	0.0.0.0	0.0.0.0
ge0/7	0.0.0.0	0.0.0.0
ge0/8	0.0.0.0	0.0.0.0
ge0/9	0.0.0.0	0.0.0.0
ge0/10	0.0.0.0	0.0.0.0
ge0/11	0.0.0.0	0.0.0.0
ge0/12	0.0.0.0	0.0.0.0
ge0/13	0.0.0.0	0.0.0.0
ge0/14	0.0.0.0	0.0.0.0
ge0/15	0.0.0.0	0.0.0.0
ge0/16	0.0.0.0	0.0.0.0
LAG1	0.0.0.0	0.0.0.0

Figure 3-31. Management > DHCP Server > Static Port Binding Configuration

The following table describes the items in the previous menu.

Table 3-29. Management > DHCP Server > Static Port Binding Configuration

Parameter	Description
Interface	Click the drop-down menu to select a port for configuration
IP Address	Enter the IP address to assign the selected port.
IP Mask	Enter the IP mask address to assign the selected port.
Delete	Click Delete to clear the current configuration settings.
Create	Click Create to accept the configuration settings and include a new entry into the DHCP Static Port Binding table.
Interface	Displays the port number/type.
IP Address	Displays the assigned IP address for the corresponding port.
IP Mask	Displays the assigned IP address for the corresponding port.
Refresh	Click Refresh to update the screen.

Pool Options

The Pool options page displays options for existing pools. To access this page, click **Management > DHCP Server > Pool Options**.

DHCP Server Pool Options

Figure 3-32. Management > DHCP Server > Pool Options

The following table describes the items in the previous menu.

Table 3-30. Management > DHCP Server > Pool Options

Parameter	Description
Pool Name	Click the drop-down menu to select a pool name.
Delete	Check the checkboxes to select the option codes need to be delete.
Option Code	Displays the option code for the selected pool.
ASCII Value	Displays the option ASCII value for the selected pool.
Hex Value	Displays the option hex value for the selected pool.
IP Address Value	Displays the option IP addresses for the selected pool.
Delete	Click Delete to delete the selected row.

Reset Configuration

The DHCP Server Reset Configuration allows users to perform a reset. To access this page, click **Management > DHCP Server > Reset Configuration**.

DHCP Server Reset Configuration

Figure 3-33. Management > DHCP Server > Reset Configuration

The following table describes the items in the previous menu.

Table 3-31. Management > DHCP Server > Reset Configuration

Parameter	Description
Clear	Click the drop-down menu to select a option needs to be delete.
IP Address	Enter the against IP address needs to be delete. It is available when Clear is Specific Dynamic Binding or Specific Address Conflict.

Table 3-31. Management > DHCP Server > Reset Configuration (Continued)

Parameter	Description
Clear All Bindings	Click Clear All Bindings to clear all the dynamic bindings. It is available when Clear is All Dynamic Bindings.
Clear Specific Binding	Click Clear Specific Binding to clear the specified dynamic binding. It is available when Clear is Specific Dynamic Binding.
Clear All Conflicts	Click Clear All Conflicts to clear all the address conflicts. It is available when Clear is All Address Conflicts.
Clear Specific Conflict	Click Clear Specific Conflict to clear the specified address conflict. It is available when Clear is Specific Address Conflicts.

Bindings Information

The Bindings Information displays the IP address, hardware address, lease time left and pool allocation type for all bindings, or specific bindings. To access this page, click **Management > DHCP Server > Bindings Information**.

DHCP Server Bindings Information

Figure 3-34. Management > DHCP Server > Bindings

Information The following table describes the items in the previous menu.

Table 3-32. Management > DHCP Server > Bindings Information

Parameter	Description
DHCP Binding	Click the drop-down menu to select the information need to be displayed.
Binding IP Address	Enter the against IP address. It is available when DHCP Binding is Specific Binding.
IP Address	Displays the client's IP address.
Hardware Address	Displays the client's hardware address.
Lease Time Left	Displays the lease time as follows: days, hours and minutes.
Type	Displays the type of binding.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Refresh	Click Refresh to update the screen.

Server Statistics

The DHCP Server Statistics page displays a list of the DHCP Server functions. To access this page, click **Management > DHCP Server > Server Statistics**.

DHCP Server Statistics

Automatic Bindings	0
Expired Bindings	0
Malformed Messages	0
Message Received	
DHCPDISCOVER	0
DHCPREQUEST	0
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
Message Sent	
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

Figure 3-35. Management > DHCP Server > Server Statistics

The following table describes the items in the previous menu.

Table 3-33. Management > DHCP Server > Server Statistics

Parameter	Description
Automatic Bindings	Displays the number of automatic bindings on the DHCP server.
Expired Bindings	Displays the number of expired bindings on the DHCP server.
Malformed Messages	Displays the number of malformed messages.
Message Received	Displays the type of messages received.
DHCPDISCOVER	Displays the number of DHCPDISCOVER messages received by the DHCP Server.
DHCPREQUEST	Displays the number of DHCPREQUEST messages received by the DHCP Server.
DHCPDECLINE	Displays the number of DHCPDECLINE messages received by the DHCP Server.
DHCPRELEASE	Displays the number of DHCPRELEASE messages received by the DHCP Server.
DHCPINFORM	Displays the number of DHCPINFORM messages received by the DHCP Server.
Message Sent	Displays the type of messages sent.
DHCPOFFER	Displays the number of DHCPOFFER messages sent by the DHCP Server.
DHCPACK	Displays the number of DHCPACK messages sent by the DHCP Server.
DHCPNAK	Displays the number of DHCPNAK messages sent by the DHCP Server.

Table 3-33. Management > DHCP Server > Server Statistics (Continued)

Parameter	Description
Refresh	Click Refresh to update the screen.
Clear Server Statistics	Click Clear Server Statistics to reset DHCP server statistics.

Conflicts Information

The Conflicts Information displays the IP address, detection method, and detection time for all conflicts, or a specific conflict. To access this page, click **Management > DHCP Server > Conflicts Information**.

DHCP Server Conflicts Information

DHCP Conflict: All Conflicts

IP Address	Detection Method	Detection Time
------------	------------------	----------------

Refresh

Figure 3-36. Management > DHCP Server > Conflicts Information

The following table describes the items in the previous menu.

Table 3-34. Management > DHCP Server > Conflicts Information

Parameter	Description
DHCP Conflict	Click the drop-down menu to select the information need to be displayed.
Conflict IP Address	Enter the conflict IP address. It is available when DHCP Conflict is Specific Conflict.
IP Address	Displays the host IP address recorded on the DHCP server.
Detection Method	Displays the manner when host IP address was found on the DHCP server.
Detection Time	Displays the time when the conflict was detected as follows: days, hh:mm:ss.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save. It is available when DHCP Conflict is Specific Conflict.
Refresh	Click Refresh to update the screen.

3.3.12 DNS

Global Configuration

Global Configuration allows users to enable or disable the admin mode from the drop-down menu, configure the default domain name, retry number, and response timeout. To access this page, click **Management > DNS > Global Configuration**.

DNS Global Configuration

Admin Mode	Enable ▾	
Default Domain Name	<input type="text"/>	(1 to 255 alphanumeric characters)
Retry Number	<input type="text" value="2"/>	(0 to 100)
Response Timeout (secs)	<input type="text" value="3"/>	(0 to 3600 secs)

Default Domain List

Domain List	Remove
-------------	--------

Figure 3-37. Management > DNS > Global Configuration

The following table describes the items in the previous menu.

Table 3-35. Management > DNS > Global Configuration

Parameter	Description
Admin Mode	Click the drop-down menu to enable or disable the administrative status of DNS client. The default is Enable.
Default Domain Name	Enter the default domain name (up to 255 characters) for DNS client.
Retry Number	Enter the number of times (between 0 to 100) to retry sending DNS queries. The default is 2.
Response Timeout (secs)	Enter the amount of times (between 0 to 3600) to wait for a response to a DNS query. The default is 3.
Domain List	Displays the domain name list for DNS client.
Remove	Check the checkboxes to select the domain names need to delete.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Refresh	Click Refresh to update the screen.

Server Configuration

DNS Server Configuration allows users to specify the DNS server address. To access this page, click **Management > DNS > Server Configuration**.

DNS Server Configuration

Figure 3-38. Management > DNS > Server Configuration

The following table describes the items in the previous menu.

Table 3-36. Management > DNS > Server Configuration

Parameter	Description
DNS Server Address	Enter the DNS server address (IPv4).
DNS Server List	
DNS Server Address	Displays the list of DNS server address.
Precedence	Displays the preference of the DNS server.
Remove	Check the checkboxes to select the DNS server addresses need to delete.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Refresh	Click Refresh to update the screen.
Delete	Click Delete to delete the selected row.

HostName IP Mapping Summary

DNS HostName IP Mapping Summary allows users to add Static Entries. To access this page, click **Management > DNS > HostName IP Mapping Summary**.

DNS HostName IP Mapping Summary

Figure 3-39. Management > DNS > HostName IP Mapping Summary

The following table describes the items in the previous menu.

Table 3-37. Management > DNS > HostName IP Mapping Summary

Parameter	Description
DNS Static Entries	
Host Name	Displays the host name of the static entry.
Inet Address	Displays the IPv4 address of the static entry.
Remove Static	Check the checkboxes to select the host names need to delete.
Add Static Entry	Click Add Static Entry to create a new static host name.
DNS Dynamic Entries	
Host Name	Displays the host name of the dynamic entry.
Total	Displays the elapsed time of the dynamic entry.
Elapsed	Elapsed time of the dynamic entry.
Type	Displays the type of the dynamic entry.
Addresses	Displays the IPv4 address of the dynamic entry.
Remove Dynamic	Check the checkboxes to select the dynamic host names need to delete.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Clear Dynamic Entries	Click Clear Dynamic Entries to delete all dynamic host names.
Refresh	Click Refresh to update the screen.

3.3.13 Date and Time

Configuration

Data and Time Global Configuration allows users to configure date and time settings. Users can select unicast, broadcast, or disable the client mode from the drop-down menu. To access this page, click **Management > Date and Time > Configuration**.

Date and Time Global Configuration

SNTP Configuration

Client Mode	<input type="text" value="Disabled"/>	
Port	<input type="text" value="0"/>	(1 to 65535; Default: 0)
Unicast Poll Interval	<input type="text" value="6"/>	(6 to 10 secs)
Broadcast Poll Interval	<input type="text" value="6"/>	(6 to 10 secs)
Unicast Poll Timeout	<input type="text" value="5"/>	(1 to 30 secs)
Unicast Poll Retry	<input type="text" value="1"/>	(0 to 10)

Manual Configuration

Time Zone	<input type="text"/>	
System Date	<input type="text" value="1939:07:30"/>	(yyyy:mm:dd)
System Time	<input type="text" value="02:31:20"/>	(hh:mm:ss)

Figure 3-40. Management > Date and Time > Configuration

The following table describes the items in the previous menu.

Table 3-38. Management > Date and Time > Configuration

Parameter	Description
SNTP Configuration	
Client Mode	Click the drop-down menu to select the SNTP client mode of operation. The options are: <ul style="list-style-type: none"> Disable - SNTP is not operational. No SNTP requests are sent from the client nor are any received SNTP messages processed. Unicast - SNTP operates in a point to point fashion. A unicast client sends a request to a designated server at its unicast address and expects a reply from which it can determine the time and, optionally the round-trip delay and local clock offset relative to the server. Broadcast - SNTP operates in the same manner as multicast mode but uses a local broadcast address instead of a multicast address. The broadcast address has a single subnet scope while a multicast address has Internet wide scope.
Port	Enter the local UDP port (between 1 to 65535). The default is 0. When Port is 0, the actual client port value is assigned by the operation system.
Unicast Poll Interval	Enter the number of seconds (between 6 to 10) between unicast poll requests expressed as a power of two when configured in unicast mode. The default is 6.
Broadcast Poll Interval	Enter the number of seconds (between 6 to 10) between broadcast poll requests expressed as a power of two when configured in unicast mode. The default is 6.
Unicast Poll Timeout	Enter the number of seconds (between 1 to 30) to wait for a SNTP response when configured in unicast mode. The default is 5.

Table 3-38. Management > Date and Time > Configuration (Continued)

Parameter	Description
Unicast Poll Retry	Enter the number of times (between 0 to 10) to retry a request to an SNTP server after the first time-out when configured in unicast mode. The default is 1.
Manual Configuration	
Time Zone	Enter the name of the system time zone.
System Date	Enter the local date of the system as follows yyyy:mm:dd.
System Time	Enter the local time of the system as follows hh:mm or hh:mm:ss.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

Status

The Date and Time Global Status displays Global, and Date and Time information. To access this page, click **Management > Date and Time > Status**.

Date and Time Global Status

SNTP Global Status

Version	4
Supported Mode	Unicast and Broadcast
Last Update Time	Jan 1 00:00:00 197C
Last Attempt Time	Jan 1 00:00:00 197C
Last Attempt Status	Other
Server IP Address	
Address Type	Unknown
Server Stratum	0
Reference Clock ID	
Server Mode	Reserved
Unicast Server Max Entries	3
Unicast Server Current Entries	0
Broadcast Count	0

Date and Time Status

Time Zone	
Time Zone Acronym	Not Available
Time Zone Offset	UTC+0:00
System Date	1E99:07:30
System Time	02:32:34

Figure 3-41. Management > Date and Time > Status

The following table describes the items in the previous menu.

Table 3-39. Management > Date and Time > Status

Parameter	Description
SNTP Global Status	
Version	Displays the client supported NTP version.
Supported Mode	Displays the SNTP modes the client supports. Multiple modes may be supported by a client.

Table 3-39. Management > Date and Time > Status (Continued)

Parameter	Description
Last Update Time	Displays the local date and time (UTC) the SNTP client last updated the system clock.
Last Attempt Time	Displays the local date and time (UTC) of the last SNTP request or receipt of an unsolicited message.
Last Attempt Status	<p>Displays 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.</p> <ul style="list-style-type: none"> • Other - None of the following enumeration values. • Success - The SNTP operation was successful and the system time was updated. • Request Timed Out - A directed SNTP request timed out without receiving a response from the SNTP server. • Bad Date Encoded - The time provided by the SNTP server is not valid. • Version Not Supported - The SNTP version supported by the server is not compatible with the version supported by the client. • Server Unsynchronized - The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • Server Kiss Of Death - The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.
Server IP Address	Displays 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	Displays the address type of the SNTP Server address for the last received valid packet.
Server Stratum	Displays the claimed stratum of the server for the last received valid packet.
Reference Clock Id	Displays the reference clock identifier of the server for the last received valid packet.
Server Mode	Displays the server mode for the last received valid packet.
Unicast Server Max Entries	Displays the maximum number of unicast server entries that can be configured on this client.
Unicast Server Current Entries	Displays the number of current valid unicast server entries configured for this client.
Broadcast Count	Displays the number of unsolicited broadcast SNTP messages received and processed by the SNTP client since last reboot.
Date and Time Status	
Time Zone	Displays the full name of the system time zone.
Time Zone Acronym	Displays the acronym of the system time zone.
Time Zone Offset	Displays the UTC offset of the system time zone.
System Date	Displays the local date of the system.

Table 3-39. Management > Date and Time > Status (Continued)

Parameter	Description
System Time	Displays the local time of the system.
Refresh	Press Refresh to update the data on the screen.

Server Configuration

The SNTP Server Configuration allows users to configure the server settings. To access this page, click **Management > Date and Time > Server Configuration**.

SNTP Server Configuration

Figure 3-42. Management > Date and Time > Server Configuration

The following table describes the items in the previous menu.

Table 3-40. Management > Date and Time > Server Configuration

Parameter	Description
Server	Click the drop-down menu to select existing Server Addresses or create one. When the user selects "Create" another text box "Address" appears where the user may enter Address for Server to be configured.
Address/Hostname	Enter the address of the SNTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a SNTP server. Unicast SNTP requests will be sent to this address. If this address is a DNS hostname, then that hostname should be resolved into an IP address each time a SNTP request is sent to it.
Address Type	Click the drop down menu to specify the address type of the configured SNTP, options include: <ul style="list-style-type: none"> • IPv4 (default) • DNS
Port	Enter the port on the server to which SNTP requests are to be sent. Allowed range is 1 to 65535 (default: 123).
Priority	Enter the priority of this server entry to determine the SNTP server target sequence. The client continues sending requests to different servers until a successful response is received or all servers are exhausted. This object indicates the order in which to query the servers. A server entry with a precedence of 1 will be queried before a server with a priority of 2, and so forth. If more than one server has the same priority then the requesting order will follow the lexicographical ordering of the entries in this table. Allowed range is 1 to 3 (default 1).

Table 3-40. Management > Date and Time > Server Configuration (Continued)

Parameter	Description
Version	Enter the NTP Version running on the server. Allowed range is 1 to 4. Default value is 4.
Submit	Press Submit to submit the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Press Delete to remove the SNTP Server entry. Sends the updated configuration to the switch. Configuration changes take effect immediately.

Server Status

The SNTP Server Status displays server information. Users can select the server IP address from the drop-down menu. To access this page, click **Management > Date and Time > Server Status**.

SNTP Server Status

No SNTP Server Exists

Figure 3-43. Management > Date and Time > Server Status

The following table describes the items in the previous menu.

Table 3-41. Management > Date and Time > Server Status

Parameter	Description
Address	Displays all the existing Server Addresses. If no Server configuration exists, a message saying "No SNTP server exists" flashes on the screen.
Last Update Time	Displays the local date and time (UTC) that the response from this server was used to update the system clock.
Last Attempt Time	Displays the local date and time (UTC) that this SNTP server was last queried.
Last Attempt Status	Displays 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. <ul style="list-style-type: none"> • Other - None of the following enumeration values. • Success - The SNTP operation was successful and the system time was updated. • Request Timed Out - A directed SNTP request timed out without receiving a response from the SNTP server. • Bad Date Encoded - The time provided by the SNTP server is not valid. • Version Not Supported - The SNTP version supported by the server is not compatible with the version supported by the client. • Server Unsynchronized - The SNTP server is not synchronized with its peers. This is indicated via the 'leap indicator' field on the SNTP message. • Server Kiss Of Death - The SNTP server indicated that no further queries were to be sent to this server. This is indicated by a stratum field equal to 0 in a message received from a server.

Table 3-41. Management > Date and Time > Server Status (Continued)

Parameter	Description
Unicast Server Num Requests	Displays the number of SNTP requests made to this server since last agent reboot.
Unicast Server Num Failed Requests	Displays the number of failed SNTP requests made to this server since last reboot.
Refresh	Press Refresh to update the data on the screen with the present state of the data in the switch.

3.3.14 ISDP

Global Configuration

The Global Configuration page allows users to configure the global settings for ISDP functions. To access this page, click **Management > ISDP > Global Configuration**.

ISDP Global Configuration

ISDP Mode	Disable
ISDP V2 Mode	Enable
Message Interval(secs)	30 (5 to 254)
Hold Time Interval(secs)	180 (10 to 255)
Device ID	AKS007J027
Device ID Format Capability	Serial Number, Host Name
Device ID Format	Serial Number

Submit

Figure 3-44. Management > ISDP > Global Configuration

The following table describes the items in the previous menu.

Table 3-42. Management > ISDP > Global Configuration

Parameter	Description
ISDP Mode	Click the drop-down menu to enable or disable Industry Standard Discovery Protocol.
ISDP V2 Mode	Click the drop-down menu to disable or enable the Industry Standard Discovery Protocol V2.
Message Interval (secs)	Enter the ISDP transmit interval: range 5 to 254 (default 30 seconds).
Hold Time Interval (secs)	Enter the ISDP holding time range (10 to 255, default: 180 seconds).
Device ID	Displays the Device ID advertised by this device. The format of this Device ID is characterized by the value of Device ID Format object.

Table 3-42. Management > ISDP > Global Configuration (Continued)

Parameter	Description
Device ID Format Capability	<p>Displays the device ID format capability of the device.</p> <ul style="list-style-type: none"> Serial Number - Indicates that the device uses serial number as the format for its Device ID. MAC Address - Indicates that the device uses layer 2 MAC address as the format for its Device ID. Other - Indicates that the device uses its platform specific format as the format for its Device ID.
Device ID format	<p>Displays the device ID format of the device.</p> <ul style="list-style-type: none"> Serial Number - Indicates that the value is in the form of an ASCII string containing the device serial number. MAC Address - 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 serial number appended/prepended with system name.
Submit	<p>Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.</p>

Cache Table

The Cache Table page displays a list of cache summary for ISDP. To access this page, click **Management > ISDP > Cache Table**.

ISDP Cache Table



Figure 3-45. Management > ISDP > Cache Table

The following table describes the items in the previous menu.

Table 3-43. Management > ISDP > Cache Table

Parameter	Description
Device ID	Displays the string with Device ID which is reported in the most recent ISDP message.
Interface	Displays the interface which this neighbor is attached to.
IP Address	Displays the (first) network-layer address which is reported in the Address TLV of the most recently received ISDP message.
Version	Displays the Version string for neighbor.
Hold Time (secs)	Displays the ISDP hold time for neighbor.
Capability	Displays the ISDP Functional Capabilities for neighbor.

Table 3-43. Management > ISDP > Cache Table (Continued)

Parameter	Description
Platform	Displays the ISDP Hardware Platform for neighbor.
Port ID	Displays the ISDP Port ID string for neighbor.
Protocol Version	Displays the ISDP Protocol Version for neighbor.
Last Time Changed (dd:hh:mm:ss)	Displays when entry was last modified: dd-days, hh-hours, mm-minutes, ss-seconds.
Clear	Click Clear to refresh the ISDP Neighbor Table of all the interfaces.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Interface Configuration

The Interface Configuration page allows users to configure the ISDP interface. To access this page, click **Management > ISDP > Interface Configuration**.

ISDP Interface Configuration

The screenshot shows a configuration form with two dropdown menus. The first dropdown is labeled 'Interface' and has 'geE/1' selected. The second dropdown is labeled 'ISDP Mode' and has 'Enable' selected. Below the dropdowns are two buttons: 'Submit' and 'Refresh'.

Figure 3-46. Management > ISDP > Interface Configuration

The following table describes the items in the previous menu.

Table 3-44. Management > ISDP > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the ISDP interface to configure.
ISDP Mode	Click the drop-down menu to enable or disable the Industry Standard Discovery Protocol.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Statistics

The Statistics page displays a summary of the ISDP Statistics. To access this page, click **Management > ISDP > Statistics**.

ISDP Statistics

Packets Received
 Packets Transmitted
 ISDPv1 Packets Received
 ISDPv1 Packets Transmitted
 ISDPv2 Packets Received
 ISDPv2 Packets Transmitted
 Bad Header
 Checksum Error
 Transmission Failure
 Invalid Format Packets Received
 Table Full
 ISDP IP Address Table Full

Clear Refresh

Figure 3-47. Management > ISDP > Statistics

The following table describes the items in the previous menu.

Table 3-45. Management > ISDP > Statistics

Parameter	Description
Packets Received	Displays the number of all ISDP PDUs received.
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.
Bad Header	Displays the number of ISDP PDUs with bad header received.
Checksum Error	Displays the number of ISDP PDUs with checksum error received.
Transmission Failure	Displays the number of ISDP PDUs transmission failures.
Invalid Format Packets Received	Displays the number of ISDP PDUs in invalid format received.
Table Full	Displays the number of ISDP entry table overflows.
ISDP IP Address Table Full	Displays the number of times ISDP IP address table was full.

Table 3-45. Management > ISDP > Statistics (Continued)

Parameter	Description
Clear	Click Clear to refresh the ISDP Statistics of all the interfaces.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.3.15 LLDP

Global Configuration

This section describes how to configure the Link Layer Discovery Protocol (LLDP). The LLDP is a one-way, device discovery protocol that transmits attributes between devices for the purpose of discovering the devices on the network.

To access this page, click **Management > LLDP > Global Configuration**.

LLDP Global Configuration

Transmit Interval	<input type="text" value="30"/>	(5 to 32768 secs)
Transmit Hold Multiplier	<input type="text" value="4"/>	(2 to 10 secs)
Re- Initialization Delay	<input type="text" value="2"/>	(1 to 10 secs)
Notification Interval	<input type="text" value="5"/>	(5 to 3600 secs)

Figure 3-48. Management > LLDP > Global Configuration

The following table describes the items in the previous menu.

Table 3-46. Management > LLDP > Global Configuration

Parameter	Description
Transmit Interval	Enter the interval in seconds to transmit LLDP frames. The range is from 5 to 32768 secs. Default value is 30 seconds.
Transmit Hold Multiplier	Enter the multiplier on Transmit Interval to assign TTL. The range is from 2 to 10 secs Default value is 4.
Re-Initialization Delay	Enter the delay before re-initialization. The range is from 1 to 10 secs. Default value is 2 seconds.
Notification Interval	Enter the interval in seconds for transmission of notifications. The range is from 5 to 3600 secs. Default value is 5 seconds.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Configuration

This section describes the configuration function for the LLDP interface. The following inter-face allows you to define the ports authorized to service LLDP.

To access this page, click **Management > LLDP > Interface Configuration**.

LLDP Interface Configuration

Figure 3-49. Management > LLDP > Interface Configuration

The following table describes the items in the previous menu.

Table 3-47. Management > LLDP > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select an LLDP - 802.1AB interface to configured.
Transmit	Click the drop-down menu to enable or disable the LLDP - 802.1AB transmit mode for the selected interface.
Receive	Click the drop-down menu to enable or disable the LLDP - 802.1AB receive mode for the selected interface.
Notify	Click the drop-down menu to enable or disable the LLDP - 802.1AB notification mode for the selected interface.
Transmit Management Information	Click the box to transmit the address in LLDP frames for the selected interface.
Optional TLV(s)	Click the related box to transmit any of the following: <ul style="list-style-type: none"> • System Name - To include system name TLV in LLDP frames. • System Description - To include system description TLV in LLDP frames. • System Capabilities - To include system capability TLV in LLDP frames. • Port Description - To include port description TLV in LLDP frames.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Status

The Interface Status screen displays the current state of the data within the switch.

To access this page, click **Management > LLDP > Interface Status**.

LLDP Interface Summary

TLV Codes: 0- Port Description, 1- System Name, 2- System Description, 3- System Capabilities

Interface	Link Status	Transmit	Receive	Notify	Optional TLV(s)	Transmit Management Information
ge0/1	Down	Disable	Disable	Disable		Nc
ge0/2	Down	Disable	Disable	Disable		Nc
ge0/3	Down	Disable	Disable	Disable		Nc
ge0/4	Down	Disable	Disable	Disable		Nc
ge0/5	Down	Disable	Disable	Disable		Nc
ge0/6	Down	Disable	Disable	Disable		Nc
ge0/7	Down	Disable	Disable	Disable		Nc
ge0/8	Up	Disable	Disable	Disable		Nc
ge0/9	Down	Disable	Disable	Disable		Nc
ge0/10	Down	Disable	Disable	Disable		Nc
ge0/11	Down	Disable	Disable	Disable		Nc
ge0/12	Down	Disable	Disable	Disable		Nc
ge0/13	Down	Disable	Disable	Disable		Nc
ge0/14	Down	Disable	Disable	Disable		Nc
ge0/15	Down	Disable	Disable	Disable		Nc
ge0/16	Down	Disable	Disable	Disable		Nc

Refresh

Figure 3-50. Management > LLDP > Interface Status

The following table describes the items in the previous menu.

Table 3-48. Management > LLDP > Interface Status

Parameter	Description
Interface	Displays the port on which LLDP - 802.1AB is configured.
Link Status	Displays the Link Status of the ports whether it is Up/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)	Displays the LLDP - 802.1AB optional TLV(s) that are included.
Transmit Management Information	Displays the selected option to transmit in LLDP frames.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Statistics

The Statistics page displays non-configurable data about the LLDP function.

To access this page, click **Management > LLDP > Statistics**.

LLDP Statistics



Figure 3-51. Management > LLDP > Statistics

The following table describes the items in the previous menu.

Table 3-49. Management > LLDP > Statistics

Parameter	Description
Last Update	Displays the time when an entry was created, modified or deleted in the tables associated with the remote system.
Total Inserts	Displays the number of times the complete set of information advertised by a particular MAC Service Access Point (MSAP) has been inserted into tables associated with the remote systems.
Total Deletes	Displays 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 the remote systems.
Total Drops	Displays the number of times the 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 the 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 timeliness interval has expired.
Interface	Displays the Slot/Port for the interfaces.
Transmit Total	Displays the number of LLDP frames transmitted by the LLDP agent on the corresponding port.
Receive Total	Displays the number of valid LLDP frames received by this 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 the remote entries because information timeliness interval had expired.

Table 3-49. Management > LLDP > Statistics (Continued)

Parameter	Description
TLV Discards	Displays the number of LLDP TLVs 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.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.
Clear	Click Clear to refresh LLDP Statistics of all the interfaces.

Local Device Information

The Local Device Information allows for the selection of interfaces to support LLDP and non-configurable data.

To access this page, click **Management > LLDP > Local Device Information**.

LLDP Local Device Information

No local interfaces are enabled to transmit LLDP data.

Figure 3-52. Management > LLDP > Local Device Information

The following table describes the items in the previous menu.

Table 3-50. Management > LLDP > Local Device Information

Parameter	Description
Interface	Displays 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 describes the source of the port identifier.
Port ID	Displays the string that describes the source of the port identifier.
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 description of the selected port associated with the local system.

Table 3-50. Management > LLDP > Local Device Information (Continued)

Parameter	Description
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	Displays the type of the management address.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Local Device Summary

The Local Device Summary displays LLDP non-configurable data: interface, port ID, and port description.

To access this page, click **Management > LLDP > Local Device Summary**.

LLDP Local Device Summary

Interface	Port ID	Port Description
Refresh		

Figure 3-53. Management > LLDP > Local Device Summary

The following table describes the items in the previous menu.

Table 3-51. Management > LLDP > Local Device Summary

Parameter	Description
Interface	Displays the ports on which LLDP - 802.1AB frames can be transmitted.
Port ID	Displays the port identifier associated with the local Interface.
Port Description	Displays the description of the port associated with the local system.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Remote Device Information

The Remote Device Information screen displays the ports configured to receive LLDP frames and non-configurable data.

To access this page, click **Management > LLDP > Remote Device Information**.

LLDP Remote Device Information

No local interfaces are enabled to receive LLDP data.

Figure 3-54. Management > LLDP > Remote Device Information The following table describes the items in the previous menu.

Table 3-52. Management > LLDP > Remote Device Information

Parameter	Description
Interface	Displays all the ports which can receive LLDP frames.
Remote ID	Displays the remote client identifier assigned to the remote system.
Chassis ID	Displays the chassis component associated with the remote system.
Chassis ID Subtype	Displays the source of the chassis identifier.
Port ID	Displays the port component associated with the remote system.
Port ID Subtype	Displays the source of port identifier.
System Name	Displays the system name of the remote system.
System Description	Displays the description of the given port associated with the remote system.
Port Description	Displays the description of the given port associated with the remote system.
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.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Remote Device Summary

The Remote Device Summary screen displays non-configurable remote information. To access this page, click **Management > LLDP > Remote Device Summary**.

LLDP Remote Device Summary

Interface	Remote ID	Chassis ID	Port ID	System Name
-----------	-----------	------------	---------	-------------

Refresh Clear

Figure 3-55. Management > LLDP > Remote Device Summary

The following table describes the items in the previous menu.

Table 3-53. Management > LLDP > Remote Device Summary

Parameter	Description
Interface	Displays the local port which can receive LLDP frames advertised by a remote system.
Remote ID	Displays the remote client identifier assigned to the remote system.
Chassis ID	Displays the chassis component associated with the remote system.
Port ID	Displays the port component associated with the remote system.
System Name	Displays the system name of the remote system.
Refresh	Displays the data on the screen with the present state of the data in the switch.
Clear	Click Clear to refresh LLDP Remote Device information received on all the interfaces.

LLDP-MED

Global Config

Global Configuration allows users to specify the number of LLDP PDUs that can be transmitted when the protocol is enabled.

To access this page, click **Management > LLDP > LLDP-MED > Global Config**.

LLDP-MED Global Config

Fast Start Repeat Count (: to 10)

Device Class

Figure 3-56. Management > LLDP > LLDP-MED > Global Config The following table describes the items in the previous menu.

Table 3-54. Management > LLDP > LLDP-MED > Global Config

Parameter	Description
Fast Start Repeat Count	Enter the number of LLDP PDUs that will be transmitted when the protocol is enabled. The range is from 1 to 10. Default value of fast repeat count is 3.
Device Class	Displays the local device's MED Classification. There are four different kinds of devices, three of them represent the actual end points (classified as 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.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Configuration

Interface Configuration allows the selection of configurable ports supporting LLDP-MED ports, the enabling of LLDP-MED mode and notification mode in addition to selecting of TLV type value lengths.

To access this page, click **Management > LLDP > LLDP-MED > Interface Configuration**.

LLDP-MED Interface Configuration

Figure 3-57. Management > LLDP > LLDP-MED > Interface Configuration

The following table describes the items in the previous menu.

Table 3-55. Management > LLDP > LLDP-MED > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the LLDP-MED - 802.1ab interface to configured. 'All' option is provided to configure all interfaces on the DUT and to be consistent with CLI. To view the summary of all interfaces refer to 'Interface Summary' webpage. Interface configuration page will not be able to display summary of 'All' interfaces, summary of individual interfaces is visible from 'Interface Configuration' webpage. 'Interface Configuration' webpage for 'All' option will always display LLDP-MED mode and notification mode as 'disabled' and checkboxes for 'Transmit TLVs' will always be unchecked.
LLDP-MED Mode	Click the drop-down menu to enable or disable the Link Layer Discovery Protocol-Media Endpoint Discovery(LLDP-MED) mode for the selected interface. By enabling MED, we will be effectively enabling the transmit and receive function of LLDP.
Config Notification Mode	Click the drop-down menu to enable or disable the LLDP-MED topology notification mode for the selected interface.
Transmit TLVs	Click an option to select a type length values (TLVs) in the LLDP-MED will be transmitted in the LLDP PDUs frames for the selected interface. <ul style="list-style-type: none"> • MED Capabilities - To transmit the capabilities TLV in LLDP frames. • Network Policy - To transmit the network policy TLV in LLDP frames.
Submit	Click Submit to update to the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Status

Interface Status displays a summary of non-configurable data for the LLDP-MED function.

To access this page, click **Management > LLDP > LLDP-MED > Interface Status**.

LLDP-MED Interface Summary

TLV Codes: 0- Capabilities, 1- Network Policy, 2- Location, 3- Extended PSE, 4- Extended Pd, 5- Inventory

Interface	Link Status	MED Status	Operational Status	Notification Status	Transmit TLVs
ge3/1	Down	Disable	Disable	Disable	0, 1
ge3/2	Down	Disable	Disable	Disable	0, 1
ge3/3	Down	Disable	Disable	Disable	0, 1
ge3/4	Down	Disable	Disable	Disable	0, 1
ge3/5	Down	Disable	Disable	Disable	0, 1
ge3/6	Down	Disable	Disable	Disable	0, 1
ge3/7	Down	Disable	Disable	Disable	0, 1
ge3/8	Up	Disable	Disable	Disable	0, 1
ge3/9	Down	Disable	Disable	Disable	0, 1
ge3/10	Down	Disable	Disable	Disable	0, 1
ge3/11	Down	Disable	Disable	Disable	0, 1
ge3/12	Down	Disable	Disable	Disable	0, 1
ge3/13	Down	Disable	Disable	Disable	0, 1
ge3/14	Down	Disable	Disable	Disable	0, 1
ge3/15	Down	Disable	Disable	Disable	0, 1
ge3/16	Down	Disable	Disable	Disable	0, 1

Refresh

Figure 3-58. Management > LLDP > LLDP-MED > Interface Status

The following table describes the items in the previous menu.

Table 3-56. Management > LLDP > LLDP-MED > Interface Status

Parameter	Description
Interface	Displays all the ports on which LLDP-MED can be configured.
Link Status	Displays the link status of the ports whether it is Up/Down.
MED Status	Displays the LLDP-MED mode is enabled or disabled on this interface.
Operational Status	Displays the LLDP-MED TLVs are transmitted or not on this interface.
Notification Status	Displays the LLDP-MED topology notification mode of the interface.
Transmit TLV(s)	Displays the LLDP-MED transmit TLV(s) that are included.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Local Device Information

Interface Device Information allows for the selection of ports which can transmit LLDP-MED frames.

To access this page, click **Management > LLDP > LLDP-MED > Local Device Information**.

LLDP-MED Local Device Information

Local interfaces are not enabled to transmit LLDP-MED data

Figure 3-59. Management > LLDP > LLDP-MED > Local Device Information

The following table describes the items in the previous menu.

Table 3-57. Management > LLDP > LLDP-MED > Local Device Information

Parameter	Description
Interface	Displays the list of all the ports on which LLDP-MED frames can be transmitted.
Network Policy Information	<p>Specifies if network policy TLV is present in the LLDP frames.</p> <ul style="list-style-type: none"> ● Media Application Type - Specifies the application type. Types of application types are unknown, voice signalling, guest voice, guest voice signalling, soft-phone voice, video conferencing, streaming video, video signalling. Each application type that is received has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been transmitted only then would this information be displayed. ● VLAN ID - Specifies the VLAN ID associated with a particular policy type. ● Priority - Specifies the priority associated with a particular policy type. ● DSCP - Specifies the DSCP associated with a particular policy type. ● Unknown Bit Status - Specifies the unknown bit associated with a particular policy type. ● Tagged Bit Status - Specifies the tagged bit associated with a particular policy type.
Location Information	<p>Displays if location information TLV is present in the LLDP frames.</p> <ul style="list-style-type: none"> ● SubType - Specifies the location subtype advertised by the local device. The possible values are: <ul style="list-style-type: none"> ● Unknown ● Coordinate Based ● Civic Address ● ELIN ● Info - Specifies the location information of the SubType.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Remote Device Information

Remote Device Information allows for the selection of ports that support the enabling of LLDP-MED. The page also displays remote client non-configurable data.

To access this page, click **Management > LLDP > LLDP-MED > Remote Device Information**.

LLDP-MED Remote Device Information

Local Interface All ▼

Remote ID

Capability Information

Supported Capabilities

Enabled Capabilities

Device Class

Network Policy Information

Media Application Type	VLAN ID	Priority	DSCP	Unknown Bit Status	Tagged Bit Status
------------------------	---------	----------	------	--------------------	-------------------

Inventory Information

Hardware Revision

Firmware Revision

Software Revision

Serial Number

Manufacturer Name

Model Name

Asset ID

Location Information

Sub Type	Location Information
----------	----------------------

Extended PoE

Figure 3-60. Management > LLDP > LLDP-MED > Remote Device Information

The following table describes the items in the previous menu.

Table 3-58. Management > LLDP > LLDP-MED > Remote Device Information

Parameter	Description
Local Interface	Click the drop-down menu to list of all the ports on which LLDP-MED is enabled.
Remote ID	Displays the remote client identifier assigned to the remote system.
Capability Information	<p>Displays the supported and enabled capabilities that was received in MED TLV on this port.</p> <ul style="list-style-type: none"> Supported Capabilities - Specifies supported capabilities that was received in MED TLV on this port. Enabled Capabilities - Specifies enabled capabilities that was received in MED TLV on this port. Device Class - Specifies device class as advertised by the device remotely connected to the port.

Table 3-58. Management > LLDP > LLDP-MED > Remote Device Information (Continued)

Parameter	Description
Network Policy Information	<p>Displays the network policy TLV is received in the LLDP frames on this port.</p> <ul style="list-style-type: none"> ● Media Application Type - Specifies the application type. Types of application types are unknown, voice signalling, guest voice, guest voice signalling, soft-phone voice, video conferencing, streaming video, video signalling. Each application type that is received has the VLAN ID, priority, DSCP, tagged bit status and unknown bit status. A port may receive one or many such application types. If a network policy TLV has been receive on this port only then would this information be displayed. ● VLAN ID - Specifies the VLAN ID associated with a particular policy type. ● Priority - Specifies the priority associated with a particular policy type. ● DSCP - Specifies the DSCP associated with a particular policy type. ● Unknown Bit Status - Specifies the unknown bit associated with a particular policy type. ● Tagged Bit Status - Specifies the tagged bit associated with a particular policy type.
Inventory Information	<p>Displays the inventory TLV is received in LLDP frames on this port.</p> <ul style="list-style-type: none"> ● Hardware Revision - Specifies hardware version of the remote device. ● Firmware Revision - Specifies Firmware version of the remote device. ● Software Revision - Specifies Software version of the remote device. ● Serial Number - Specifies serial number of the remote device. ● Manufacturer Name - Specifies manufacturers name of the remote device. ● Model Name - Specifies model name of the remote device. ● Asset ID - Specifies asset ID of the remote device.
Location Information	<p>Displays location TLV is received in LLDP frames on this port.</p> <ul style="list-style-type: none"> ● Sub Type - Specifies type of location information. ● Location Information - Specifies the location information as a string for given type of location id.
Extended PoE	<p>Specifies if remote device is a PoE device.</p> <ul style="list-style-type: none"> ● Device Type - Specifies remote device's PoE device type connected to this port.
Extended PoE PSE	<p>Displays extended PSE TLV is received in LLDP frame on this port.</p> <ul style="list-style-type: none"> ● Available - Specifies the remote ports PSE power value in tenths of watts. ● Source - Specifies the remote ports PSE power source. ● Priority - Specifies the remote ports PSE power priority.

Table 3-58. Management > LLDP > LLDP-MED > Remote Device Information (Continued)

Parameter	Description
Extended PoE PD	Displays extended PD TLV is received in LLDP frame on this port. <ul style="list-style-type: none"> Required - Specifies the remote port's PD power requirement. Source - Specifies the remote port's PD power source. Priority - Specifies the remote port's PD power priority.
Refresh	Refresh the data on the screen with the present state of the data in the switch.

3.3.16 TACACS+

Configuration

The Configuration page allows users to configure key string and connection timeout settings for TACACS+. To access this page, click **Management > TACACS+ > Configuration**.

TACACS+ Configuration

The screenshot shows the TACACS+ Configuration page. It features two input fields: 'Key String' with a placeholder '(0 to 120 characters)' and an 'Apply' checkbox, and 'Connection Timeout' with a value of '5' and a placeholder '(1 to 30 secs)'. A 'Submit' button is located below the fields.

Figure 3-61. Management > TACACS+ > Configuration

The following table describes the items in the previous menu.

Table 3-59. Management > TACACS+ > Configuration

Parameter	Description
Key String	Enter 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.
Apply	Click Apply to enter the key in the Key String field. If the checkbox is not checked, you will not be able to enter the key. By default its unchecked.
Connection Timeout	Enter the maximum number of seconds allowed to establish a TCP connection between the device and the TACACS+ server. The default value is 5 seconds. The valid range is 1 to 30.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Server Configuration

The Server Configuration page allows users to configure settings for TACACS+ servers. To access this page, click **Management > TACACS+ > Server Configuration**.

TACACS+ Server Configuration

The screenshot shows a web interface for configuring TACACS+ servers. At the top, there is a label 'TACACS+ Server' and a dropdown menu with 'ADD' selected. Below this is a text input field for 'Server Address' with a placeholder '(Max 255 characters/X.X.X.X)'. At the bottom of the form is a 'Submit' button.

Figure 3-62. Management > TACACS+ > Server Configuration

The following table describes the items in the previous menu.

Table 3-60. Management > TACACS+ > Server Configuration

Parameter	Description
TACACS+ Server	Click the drop-down menu to select the TACACS+ server for which data is to be displayed or configured. If the add item is selected, a new TACACS server can be configured.
Server Address	Enter the TACACS+ Server IP address or Hostname. Hostnames are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 255 characters.
Priority	Enter the order in which the TACACS+ servers are used. Default value is 0. It should be within the range 0-65535.
Port	Enter the authentication port. Default value is 49. It should be within the range 0-65535.
Key String	Enter the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. The valid range is 0-128 characters. Default is blank. The key must match the encryption used on the TACACS+ server.
Apply	Click Apply to submit the key in the Key String field. If the checkbox is not checked, you will not be able to enter the key. By default its unchecked.
Connection Timeout	Enter the time to allot the amount of time that passes before the connection between the device and the TACACS+ server time out. The range is 1 to 30. Default value is 5. Enter 0 to set it to default value.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Remove	Click Remove to delete the selected server from the configuration.

3.3.17 RADIUS

Configuration

The configuration page allows users to view and configure various settings for the RADIUS servers configured on the system. To access this page, click **Management > RADIUS > Configuration**.

RADIUS Configuration

Number of Configured Authentication Servers	1
Number of Configured Accounting Servers	1
Number of Named Authentication Server Groups	1
Number of Named Accounting Server Groups	1
Max Number of Retransmits	<input type="text" value="4"/> (: to 15)
Timeout Duration (secs)	<input type="text" value="5"/> (: to 30)
Accounting Mode	<input type="text" value="Disable"/>
Enable RADIUS Attribute 4 (NAS IP Address)	<input type="checkbox"/>
NAS-IP Address	<input type="text" value="0.0.0.0"/> (X.X.X.X)

Figure 3-63. Management > RADIUS > Configuration

The following table describes the items in the previous menu.

Table 3-61. Management > RADIUS > Configuration

Parameter	Description
Number of Configured Authentication Servers	Displays the number of configured Authentication RADIUS servers. The value can range from 0 to 32.
Number of Configured Accounting Servers	Displays the number of RADIUS Accounting Servers configured. The value can range from 0 to 32.
Number of Named Authentication Server Groups	Displays the number of Named RADIUS server Authentication groups configured.
Number of Named Accounting Server Groups	Displays the number of Named RADIUS server Accounting groups configured.
Max Number of Retransmits	Enter the value for 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.

Table 3-61. Management > RADIUS > Configuration (Continued)

Parameter	Description
Timeout Duration (secs)	Enter the timeout value, in seconds, for request retransmissions. The valid range is 1 - 30. Default value is 5. See the Max Number of Retransmits field description for more information about configuring the timeout duration.
Accounting Mode	Click the drop-down menu to select whether the RADIUS accounting mode is enabled or disabled on the current server. By default it is disabled.
Enable RADIUS Attribute 4 (NAS-IP Address)	Click the box 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. By default this mode is disabled.
NAS-IP Address	Enter the NAS-IP Address of the RADIUS authentication client referred to in this table entry. By default it is not configured.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to clear the database and display it again starting with the first entry in the table.

Server Configuration

The Server Configuration page allows users to view and configure RADIUS Server. To access this page, click **Management > RADIUS > Server Configuration**.

RADIUS Server Configuration

RADIUS Server Host Address	admin	
Port	1812	(1 to 55555)
Secret		
Primary Server	No	
Message Authenticator	Enable	
Secret Configured	No	
Current	Yes	
RADIUS Server Name	Default RADIUS Server	(0 to 32 characters)

Submit Remove Refresh

Figure 3-64. Management > RADIUS > Server Configuration

The following table describes the items in the previous menu.

Table 3-62. Management > RADIUS > Server Configuration

Parameter	Description
RADIUS Server Host Address	Click the drop-down menu to select the IP Address or Hostname of the configured RADIUS server. Hostnames are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire host-name has a maximum of 255 characters. This object cannot be changed after creation.
Port	Enter 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	Enter the pass phrase for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This secret must match the RADIUS encryption. <ul style="list-style-type: none"> 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	Click the drop-down menu to set the selected server to the Primary (Yes) or Secondary (No) server. If you configure multiple RADIUS servers with the same RADIUS 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. If the server is not set as Primary, by default it is set as Secondary.
Message Authenticator	Click the drop-down menu to enable or disable the message authenticator attribute for the selected server. By default this mode is enable for the selected server.
Secret Configured	Displays the shared secret configuration status. Indicates whether the shared secret for this server has been configured. By default the secret key will not be set for the server.
Current	Displays the current status of the selected RADIUS server (Yes, current: No, backup). 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 configured, the current server is the most recently configured RADIUS server.
RADIUS Server Name	Enter the RADIUS server name. To change the name, enter up to 31 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.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Table 3-62. Management > RADIUS > Server Configuration (Continued)

Parameter	Description
Remove	Click Remove 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.
Refresh	Click Refetch to the database and display it again starting with the first entry in the table.

Named Server Status

The Named Server Status displays information about the RADIUS servers configured on the system. To access this page, click **Management > RADIUS > Named Server Status**.

RADIUS Named Server Status

Current	RADIUS Server IP Address	RADIUS Server Name	Port Number	Server Type	Secret Configured	Message Authenticator
True	admin	Default-RADIUS-Server	1812	Secondary	No	Enable

Figure 3-65. Management > RADIUS > Named Server Status

The following table describes the items in the previous menu.

Table 3-63. Management > RADIUS > Named Server Status

Parameter	Description
Current	Displays whether the selected RADIUS server is the current server (True) or a backup server (False). 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 configured, the current server is the most recently configured RADIUS server.
RADIUS Server IP Address	Displays the IP address of the RADIUS server.
RADIUS Server Name	Displays 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	Displays the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.
Server Type	Displays the server status: Primary or Secondary server.
Secret Configured	Displays the configuration status of the shared secret (pass phrase) for this server.

Table 3-63. Management > RADIUS > Named Server Status (Continued)

Parameter	Description
Message Authenticator	Displays the status (enabled or disabled) for the message authenticator attribute for the selected server.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Server Statistics

The Server Statistics page displays statistical information for each RADIUS server configured on the system. To access this page, click **Management > RADIUS > Server Statistics**.

RADIUS Server Statistics

RADIUS Server Host Address	admin
Round Trip Time (secs)	0.00
Access Requests	0
Access Retransmissions	0
Access Accepts	0
Access Rejects	0
Access Challenges	0
Malformed Access Responses	0
Bad Authenticators	0
Pending Requests	0
Timeouts	0
Unknown Types	0
Packets Dropped	0

Figure 3-66. Management > RADIUS > Server Statistics

The following table describes the items in the previous menu.

Table 3-64. Management > RADIUS > Server Statistics

Parameter	Description
RADIUS Server Host Address	Click the drop-down menu to select the IP address of the RADIUS server for which statistics are to be displayed.
Round Trip Time (secs)	Displays 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	Displays the number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	Displays the number of RADIUS Access-Request packets retransmitted to this server.
Access Accepts	Displays the number of RADIUS Access-Accept packets, including both valid and invalid packets, that were received from this server.
Access Rejects	Displays the number of RADIUS Access-Reject packets, including both valid and invalid packets, that were received from this server.
Access Challenges	Displays the number of RADIUS Access-Challenge packets, including both valid and invalid packets, that were received from this server.

Table 3-64. Management > RADIUS > Server Statistics (Continued)

Parameter	Description
Malformed Access Responses	Displays 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	Displays the number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	Displays the number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	Displays the number of authentication timeouts to this server.
Unknown Types	Displays the number of RADIUS packets of unknown type which were received from this server on the authentication port.
Packets Dropped	Displays the number of RADIUS packets received from this server on the authentication port and dropped for some other reason.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Accounting Server Configuration

The RADIUS Accounting Server Configuration page allows users to view and configure various settings for the current RADIUS accounting servers configured on the system. To access this page, click **Management > RADIUS > Accounting Server Configuration**.

RADIUS Accounting Server Configuration

Accounting Server Host Address: admin

Port: 1813 (1 to 65535)

Secret: (Max 16 characters) Apply

Secret Configured: False

RADIUS Accounting Server Name: Default-RADIUS-Server (Max 31 characters)

Submit Remove Refresh

Figure 3-67. Management > RADIUS > Accounting Server Configuration

The following table describes the items in the previous menu.

Table 3-65. Management > RADIUS > Accounting Server Configuration

Parameter	Description
Accounting Server Host Address	Click the drop-down menu to select the IP address of the accounting server to view or configure. Select Add to configure additional RADIUS servers.
Host Address	Enter the IP Address or Hostname of the configured Accounting RADIUS server. Hostnames are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire hostname has a maximum of 255 characters. This object cannot be changed after creation.

Table 3-65. Management > RADIUS > Accounting Server Configuration (Continued)

Parameter	Description
Port	Displays 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	Enter the pass phrase to use with the specified accounting server. This field is only displayed if you are logged into the switch with READWRITE access. The name contain up to 16 characters. <ul style="list-style-type: none"> 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.
Secret Configured	Displays the configuration status of the shared pass phrase. By default the secret key will not be set for the server.
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 cannot use the same name for multiple RADIUS accounting servers.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Remove	Click Remove 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.
Refresh	Click Refresh to update the database and display it again starting with the first entry in the table.

Named Accounting Server Status

The Named Accounting Server Status page displays information about the accounting serv-ers configured on the system. To access this page, click **Management > RADIUS > Named Accounting Server Status**.

RADIUS Named Accounting Server Status

RADIUS Accounting Server Name	IP Address	Port Number	Secret Configured
Default-RADIUS-Server	admin	1813	False

Refresh

Figure 3-68. Management > RADIUS > Named Accounting Server Status

The following table describes the items in the previous menu.

Table 3-66. Management > RADIUS > Named Accounting Server Status

Parameter	Description
RADIUS Accounting Server Name	Displays 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	Displays the IP address of the RADIUS server.
Port Number	Displays the authentication port the server uses to verify the RADIUS server authentication. The port is a UDP port.
Secret Configured	Displays the configuration status of the shared secret for this server.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Accounting Server Statistics

The Accounting Server Statistics page displays statistical information for each RADIUS server configured on the system. To access this page, click **Management > RADIUS > Accounting Server Statistics**.

RADIUS Accounting Server Statistics



Figure 3-69. Management > RADIUS > Accounting Server Statistics

The following table describes the items in the previous menu.

Table 3-67. Management > RADIUS > Accounting Server Statistics

Parameter	Description
Accounting Server Host Address	Click 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	Displays the number of RADIUS Accounting-Request packets sent to this server. This number does not include retransmissions.

Table 3-67. Management > RADIUS > Accounting Server Statistics (Continued)

Parameter	Description
Accounting Retransmissions	Displays 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 contained invalid authenticators received from this accounting server.
Pending Requests	Displays the number of RADIUS Accounting-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	Displays the number of accounting timeouts to this server.
Unknown Types	Displays the number of RADIUS packets of unknown type which were received from this server on the accounting port.
Packets Dropped	Displays the number of RADIUS packets received from this server on the accounting port and dropped.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Clear Statistics

The Clear Statistics page allows users to reset all RADIUS authentication and accounting statistics to zero. To access this page, click **Management > RADIUS > Clear Statistics**.

RADIUS Clear Statistics

Clear All RADIUS Statistics

Clear

Figure 3-70. Management > RADIUS > Clear Statistics

The following table describes the items in the previous menu.

Table 3-68. Management > RADIUS > Clear Statistics

Parameter	Description
Clear	Clears all statistics for the RADIUS authentication and accounting server.

3.3.18 ARP Table

The Address Resolution Protocol (ARP) dynamically maps physical (MAC) addresses to Internet (IP) addresses. This panel displays the current contents of the ARP cache.

To access this page, click **Management > ARP Table**.

System ARP Cache

MAC Address	IP Address	Slot/Port
E0:FD:49:70:12:C5	192.168.1.60	ge0/8

Figure 3-71. Management > ARP Table

The following table describes the items in the previous menu.

Table 3-69. Management > ARP Table

Parameter	Description
MAC Address	Displays the associated physical (MAC) Address for the connection.
IP Address	Displays the IP address of the connection.
Slot/Port	Displays the port being used for the connection.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.
Clear	Click Clear to refresh the Management ARP Cache in the switch.

3.3.19 Reset Button

Reset Button allows for function definition associated with the reset button. The following functions are available: firmware-upload, startup-config, factory-default or reboot.

To access this page, click **Management > Reset Button**.

Reset Button Setting

Index:

Feature Description:

EnableOrNot:

Index	Feature Description	EnableOrNot
0	firmware-upload	Disable
1	startup-config	Disable
2	factory-default	Disable
3	reboot	Disable

Figure 3-72. Management > Reset Button

The following table describes the items in the previous menu.

Table 3-70. Management > Reset Button

Parameter	Description
Index	Click the drop-down menu to select an index number (0-3) to associated with a specific function on the reset button function.
Feature Description	Displays the index selection definition.
EnableOrNot	Click the drop-down menu to enable or disable the selected index function.
Submit	Click Submit to accept the updates to the settings.
Index	Displays the Index number associated with the rest button setting.
Feature Description	Displays the function definition for the reset button setting.
EnableOrNot	Displays the enabled state of the function.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.3.20 Login Sessions

The Login Sessions page displays a summary of all login information for all users. To access this page, click **Management > Login Sessions**.

Login Sessions

ID	User Name	Connection From	Idle Time	Session Time	Session Type
11	admin	:92.168.1.60	00:00:00	00:11:20	HTTP

Figure 3-73. Management > Login Sessions

The following table describes the items in the previous menu.

Table 3-71. Management > Login Sessions

Parameter	Description
ID	Displays the ID of this row.
User Name	Displays the user name of user made the session.
Connection From	Displays the user is connected from which machine.
Idle Time	Displays the idle session time.
Session Time	Displays the total session time.
Session Type	Displays the type of session: Telnet, Serial, SSH, HTTP or HTTPS.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.4. Switching

3.4.1 MAC Address Table

Aging Timer

Configuration

The Aging Timer Configuration page allows users to set the Address Aging Timeout for the forwarding database. To access this page, click **Switching > MAC Address Table > Aging Timer > Configuration**.

Forwarding Database Configuration

Aging Interval (secs) (10 to 1000000)

Figure 3-74. Switching > MAC Address Table > Aging Timer >

Configuration The following table describes the items in the previous menu.

Table 3-72. Switching > MAC Address Table > Aging Timer > Configuration

Parameter	Description
Aging Interval (secs)	Enter 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. You specify that time by entering a value for the Address Aging Timeout. You may enter any number of seconds between 10 and 1000000. IEEE 802.1D recommends a default of 300 seconds, which is the factory default.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

MAC Filtering

Configuration

The MAC Filtering Configuration page allows users to configure the MAC filter settings. To access this page, click **Switching > MAC Address Table > MAC Filtering > Configuration**.

MAC Filter Configuration

MAC Filter

VLAN ID

MAC Address

Source Port Members

Destination Port Members

Figure 3-75. Switching > MAC Address Table > MAC Filtering > Configuration

The following table describes the items in the previous menu.

Table 3-73. Switching > MAC Address Table > MAC Filtering > Configuration

Parameter	Description
MAC Filter	Click the drop-down menu to list of created MAC address entries or create a new entry. To change the port mask(s) for an existing filter, select the entry you want to change. To add a new filter, select "Create" from the top of the list.
VLAN ID	Click the drop-down menu to select the VLAN ID to associate with the selected MAC address to fully identify packets you want filtered. You can only change this field when you have selected the "Create" option.
MAC Address	Enter 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" option. You cannot define filters for these MAC addresses: <ul style="list-style-type: none"> • 00:00:00:00:00:00 • 01:80:C2:00:00:00 to 01:80:C2:00:00:0F • 01:80:C2:00:00:20 to 01:80:C2:00:00:21 • FF:FF:FF:FF:FF:FF
Source Port Members	Select the source port to include in the inbound filter. If a packet with the MAC address and VLAN ID you selected is received on a port that is not in the list, it will be dropped.
Destination Port Members	Select the destination port to include in the outbound filter. Packets with the MAC address and VLAN ID you selected will only be transmitted out of ports that are in the list.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Click Delete to remove the currently selected filter.
Delete All	Click Remove All to delete all create configured filters.

Status

The MAC Filter Summary page displays the VLAN ID and assigned source port members and destination member for each MAC address created. To view this page, click **Switching > MAC Address Table > MAC Filtering > Status**.

MAC Filter Summary

MAC Address	VLAN ID	Source Port Members	Destination Port Members
Refresh			

Figure 3-76. Switching > MAC Address Table > MAC Filtering > Status

The following table describes the items in the previous menu.

Table 3-74. Switching > MAC Address Table > MAC Filtering > Status

Parameter	Description
MAC Address	Displays the MAC address of the filter in the format 00:01:1A:B2:53:4D.
VLAN ID	Displays the VLAN ID associated with the filter.
Source Port Mem- bers	Displays the ports to be used for filtering inbound packets.
Destination Port Members	Displays the ports to which filtered packets can be forwarded.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Port Security

Global Configuration

The Port Security Administration page allows users to enable or disable the port security mode. To access this page, click **Switching > MAC Address Table > Port Security > Global Configuration**.

Port Security Administration

The screenshot shows a web interface for 'Port Security Administration'. It features a form with a label 'Port Security Mode' and a dropdown menu currently displaying 'Disable'. Below the form is a 'Submit' button.

Figure 3-77. Switching > MAC Address Table > Port Security > Global

Configuration The following table describes the items in the previous menu.

Table 3-75. Switching > MAC Address Table > Port Security > Global Configuration

Parameter	Description
Port Security Mode	Click the drop-down menu to enable or disable the port security feature.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Configuration

The Port Security Configuration page allows users to configure port security for each interface. To access this page, click **Switching > MAC Address Table > Port Security > Interface Configuration**.

Port Security Interface Configuration

The screenshot shows the 'Port Security Interface Configuration' form. It contains the following fields and values:

- Interface: ge0/1
- Port Security: Disable
- Maximum Number of Dynamically Learned MAC Addresses Allowed: 600 (range: 0 to 600)
- Maximum Number of Statically Locked MAC Addresses Allowed: 20 (range: 0 to 20)
- Add a Static MAC Address: 0C:00:00:00:00:00 (checkbox: checked)
- VLAN ID: 1 (range: 1 to 4093)
- Enable Violation Traps: No
- Enable Sticky Mode: No
- Convert dynamically learned address to statically locked: Move

A 'Submit' button is located at the bottom center of the form.

Figure 3-78. Switching > MAC Address Table > Port Security > Interface Configuration

The following table describes the items in the previous menu.

Table 3-76. Switching > MAC Address Table > Port Security > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the interface to be configured.
Port Security	Click the drop-down menu to enable or disable the port security feature for the selected interface. It is disabled by default.
Maximum Number of Dynamically Learned MAC Address Allowed	Enter the maximum number of dynamically learned MAC addresses on the selected interface. Valid range is 0 to 600. Default value is 600.
Maximum Number of Statically Locked MAC Address Allowed	Enter the maximum number of statically locked MAC addresses on the selected interface. Valid range is 0 to 20. Default value is 20.
Add a Static MAC Address	Enter the static MAC address. Set the checkbox to add a MAC address to the list of statically locked MAC addresses for the selected interface.
VLAN ID	Enter the VLAN ID number to add to the list of statically locked MAC addresses for the selected interface. Valid range is 1 to 4093.
Enable Violation Traps	Click the drop-down menu to enable or disable 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.
Enable Sticky Mode	Click the drop-down menu to enable or disable sticky learning on the interface.
Convert dynamically learned address to statically locked	Click Move to convert dynamic MAC address entries to Static MAC address entries. Shows "Static Limit Reached. No Dynamic Addresses will be moved." when added Static MAC entries reaches to configured value of Maximum Number of Statically Locked MAC Addresses Allowed.

Table 3-76. Switching > MAC Address Table > Port Security > Interface Configuration (Continued)

Parameter	Description
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Static MAC Address

The Port Security Statically Configured MAC address page displays the MAC address and VLAN ID settings for each interface, and allows users to delete a static MAC address and assign VLAN IDs. To access this page, click **Switching > MAC Address Table > Port Security > Static MAC Address**.

Port Security Statically Configured MAC Addresses

Figure 3-79. Switching > MAC Address Table > Port Security > Static MAC Address The following table describes the items in the previous menu.

Table 3-77. Switching > MAC Address Table > Port Security > Static MAC Address

Parameter	Description
Interface	Click the drop-down menu to select the physical interface for which you want to display data.
MAC Address	Displays the user specified statically locked MAC address.
VLAN ID	Displays the VLAN ID corresponding to the MAC address.
Delete a static MAC Address	Click Delete to remove the MAC address from the Port-Security Static MAC address table.
VLAN ID	Enter the VLAN ID corresponding to the MAC address being deleted. Valid range is 1 to 4093.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Dynamic MAC Address

The Port Security Dynamically Learned MAC address page displays the MAC address, VLAN ID settings for each interface, and the number of dynamic MAC addresses learned.

To access this page, click **Switching > MAC Address Table > Port Security > Dynamic MAC Address**.

Port Security Dynamically Learned MAC Addresses

Interface

MAC Address	VLAN ID
Number Of Dynamic MAC Addresses Learned 0	

Figure 3-80. Switching > MAC Address Table > Port Security > Dynamic MAC Address
The following table describes the items in the previous menu.

Table 3-78. Switching > MAC Address Table > Port Security > Dynamic MAC Address

Parameter	Description
Interface	Click the drop-down menu to select the physical interface for which you want to display data.
MAC Address	Displays the MAC addresses learned on a specific port.
VLAN ID	Displays the VLAN ID corresponding to the MAC address.
Number Of Dynamic MAC Addresses Learned	Displays the number of dynamically learned MAC addresses on a specific port.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

MAC Violation Status

The Port Security Violation Status page displays the violation record for each interface. To access this page, click **Switching > MAC Address Table > Port Security > MAC Violation Status**.

Port Security Violation Status

Interface

Last Violation MAC Address	VLAN ID
----------------------------	---------

Figure 3-81. Switching > MAC Address Table > Port Security > MAC Violation Status

The following table describes the items in the previous menu.

Table 3-79. Switching > MAC Address Table > Port Security > MAC Violation Status

Parameter	Description
Interface	Click the drop-down menu to select the physical interface for which you want to display data.
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.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Forward Database

Use this panel to display information about entries in the forwarding database. These entries are used by the transparent bridging function to determine how to forward a received frame. To access this page, click **Switching > MAC Address Table > Forward Database**.

Forwarding Database Search

Filter All ▼

MAC Address Search

MAC address	Source Slot/Port(s)	Interface Index	Status
03:01:30:08:9B:BD 93:5E	geC/8	8	Learned
03:01:30:1F:D0:CC:4E AA	geC/8	8	Learned
03:01:30:24:1D:1C:53:7D	geC/8	8	Learned
03:01:30:24:1D:7F 34:05	geC/8	8	Learned
03:01:30:26:18:F1:7F:D6	geC/8	8	Learned
03:01:30:DC:C9:75:16:FF	CPU	17	Management
03:01:30:E0:2B:00:03:01	geC/8	8	Learned
03:01:1C:6F:65:28 35:44	geC/8	8	Learned
03:01:1C:6F:65:28 35:B6	geC/8	8	Learned
03:01:1C:6F:65:C8:B1:03	geC/8	8	Learned
03:01:1C:6F:65:C8:BB:4F	geC/8	8	Learned
03:01:50:E5:49:52:93:BF	geC/8	8	Learned
03:01:5C:FC:49:70 12:C5	geC/8	8	Learned
03:01:38:DC:96:16:A3 FB	geC/8	8	Learned

Figure 3-82. Switching > MAC Address Table > Forward Database

The following table describes the items in the previous menu.

Table 3-80. Switching > MAC Address Table > Forward Database

Parameter	Description
Management Unit	Displays management unit for which Forwarding Database Table is to be displayed.
Filter	Click the drop-down menu to select the entry to be displayed. <ul style="list-style-type: none"> Learned: If you choose "learn" only MAC addresses that have been learned will be displayed. All: If you choose "all" the whole table will be displayed.

Table 3-80. Switching > MAC Address Table > Forward Database (Continued)

Parameter	Description
MAC Address Search	Enter the MAC address and click Search to initiate a search. 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. Then click on the search button. If the address exists, that entry is displayed as the first entry followed by the remaining (greater) MAC addresses. An exact match is required.
Search	Click Search to initiate a specified MAC address search.
MAC Address	Displays a unicast MAC address for which the switch has forwarding and/or filtering information. The format is a two byte hexadecimal VLAN ID number followed by a six byte MAC address with each byte separated by colons. For example: 01:23:45:67:89:AB:CD:EF, where 01:23 is the VLAN ID and 45:67:89:AB:CD:EF is the MAC address.
Source Slot/Port(s)	Displays a port where this address was learned -- i.e. the port through which the MAC address can be reached.
Interface Index	Displays an Interface Index of the MIB interface table entry associated with the source port.
Status	<p>Displays the status of this entry. The possible values are:</p> <ul style="list-style-type: none"> ● Static: the entry was added when a static MAC filter was defined. ● Learned: the entry was learned by observing the source MAC addresses of incoming traffic, and is currently in use. ● Management: the system MAC address, which is identified with interface 0.1. ● Self: the MAC address of one of the switch's physical interfaces.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.4.2 Interface Setting

Configuration

The Port Configuration page allows users to configure the settings for each interface. To access this page, click **Switching > Interface Setting > Configuration**.

Port Configuration

The screenshot shows the 'Port Configuration' page with the following settings:

- Interface: gel/1
- Port Type: Normal
- STP Mode: Enable
- Admin Mode: Enable
- Broadcast Storm Recovery Mode: Disable
- Broadcast Storm Recovery Level: 5
- Multicast Storm Recovery Mode: Disable
- Multicast Storm Recovery Level: 5
- Unicast Storm Recovery Mode: Disable
- Unicast Storm Recovery Level: 5
- LACP Mode: Enable
- Physical Mode: Auto
- Physical Status: Unknown
- Link Status: Link Down
- Link Trap: Enable
- Maximum Frame Size: 1518 (Range: [1518-12286] Default: 1518)
- Interface Index: 1

There are three 'Unit' dropdown menus on the right side, each set to 'Percent'.

Figure 3-83. Switching > Interface Setting > Configuration

The following table describes the items in the previous menu.

Table 3-81. Switching > Interface Setting > Configuration

Parameter	Description
Interface	Click the drop-down menu to select the interface for which data is to be displayed or configured.
Port Type	Displays the possible values are: <ul style="list-style-type: none"> Normal - the port is a normal port. Trunk Member - the port is a member of a Link Aggregation trunk. Look at the LAG screens for more information. Mirrored - the port is a mirrored port. Probe - the port is a monitoring port. Look at the Port Monitoring screens for more information.
STP Mode	Click the drop-down menu to enable or disable the Spanning Tree Protocol Administrative Mode for the port or LAG. The possible values are: <ul style="list-style-type: none"> Enable - select this to enable the Spanning Tree Protocol for this port. Disable - select this to disable the Spanning Tree Protocol for this port. STP Mode is disabled by default.
Admin Mode	Click the drop-down menu to enable or disable the pull-down menu to select the Port control administration state. You must select enable if you want the port to participate in the network. The factory default is Enable.

Table 3-81. Switching > Interface Setting > Configuration (Continued)

Parameter	Description
Broadcast Storm Recovery Mode	Click the drop-down menu to enable or disable this option by selecting the corresponding line on the pull-down entry field. When you specify Enable for Broadcast Storm Recovery and the broadcast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the broadcast traffic. The factory default is Disable.
Broadcast Storm Recovery Level	Enter a value to 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. The range of Broadcast Storm Recovery Level in packets-per-second is 0 to 1488000.
Multicast Storm Recovery Mode	Click the drop-down menu to enable or disable this option by selecting the corresponding line on the pull-down entry field. When you specify Enable for Multicast Storm Recovery and the multicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the multicast traffic. The factory default is Disable.
Multicast Storm Recovery Level	Enter a value to 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. The range of Multicast Storm Recovery Level in packets-per-second is 0 to 1488000.
Unicast Storm Recovery Mode	Click the drop-down menu to enable or disable this option by selecting the corresponding line on the pull-down entry field. When you specify Enable for Unicast Storm Recovery and the unicast traffic on the specified Ethernet port exceeds the configured threshold, the switch blocks (discards) the unicast traffic. The factory default is Disable.
Unicast Storm Recovery Level	Enter a value to 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. The range of Unicast Storm Recovery Level in packets-per-second is 0 to 1488000.
LACP Mode	Click the drop-down menu to select the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation. May be enabled or disabled by selecting the corresponding line on the pull-down entry field. The factory default is Enable.
Physical Mode	Click the drop-down menu to select the port's speed and duplex mode. If you select auto the duplex mode and speed will be set by the auto-negotiation process. Note that the port's maximum capability (full duplex and 100 Mbps) will be advertised. Otherwise, your selection will determine the port's duplex mode and transmission rate. The factory default is Auto. The selection when applied against the "All" option in Slot/Port is applied to all applicable interfaces only.
Physical Status	<p>Displays the physical status.</p> <ul style="list-style-type: none"> ● Normal - the port is a normal port. ● Trunk Member - the port is a member of a Link Aggregation trunk. Look at the LAG screens for more information. ● Mirrored - the port is a mirrored port. ● Probe - the port is a monitoring port. Look at the Port Monitoring screens for more information.

Table 3-81. Switching > Interface Setting > Configuration (Continued)

Parameter	Description
Link Status	Displays the link status (up or down).
Link Trap	Click the drop-down menu to enable or disable the Link Trap function. This object determines whether or not to send a trap when link status changes. The factory default is Enable.
Maximum Frame Size	Enter a value to specify the maximum ethernet frame size the interface supports or is configured, including ethernet header, CRC, and payload. 1518 to 12288. The default maximum frame size is 1518.
Interface Index	Displays the interface index of the interface table entry associated with this port.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Status

The Port Summary page displays the summary of the port configuration. To access this page, click **Switching > Interface Setting > Status**.

Port Summary

MST ID 0 ▼
MST : CST

Interface	Port Type	STP Mode	Forwarding State	Port Role	Admin Mode	Bcast Storm Mode	Bcast Storm Level	Mcast Storm Mode	Mcast Storm Level	Ucast Storm Mode	Ucast Storm Level	LACP Mode	Physical Mode	Physical Status	Link Status	Link Trap
ge0/1	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/2	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/3	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/4	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/5	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/6	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/7	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/8	Normal	Enable	Forwarding	Designated	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	100C Mbps	Link Up	Enable
ge0/9	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/10	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/11	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/12	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/13	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable
ge0/14	Normal	Enable	Disabled	Disabled	Enable	Disable	5%	Disable	5%	Disable	5%	Enable	Auto	Unknown	Link Down	Enable

Figure 3-84. Switching > Interface Setting > Status

The following table describes the items in the previous menu.

Table 3-82. Switching > Interface Setting > Status

Parameter	Description
MST ID	Click the drop-down menu to 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 Spanning Tree is disabled this will be a static value, CST, instead of a selector.
Interface	Displays the port.
Port Type	Displays the port values: <ul style="list-style-type: none"> ● Normal - the port is a normal port. ● Trunk Member - the port is a member of a Link Aggregation trunk. Look at the LAG screens for more information. ● Mirrored - the port is a mirrored port. ● Probe - the port is a monitoring port. Look at the Port Monitoring screens for more information.
STP Mode	Displays the Spanning Tree Protocol Administrative Mode associated with the port or LAG. The possible values are: <ul style="list-style-type: none"> ● Enable - spanning tree is enabled for this port. ● Disable - spanning tree is disabled for this port.
Forwarding State	Displays 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: <ul style="list-style-type: none"> ● Disabled ● Blocking ● Listening ● Learning ● Forwarding ● Broken
Port Role	Displays 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	Displays the The Port control administration state. The port must be enabled in order for it to be allowed into the network. The factory default is Enable.
Bcast Storm Mode	Displays the broadcast storm control status (enabled or disabled) for the port. The factory default is Disable.
Bcast Storm Level	Displays the broadcast storm control threshold for the port. The factory default is 5 percent.
Mcast Storm Mode	Displays the multicast storm control status (enabled or disabled) for the port. The factory default is Disable.

Table 3-82. Switching > Interface Setting > Status (Continued)

Parameter	Description
Mcast Storm Level	Displays the multicast storm control threshold for the port. The factory default is 5 percent.
Ucast Storm Mode	Displays the unicast storm control status (enabled or disabled) for the port. The factory default is Disable.
Ucast Storm Level	Displays the unicast storm control threshold for the port. The factory default is 5 percent.
LACP Mode	Displays the Link Aggregation Control Protocol administration state. The mode must be enabled in order for the port to participate in Link Aggregation.
Physical Mode	Displays the port speed and duplex mode. In auto-negotiation mode the duplex mode and speed are set from the auto-negotiation process.
Physical Status	Displays the port speed and duplex mode for Physical interfaces. Does not report Physical Status for LAG interfaces. Physical status is unknown when a port is down.
Link Status	Displays the Link status (up or down).
Link Trap	Displays the port send trap status.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Interface Description

The Port Description page displays physical address, port list bit offset, interface index, and port description for each interface. To access this page, click **Switching > Interface Setting > Interface Description**.

Port Description

Interface ge0/1 ▾

Port Description (0 to 54 characters)

Interface	Physical Address	Port List Bit Offset	Interface Index	Port Description
ge0/1	00:D0:C9 75:16:FF	1	1	
ge0/2	00:D0:C9 75:16:FF	2	2	
ge0/3	00:D0:C9 75:16:FF	3	3	
ge0/4	00:D0:C9 75:16:FF	4	4	
ge0/5	00:D0:C9 75:16:FF	5	5	
ge0/6	00:D0:C9 75:16:FF	6	6	
ge0/7	00:D0:C9 75:16:FF	7	7	
ge0/8	00:D0:C9 75:16:FF	8	8	
ge0/9	00:D0:C9 75:16:FF	9	9	
ge0/10	00:D0:C9 75:16:FF	10	10	
ge0/11	00:D0:C9 75:16:FF	11	11	
ge0/12	00:D0:C9 75:16:FF	12	12	
ge0/13	00:D0:C9 75:16:FF	13	13	

Figure 3-85. Switching > Interface Setting > Interface Description

The following table describes the items in the previous menu.

Table 3-83. Switching > Interface Setting > Interface Description

Parameter	Description
Interface	Click the drop-down menu to select the interface for which data is to be displayed or configured.
Port Description	Enter the Description string to be attached to a port. It can be up to 64 characters in length.
Interface	Displays the port type/number for the list entry.
Physical Address	Displays the physical address of the specified interface.
Port List Bit Offset	Displays the bit offset value which corresponds to the port when the MIB object type Port List is used to manage in SNMP.
Interface Index	Displays the interface index associated with the port.
Port Description	Description string attached to a port. It can be of up to 64 characters in length.
Submit	Click Submit the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Transceiver Status

The Transceiver Information page displays temperature, voltage, bias current, Tx power, and RX power settings for each interface. To access this page, click **Switching > Interface Setting > Transceiver Status**.

Transceiver Information

Interface	Temperature	Voltage	Bias Current	Tx Power	Rx Power
Refresh					

Figure 3-86. Switching > Interface Setting > Transceiver Status

The following table describes the items in the previous menu.

Table 3-84. Switching > Interface Setting > Transceiver Status

Parameter	Description
Interface	Displays the port.
Temperature	Displays the internal temperature of the transceiver measured value.
Voltage	Displays the supply voltage of the transceiver measured value.
Bias Current	Displays the bias current of the transceiver measured value.
Tx Power	Displays the transmission power of the transceiver measured value.
Rx Power	Displays the received power of the transceiver measured value.

Table 3-84. Switching > Interface Setting > Transceiver Status (Continued)

Parameter	Description
Normal	Displays the measured value.
High Alarm	Displays the measured value.
High Warning	Displays the measured value.
Low Warning	Displays the measured value.
Low Alarm	Displays the measured value.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.4.3 Interface Statistics

CPU Detail Statistics

The Switch Detailed Statistics page displays detailed CPU information for each index. To access this page, click **Switching > Interface Statistics > CPU Detail Statistics**.

Switch Detailed Statistics

ifIndex	17
Octets Received	771395
Packets Received Without Error	7508
Unicast Packets Received	1720
Multicast Packets Received	0
Broadcast Packets Received	5788
Receive Packets Discarded	0
Octets Transmitted	2517842
Packets Transmitted Without Errors	6291
Unicast Packets Transmitted	2538
Multicast Packets Transmitted	3652
Broadcast Packets Transmitted	1
Transmit Packets Discarded	0
Most Address Entries Ever Used	15
Address Entries in Use	14
Maximum VLAN Entries	4093
Most VLAN Entries Ever Used	1
Static VLAN Entries	1
Dynamic VLAN Entries	0
VLAN Deletes	0
Time Since Counters Last Cleared	0 day 2 hr 8 min 30 sec (dd:hh:mm:ss)

Figure 3-87. Switching > Interface Statistics > CPU Detail Statistics

The following table describes the items in the previous menu.

Table 3-85. Switching > Interface Statistics > CPU Detail Statistics

Parameter	Description
ifIndex	Displays the object indicates the interface index of the interface table entry associated with the Processor of this switch.
Octets Received	Displays the total number of octets of data received by the processor (excluding framing bits but including FCS octets).
Packets Received Without Errors	Displays the total number of packets (including broadcast packets and multicast packets) received by the processor.
Unicast Packets Received	Displays the number of subnetwork-unicast packets delivered to a higher-layer protocol.
Multicast Packets Received	Displays 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	Displays the total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	Displays 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	Displays the total number of octets transmitted out of the interface, including framing characters.
Packets Transmitted Without Errors	Displays the total number of packets transmitted out of the interface.
Unicast Packets Transmitted	Displays 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	Displays 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	Displays 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	Displays 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	Displays 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	Displays the number of Learned and static entries in the Forwarding Database Address Table for this switch.
Maximum VLAN Entries	Displays the maximum number of Virtual LANs (VLANs) allowed on this switch.

Table 3-85. Switching > Interface Statistics > CPU Detail Statistics (Continued)

Parameter	Description
Most VLAN Entries Ever Used	Displays the largest number of VLANs that have been active on this switch since the last reboot.
Static VLAN Entries	Displays the number of presently active VLAN entries on this switch that have been created statically.
Dynamic VLAN Entries	Displays the number of presently active VLAN entries on this switch that have been created by GVRP registration.
VLAN Deletes	Displays the number of VLANs on this switch that have been created and then deleted since the last reboot.
Time Since Counters Last Cleared	Displays the elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared (in dd:hh:mm:ss).
Clear Counters	Click Clear Counters to reset all the counters, resetting all switch summary and detailed statistics to default values. The discarded packets count cannot be cleared.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

CPU Brief Statistics

The Switch Statistics Summary page displays a brief summary of the CPU. To access this page, click **Switching > Interface Statistics > CPU Brief Statistics**.

Switch Statistics Summary

Interface	17
Total Packets Received Without Errors	7586
Broadcast Packets Received	5855
Packets Received With Error	0
Packets Transmitted Without Errors	6455
Broadcast Packets Transmitted	1
Transmit Packet Errors	0
Address Entries Currently in Use	15
VLAN Entries Currently in Use	1
Time Since Counters Last Cleared	0 day 2 hr 10 min 3 sec (dd:hh:mm:ss)

Clear Counters Refresh

Figure 3-88. Switching > Interface Statistics > CPU Brief Statistics

The following table describes the items in the previous menu.

Table 3-86. Switching > Interface Statistics > CPU Brief Statistics

Parameter	Description
Interface	Displays the object indicates the interface index of the interface table entry associated with the Processor of this switch.
Total Packets Received Without Errors	Displays the total number of packets (including broadcast packets and multicast packets) received by the processor.

Table 3-86. Switching > Interface Statistics > CPU Brief Statistics (Continued)

Parameter	Description
Broadcast Packets Received	Displays 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	Displays the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Errors	Displays the total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	Displays 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	Displays the number of outbound packets that could not be transmitted because of errors.
Address Entries Currently in Use	Displays the total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently in Use	Displays the number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	Displays the time since the last clear counters.
Clear Counters	Click Clear Counters to reset all the counters, resetting all summary and switch detailed statistics to defaults. The discarded packets count cannot be cleared.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Interface Detail Statistics

The Port Detailed Statistics displays detailed packet information for each interface. To access this page, click **Switching > Interface Statistics > Interface Detail Statistics**.

Port Detailed Statistics

Interface	geC/1
ifIndex	1
Packets RX and TX 64 Octets	0
Packets RX and TX 65-127 Octets	0
Packets RX and TX 128-255 Octets	0
Packets RX and TX 256-511 Octets	0
Packets RX and TX 512-1023 Octets	0
Packets RX and TX 1024-1518 Octets	0
Packets RX and TX 1519-2047 Octets	0
Packets RX and TX 2048-4095 Octets	0
Packets RX and TX 4096-9216 Octets	0
Total Packets Received (Octets)	0
Packets Received 64 Octets	0
Packets Received 65-127 Octets	0
Packets Received 128-255 Octets	0
Packets Received 256-511 Octets	0
Packets Received 512-1023 Octets	0
Packets Received 1024-1518 Octets	0
Packets Received > 1518 Octets	0
Total Packets Received Without Errors	0
Unicast Packets Received	0
Multicast Packets Received	0
Broadcast Packets Received	0
Receive Packets Discarded	0
Total Packets Received with MAC Errors	0
Jabbers Received	0
Fragments Received	0
Undersize Received	0
Alignment Errors	0
Rx FCS Errors	0
Overruns	0
Total Received Packets Not Forwarded	0
802.3x Pause Frames Received	0
Unacceptable Frame Type	0
Total Packets Transmitted (Octets)	0
Packets Transmitted 64 Octets	0
Packets Transmitted 65-127 Octets	0
Packets Transmitted 128-255 Octets	0
Packets Transmitted 256-511 Octets	0
Packets Transmitted 512-1023 Octets	0
Packets Transmitted 1024-1518 Octets	0
Packets Transmitted > 1518 Octets	0
Maximum Frame Size	1518
Total Packets Transmitted Successfully	0

Figure 3-89. Switching > Interface Statistics > Interface Detail Statistics 1/2

Unicast Packets Transmitted	0
Multicast Packets Transmitted	0
Broadcast Packets Transmitted	0
Transmit Packets Discarded	0
Total Transmit Errors	0
Total Transmit Packets Discarded	0
Single Collision Frames	0
Multiple Collision Frames	0
Excessive Collision Frames	0
STP BPDUs Transmitted	0
STP BPDUs Received	0
RSTP BPDUs Transmitted	0
RSTP BPDUs Received	0
MSTP BPDUs Transmitted	0
MSTP BPDUs Received	0
802.3x Pause Frames Transmitted	0
GVRP PDUs Received	0
GVRP PDUs Transmitted	0
GVRP Failed Registrations	0
GMRP PDUs Received	0
GMRP PDUs Transmitted	0
GMRP Failed Registrations	0
EAPOL Frames Transmitted	0
EAPOL Start Frames Received	0
Time Since Counters Last Cleared	0 day 2 hr 11 min 4 sec (dd:hh:mm:ss)

Clear Counters Clear All Counters Refresh

Figure 3-90. Switching > Interface Statistics > Interface Detail Statistics 2/2

The following table describes the items in the previous menu.

Table 3-87. Switching > Interface Statistics > Interface Detail Statistics

Parameter	Description
Interface	Click the drop-down menu to select the interface and data to display.
ifIndex	Displays the ifIndex of the interface table entry associated with this port on an adapter.
Packets RX and TX 64 Octets	Displays 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	Displays 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	Displays 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	Displays 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).

Table 3-87. Switching > Interface Statistics > Interface Detail Statistics (Continued)

Parameter	Description
Packets RX and TX 512-1023 Octets	Displays 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	Displays 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 1519-2047 Octets	Displays the total number of packets (including bad packets) received or transmitted that were between 1519 and 2047 octets in length inclusive (excluding framing bits but including FCS octets).
Packets RX and TX 2048-4095 Octets	Displays 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	Displays 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).
Total Packets Received (Octets)	Displays 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	Displays the total number of received packets that are 64 octets in length.
Packets Received 65-127 Octets	Displays the total number of received packets that are 65 to 127 octets in length (excluding framing bits, including FCS octets).
Packets Received 128-255 Octets	Displays the total number of received packets that are 128 to 255 octets in length (excluding framing bits, including FCS octets).
Packets Received 256-511 Octets	Displays the total number of received Packets that are 256 To 511 octets in length (excluding framing bits, including FCS octets).
Packets Received 512-1023 Octets	Displays the total number of received Packets that are 512 to 1023 octets in length (excluding framing bits, including FCS octets).
Packets Received 1024-1518 Octets	Displays the total number of received Packets that are 1024 to 1518 octets in length (excluding framing bits, including FCS octets).
Packets Received > 1518 Octets	Displays the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Total Packets Received Without Errors	Displays the total number of packets received that were without errors.
Unicast Packets Received	Displays the number of sub network unicast packets delivered to a higher layer protocol.

Table 3-87. Switching > Interface Statistics > Interface Detail Statistics (Continued)

Parameter	Description
Multicast Packets Received	Displays the total number of good packets received that were directed to a multi-cast address. Note that this number does not include packets directed to the broadcast address.
Broadcast Packets Received	Displays the total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Received Packets Discarded	Displays 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. One possible reason for discarding such a packet could be to free up buffer space.
Total Packets Received with MAC Errors	Displays the total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Jabbers Received	Displays 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	Displays 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	Displays 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	Displays 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	Displays 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	Displays 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	Displays the count of valid frames received which were discarded (i.e. filtered) by the forwarding process.
802.3x Pause Frames Received	Displays the 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	Displays the number of frames discarded from this port due to being an unacceptable frame type.

Table 3-87. Switching > Interface Statistics > Interface Detail Statistics (Continued)

Parameter	Description
Total Packets Transmitted (Octets)	Displays 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	Displays the total number of transmitted Packets that are 64 octets in length.
Packets Transmitted 65-127 Octets	Displays the total number of transmitted Packets that are 65 to 127 octets in length (excluding framing bits, including FCS octets).
Packets Transmitted 128-255 Octets	Displays the total number of transmitted Packets that are 128 to 255 octets in length (excluding framing bits, including FCS octets).
Packets Transmitted 256-511 Octets	Displays the total number of transmitted Packets that are 256 To 511 octets in length (excluding framing bits, including FCS octets).
Packets Transmitted 512-1023 Octets	Displays the total number of transmitted Packets that are 512 to 1023 octets in length (excluding framing bits, including FCS octets).
Packets Transmitted 1024-1518 Octets	Displays the total number of transmitted Packets that are 1024 to 1518 octets in length (excluding framing bits, including FCS octets).
Packets Transmitted > 1518 Octets	Displays the total number of packets transmitted that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed. This counter has a max increment rate of 815 counts per sec at 10 Mb/s.
Maximum Frame Size	Displays 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	Displays the number of frames that have been transmitted by this port to its segment.
Unicast Packets Transmitted	Displays the total number of packets that higher-level protocols requested be transmitted to a sub network-unicast address, including those that were discarded or not sent.
Multicast Packets Transmitted	Displays 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	Displays 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	Displays the number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Total Transmit Errors	Displays the sum of Single, Multiple, and Excessive Collisions.
Total Transmit Packets Discarded	Displays the sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.
Single Collision Frames	Displays the count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Table 3-87. Switching > Interface Statistics > Interface Detail Statistics (Continued)

Parameter	Description
Multiple Collision Frames	Displays the count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Excessive Collision Frames	Displays the count of frames for which transmission on a particular interface fails due to excessive collisions.
STP BPDUs Transmitted	Displays the number of STP BPDUs transmitted from the selected port.
STP BPDUs Received	Displays the number of STP BPDUs received at the selected port.
RSTP BPDUs Received	Displays the number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Displays the number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Transmitted	Displays the number of MSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Displays the number of MSTP BPDUs received at the selected port.
802.3x Pause Frames Transmitted	Displays the 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	Displays the count of GVRP PDUs received in the GARP layer.
GVRP PDUs Transmitted	Displays the count of GVRP PDUs transmitted from the GARP layer.
GVRP Failed Registrations	Displays the number of times attempted GVRP registrations could not be completed.
GMRP PDUs Received	Displays the count of GMRP PDUs received from the GARP layer.
GMRP PDUs Transmitted	Displays the count of GMRP PDUs transmitted from the GARP layer.
GMRP Failed Registrations	Displays the number of times attempted GMRP registrations could not be completed.
EAPOL Frames Transmitted	Displays the number of EAPOL frames of any type that have been transmitted by this Authenticator.
EAPOL Start Frames Received	Displays the number of EAPOL frames of any type that have been received by this Authenticator.
Time Since Counters Last Cleared	Displays the elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared (in dd:hh:mm:ss).
Clear Counters	Click Clear Counter to refresh all the counters, resetting all statistics for this port to default values.

Table 3-87. Switching > Interface Statistics > Interface Detail Statistics (Continued)

Parameter	Description
Clear All Counters	Click Clear All Counters to refresh all the counters for all ports, resetting all statistics for all ports to default values.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Interface Brief Statistics

The Port Statistics Summary displays a brief summary of the packet information for each interface. To access this page, click **Switching > Interface Statistics > Interface Brief Statistics**.

Port Statistics Summary

Interface	ge0/1
IfIndex	1
Total Packets Received Without Errors	0
Packets Received With Error	0
Broadcast Packets Received	0
Receive Packets Discarded	0
Packets Transmitted Without Errors	0
Transmit Packets Discarded	0
Transmit Packet Errors	0
Collision Frames	0
Time Since Counters Last Cleared	0 day 2 hr 14 min 7 sec (dd:hh:mm:ss)

Figure 3-91. Switching > Interface Statistics > Interface Brief

Statistics The following table describes the items in the previous menu.

Table 3-88. Switching > Interface Statistics > Interface Brief Statistics

Parameter	Description
Interface	Click the drop-down menu to select the interface for which data is to be displayed or configured.
ifIndex	Displays the object indicates the ifIndex of the interface table entry associated with this port on an adapter.
Total Packets Received Without Errors	Displays the total number of packets received that were without errors.
Received Packets Discarded	Displays 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. One possible reason for discarding such a packet could be to free up buffer space.
Packets Received With Error	Displays the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	Displays the total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Table 3-88. Switching > Interface Statistics > Interface Brief Statistics (Continued)

Parameter	Description
Packets Transmitted Without Errors	Displays the number of frames that have been transmitted by this port to its segment.
Transmit Packets Discarded	Displays the number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Packet Errors	Displays the number of outbound packets that could not be transmitted because of errors.
Collision Frames	Displays the best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	Displays the elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared (in dd:hh:mm:ss).
Clear Counters	Click Clear Counters to reset all the counters, resetting all statistics for this port to default values.
Clear All Counters	Click Clear All Counters to reset all the counters for all ports, resetting all statistics for all ports to default values.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.4.4 Port Mirroring

Port Mirroring

The Port Multiple Port Mirroring page allows users to assign session IDs, modes, destination ports, and add source ports. This page also displays a brief summary of the direction and source ports. To access this page, click **Switching > Port Mirroring > Port Mirroring**.

Port Multiple Port Mirroring

Session ID	1
Mode	Disable
Destination Port	None

Direction	Source Port(s)
Tx and Rx	None
Rx	None
Tx	None

Figure 3-92. Switching > Port Mirroring > Port Mirroring

The following table describes the items in the previous menu.

Table 3-89. Switching > Port Mirroring > Port Mirroring

Parameter	Description
Session ID	Click the drop-down menu to select a port mirroring session from the list. The number of sessions allowed is platform specific. By default the First Session is selected.
Mode	Click the drop-down menu to enable or disable the Session Mode for a selected session ID. The default Session Mode is disabled.
Destination Port	Click the drop-down menu to select the destination port and receive all the traffic from configured mirrored port(s). Default value is None.
Direction	Displays the direction of traffic on source port(s) which will be sent to the probe port. Possible values are: <ul style="list-style-type: none"> • Tx and Rx - Both Ingress and Egress traffic. • Rx - Ingress traffic only. • Tx - Egress traffic only.
Source Port(s)	Displays the source port(s) with directions as mirrored port(s). Traffic of the source port(s) is sent to the probe port. Up to 16 source ports can be selected per session.
Add Source Port	Click Add Source Port to add Source Port(s) to the selected session.
Remove Source Port	Click Remove Source Port to remove a configured Source Port(s) of the selected session.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Click Delete to remove the selected session configuration.



The Add Source Port allows users to add source ports and configure the direction for each session ID.

Multiple Port Mirroring - Add Source Ports

Session ID

Direction	Source Port(s)
Tx and Rx	None
Rx	None
Tx	None

Source Port(s)

Direction

Figure 3-93. Switching > Port Mirroring > Port Mirroring > Add Source Ports

The following table describes the items in the previous menu.

Table 3-90. Switching > Port Mirroring > Port Mirroring > Add Source Ports

Parameter	Description
Session ID	Click the drop-down menu to select the session ID for which source ports are to be added.
Direction	Displays the direction of traffic on the listed entry.
Source Port(s)	Displays the source port on the listed entry.
Source Port(s)	Select the configured port(s) with directions as mirrored port(s). Traffic of the source port(s) is sent to the probe port. Up to 16 source ports can be selected per session.
Direction	Click the drop-down menu to select the direction of traffic on source port(s) which will be sent to the probe port. Possible values are: <ul style="list-style-type: none"> • Tx and Rx - Both Ingress and Egress traffic. • Rx - Ingress traffic only. • Tx - Egress traffic only.
Add	Click Add to add the selected source ports to the list of configured source ports.
Cancel	Click Cancel to discard the changes made on the page.

3.4.5 VLAN Setting

VLAN Membership

The VLAN Configuration page allows users to configure the participation and tagging of each interface for each session ID. Users can assign a name to each VLAN ID. To access this page, click **Switching > VLAN Setting > VLAN Membership**.

VLAN Configuration

VLAN ID List: 1

VLAN Name: default (0 to 32 characters)

VLAN Type: Default

VLAN Participation All:

Participation All: Autodelete Tagging All Flood Unknown Multicast

VLAN Participation:

Interface	Interface Status	Participation	Tagging
ge0/1	Include	Include	Untagged
ge0/2	Include	Include	Untagged
ge0/3	Include	Include	Untagged
ge0/4	Include	Include	Untagged
ge0/5	Include	Include	Untagged
ge0/6	Include	Include	Untagged
ge0/7	Include	Include	Untagged
ge0/8	Include	Include	Untagged
ge0/9	Include	Include	Untagged
ge0/10	Include	Include	Untagged
ge0/11	Include	Include	Untagged
ge0/12	Include	Include	Untagged
ge0/13	Include	Include	Untagged
ge0/14	Include	Include	Untagged

Figure 3-94. Switching > VLAN Setting > VLAN Membership

The following table describes the items in the previous menu.

Table 3-91. Switching > VLAN Setting > VLAN Membership

Parameter	Description
VLAN ID List	Click the drop-down menu to select an entry to modify, create an entry, or delete an entry. You can use this screen view/modify/delete an existing VLAN configuration or to create new single/multiple VLAN IDs specified in VLAN ID field. Use this drop-down menu to select one of the existing VLANs to view/modify the configuration. You can select 'Create' to add new VLANs or select 'Delete' from the pull-down to delete the existing VLANs.
VLAN Name	Enter the value to use as the name for this configuration.
VLAN Type	Displays the VLAN type for the configuration.
Participation All	Click the box to specify the use of all the ports to participate in this VLAN. The factory default is Autodetect. The possible values are: <ul style="list-style-type: none"> ● Include - All the ports are always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1q standard. ● Exclude - All the ports are never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1q standard. ● Autodetect - Specifies that all ports may be dynamically registered in this VLAN via GVRP. All ports 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 All	Click the box to select the tagging behavior for all the ports in this VLAN. The factory default is Untagged. The possible values are: <ul style="list-style-type: none"> ● Tagged - all frames transmitted for this VLAN will be tagged. ● Untagged - all frames transmitted for this VLAN will be untagged.
Flood Unknown Multicast	Click the box to specify the use of all the ports to forward unknown multicast frames in this VLAN. The factory default is Discarding. The possible values are: <ul style="list-style-type: none"> ● Flooding - flood all unknown multicast frames to all the ports in this VLAN, except for the receiving port. ● Discarding - discard all unknown multicast frames received from all the ports in this VLAN.
VLAN Participation	Click the box to specify the use of a port to participate in this VLAN. The factory default is Autodetect. The possible values are: <ul style="list-style-type: none"> ● Include - This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1q standard. ● Exclude - This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1q standard. ● Autodetect - Specifies that port may be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless it receives a GVRP request. This is equivalent to registration normal in the IEEE 802.1q standard.

Table 3-91. Switching > VLAN Setting > VLAN Membership (Continued)

Parameter	Description
Tagging	Displays the tagging behavior for this port in this VLAN. The factory default is Untagged. The possible values are: <ul style="list-style-type: none"> • Tagged - all frames transmitted for this VLAN will be tagged. • Untagged - all frames transmitted for this VLAN will be untagged.
VLAN ID - Individual/Range	Displays the VLAN Identifier for the new VLAN. (You can only enter data in this field when you are creating a new VLAN.)Specify the VLAN Identifiers for the VLANs being created or deleted. Single or Multiple VLANs can be specified at once. This field can accept single VLAN ID or range of VLAN IDs or a combination of both in sequence separated by ','. You can specify individual VLAN ID. Eg: 10 You can specify the VLAN range values separated by '-'. E.g. 10-13 You can specify the combination of both separated by ','. Eg: 12,15,40-43,1000-1005,2000 The range of the VLAN ID is 2 to 4093.
VLAN Name	Displays the 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 always has a name of 'Default'.
VLAN ID	Displays the VLAN ID. The range of the VLAN ID is 1 to 4093.
VLAN Participation All	Displays the VLAN participation selection of all the interfaces. By default, the field is disabled. Set the checkbox to enable the field.
VLAN Participation	Displays the VLAN participation selection. By default, the field is disabled. Set the checkbox to enable the field.
Convert VLAN Type to Static	Displays the VLAN type conversion option. A VLAN that is created by GVRP registration initially has a type of 'Dynamic'. By default, the field is disabled. Set the checkbox to enable the field.
VLAN Type	Displays the VLAN type. 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'.
Error Console	Displays the reason for failure if any occurred during creation or deletion of VLANs.
Interface	Displays the port associated with the fields on this line.
Status	Displays the current value of the participation parameter for the port.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Clear Log	Click Clear Log to reset the log history.

VLAN Database

The VLAN Database displays a summary of the status of each VLAN ID. To access this page, click **Switching > VLAN Setting > VLAN Database**.

VLAN Status

VLAN ID	VLAN Name	VLAN Type	Unknown Multicast
1	default	Default	Discarding

Figure 3-95. Switching > VLAN Setting > VLAN Database

The following table describes the items in the previous menu.

Table 3-92. Switching > VLAN Setting > VLAN Database

Parameter	Description
VLAN ID	Displays the VLAN Identifier (VID) of the VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	Displays the name of the VLAN. VLAN ID 1 is always named "Default".
VLAN Type	The VLAN type: <ul style="list-style-type: none"> • Default (VLAN ID = 1) -- always present • Static -- a VLAN you have configured • Dynamic -- a VLAN created by GVRP registration that you have not converted to static, and that GVRP may therefore remove
Unknown Multicast	Displays the policy to apply to unknown multicast traffic.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Port-based VLAN

Configuration

The VLAN Port Configuration allows users to configure the VLAN settings for each interface. To access this page, click **Switching > VLAN Setting > Port-based VLAN > Configuration**.

VLAN Port Configuration

Interface	<input type="text" value="Gig1"/>
Port VLAN ID	<input type="text" value="1"/> (1 to 4093)
Acceptable Frame Types	<input type="text" value="Admit All"/>
Ingress Filtering	<input type="text" value="Disable"/>
Port Priority	<input type="text" value="0"/> (0 to 7)

Figure 3-96. Switching > VLAN Setting > Port-based VLAN > Configuration

The following table describes the items in the previous menu.

Table 3-93. Switching > VLAN Setting > Port-based VLAN > Configuration

Parameter	Description
Interface	Click the drop-down menu to select the physical interface for which you want to display or configure data. Select 'All' to set the parameters for all ports to same values.
Port VLAN ID	Enter the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The value ranges 1 to 4093. The factory default is 1.
Acceptable Frame Type	Click the drop-down menu to specify the port to handle untagged and priority tagged frames. If you select 'AdmitTaggedOnly', the port will discard any untagged or priority tagged frames it receives. If you select 'AdmitUntaggedOnly', the port discard tagged frames it receives. If you select '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. Whichever you select, VLAN tagged frames will be forwarded in accordance with the IEEE 802.1Q VLAN standard. The factory default is Admit All.
Ingress Filtering	Click the drop-down menu to specify how you want the port to handle tagged frames. If you enable Ingress Filtering on the pull-down menu, a tagged frame will be discarded if this port is not a member of the VLAN identified by the VLAN ID in the tag. If you select disable from the pull-down menu, all tagged frames will be accepted. The factory default is Disable.
Port Priority	Enter the value to specify the default 802.1p priority assigned to untagged packets arriving at the port. The value ranges from 0 to 7.Default value is 0.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Status

The VLAN Port Summary displays the list of all ports on the switch. To access this page, click **Switching > VLAN Setting > Port-based VLAN > Status**.

VLAN Port Summary

List of all Ports on the Switch

Interface	Port VLAN ID Configured	Acceptable Frame Types	Ingress Filtering Configured	Port Priority
ge0/1	1	Admit All	Disable	0
ge0/2	1	Admit All	Disable	0
ge0/3	1	Admit All	Disable	0
ge0/4	1	Admit All	Disable	0
ge0/5	1	Admit All	Disable	0
ge0/6	1	Admit All	Disable	0
ge0/7	1	Admit All	Disable	0
ge0/8	1	Admit All	Disable	0
ge0/9	1	Admit All	Disable	0
ge0/10	1	Admit All	Disable	0
ge0/11	1	Admit All	Disable	0
ge0/12	1	Admit All	Disable	0
ge0/13	1	Admit All	Disable	0
ge0/14	1	Admit All	Disable	0
ge0/15	1	Admit All	Disable	0
ge0/16	1	Admit All	Disable	0
LAG1	1	Admit All	Disable	0
LAG2	1	Admit All	Disable	0
LAG3	1	Admit All	Disable	0
LAG4	1	Admit All	Disable	0

Figure 3-97. Switching > VLAN Setting > Port-based VLAN > Status

The following table describes the items in the previous menu.

Table 3-94. Switching > VLAN Setting > Port-based VLAN > Status

Parameter	Description
Interface	Displays the interface port.
Port VLAN ID Configured	Displays the VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port.
Acceptable Frame Types	Displays the types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1q VLAN specification.
Ingress Filtering Configured	Displays the status of the filtering. If enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1q VLAN bridge specification. The factory default is Disable.

Table 3-94. Switching > VLAN Setting > Port-based VLAN > Status (Continued)

Parameter	Description
Port Priority	Displays the set priority of the entry. The default 802.1p priority assigned to untagged packets arriving at the port.
Refresh	Refresh the data on the screen with the present state of the data in the switch.

Protocol-based VLAN

Configuration

The Protocol-based VLAN Configuration allows the users to configure settings for protocol-based VLAN. To access this page, click **Switching > VLAN Setting > Protocol-based VLAN > Configuration**.

Protocol-based VLAN Configuration

Figure 3-98. Switching > VLAN Setting > Protocol-based VLAN > Configuration

The following table describes the items in the previous menu.

Table 3-95. Switching > VLAN Setting > Protocol-based VLAN > Configuration

Parameter	Description
Group ID	Click the drop-down menu to configure or delete an existing protocol-based VLAN, or create a new one. Use this pull-down menu to select one of the existing PBV-LANs, or select 'Create New Group' to add a new one. You can create up to 128 groups.
Group ID	Enter a value to assign a Group ID.
Group Name (Optional)	Enter a value to assign a name to an existing group. You may enter up to 16 alphanumeric characters including underscores, hyphens and spaces. Configuring name for a Group is optional.
VLAN	Enter a value to assign the VLAN, range 1 to 4093. All the ports in the group will assign this VLAN ID to untagged packets received for the protocols you included in this group.
Protocol-list	Enter a value to assign the Protocol-list--valid comma(,) separated string with standard "arp", "ip", "ipx" keywords, hexadecimal or decimal values in the range of 0x0600 (1536) to 0xFFFF (65535).
Interface	Select the interface(s) you want to be included in the group. Note that a given interface can only belong to one group for a given protocol. Ex: If you have already added interface 0.1 to a group for 0x0800, you cannot add it to another group that also includes 0x0800, although you could add it to a new group for other ethertype value.

Table 3-95. Switching > VLAN Setting > Protocol-based VLAN > Configuration (Continued)

Parameter	Description
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Click Delete to remove the Protocol Based VLAN group identified by the value in the Group ID field. If you want the switch to retain the deletion across a power cycle, you must perform a save.

Status

The Protocol-based VLAN Summary displays the list of all groups. To access this page, click **Switching > VLAN Setting > Protocol-based VLAN > Status**.

Protocol-based VLAN Summary

Group Name	Group ID	Protocol(s)	VLAN	Interface(s)
Refresh				

Figure 3-99. Switching > VLAN Setting > Protocol-based VLAN > Status The following table describes the items in the previous menu.

Table 3-96. Switching > VLAN Setting > Protocol-based VLAN > Status

Parameter	Description
Group Name	Displays the name associated with the group. Group names can be up to 16 characters long. The maximum number of groups allowed is 128.
Group ID	Displays the number used to identify the group.
Protocol(s)	Displays the protocol(s) that belongs to the group.
VLAN	Displays the VLAN ID associated with the group.
Interface(s)	Displays the interfaces associated with the group.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

IP Subnet-based VLAN

Configuration

The IP Subnet-based VLAN Configuration allows users to configure IP and subnet mask settings. To access this page, click **Switching > VLAN Setting > IP Subnet-based VLAN > Configuration**.

IP Subnet-based VLAN Configuration

Figure 3-100. Switching > VLAN Setting > IP Subnet-based VLAN > Configuration
The following table describes the items in the previous menu.

Table 3-97. Switching > VLAN Setting > IP Subnet-based VLAN > Configuration

Parameter	Description
IP Address	Click the drop-down menu to select the IP Address bound to a VLAN ID. To add another IP Subnet-based VLAN, select “Add” option.
IP Address	Enter the IP Address bound to VLAN ID. This field is configurable only when a new IP Subnet Based VLAN is being created. IP Address in dotted decimal notation.
Subnet Mask	Enter the Subnet Mask of the IP Address. This field is configurable only when a new IP Subnet-based VLAN is being created. Subnet mask should be in dotted decimal notation.
VLAN	Enter the VLAN ID can be any number in the range of 1 to 4093.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Click Delete to remove an entry of IP Subnet to VLAN mapping.

Status

The IP Subnet-based VLAN Summary displays information for each IP address. To access this page, click **Switching > VLAN Setting > IP Subnet-based VLAN > Status**.

IP Subnet-based VLAN Summary

Figure 3-101. Switching > VLAN Setting > IP Subnet-based VLAN > Status

The following table describes the items in the previous menu.

Table 3-98. Switching > VLAN Setting > IP Subnet-based VLAN > Status

Parameter	Description
IP Address	Displays the IP Address of the subnet that is being bound to a VLAN ID.
Subnet Mask	Displays the subnet mask of the IP Address bound to VLAN ID.
VLAN ID	Displays the VLAN ID to which above mentioned IP Subnet is being bound to. VLAN ID can be any number in the range of 1 to 4093.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

MAC-based VLAN

Configuration

The MAC-based VLAN Configuration allows users to configure MAC address and VLAN ID. To access this page, click **Switching > VLAN Setting > MAC-based VLAN > Configuration**.

MAC-based VLAN Configuration

Figure 3-102. Switching > VLAN Setting > MAC-based VLAN >

Configuration The following table describes the items in the previous menu.

Table 3-99. Switching > VLAN Setting > MAC-based VLAN > Configuration

Parameter	Description
MAC Address	Click the drop-down menu to select the MAC Address bound to a VLAN. To add another MAC VLAN entry, select “Add” option.
MAC Address	Enter the MAC address which is to be bound to a VLAN ID. This field is configurable only when a MAC-based VLAN is created.
VLAN	Enter a value for a VLAN ID: range 1 to 4093.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Click Delete to remove an entry of MAC Address to VLAN mapping.

Summary

The MAC-based VLAN Summary displays information for each MAC address. To access this page, click **Switching > VLAN Setting > MAC-based VLAN > Summary**.

MAC-based VLAN Summary

MAC Address	VLAN ID
Refresh	

Figure 3-103. Switching > VLAN Setting > MAC-based VLAN > Summary The following table describes the items in the previous menu.

Table 3-100. Switching > VLAN Setting > MAC-based VLAN > Summary

Parameter	Description
MAC Address	Displays the MAC Address bound to a VLAN ID.
VLAN ID	Displays the VLAN ID to which a MAC Address is bound.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.4.6 QinQ

Global Configuration

The DVLAN Configuration allows users to select the Global EtherType through the drop-down menu. To access this page, click **Switching > QinQ > Global Configuration**.

DVLAN Configuration

Configure Primary TPID <input type="checkbox"/>	Global EtherType 802.1Q Tag ▼
Submit Remove	

Figure 3-104. Switching > QinQ > Global Configuration The following table describes the items in the previous menu.

Table 3-101. Switching > QinQ > Global Configuration

Parameter	Description
Configure Primary TPID	Click the box to configure the selected Global EtherType as the Primary TPID.

Table 3-101. Switching > QinQ > Global Configuration (Continued)

Parameter	Description
Global EtherType	Click the drop-down menu to specify the global EtherType available. The two-byte hex EtherType to be used as the first 16 bits of the DVLAN tag. <ul style="list-style-type: none"> 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.
Custom Value	Enter the value to assign the custom tag in any range from 1 to 65535.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Remove	Click Remove to deletes the selected Global Ether Type.

Global Status

The DVLAN Summary page displays information for each TPID. To access this page, click **Switching > QinQ > Global Status**.

DVLAN Summary

The screenshot shows a form with two rows: 'Primary TPID' with the value '0x0100' and 'Secondary TPIDs' which is empty. Below the form is a 'Refresh' button.

Figure 3-105. Switching > QinQ > Global Status

The following table describes the items in the previous menu.

Table 3-102. Switching > QinQ > Global Status

Parameter	Description
Global TPIDs	Displays the Global tag protocol identifiers (TPIDs) configured.
Primary TPID	Displays the Primary tag protocol identifier (TPID) configured.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Interface Configuration

The DVLAN Interface Configuration page allows users to enable or disable settings for each interface. To access this page, click **Switching > QinQ > Interface Configuration**,

DVLAN Interface Configuration

The screenshot shows a form with two rows: 'Interface' with a dropdown menu showing 'ge0/1' and 'Interface Mode' with a dropdown menu showing 'Disable'. Below the form is a 'Submit' button.

Figure 3-106. Switching > QinQ > Interface Configuration

The following table describes the items in the previous menu.

Table 3-103. Switching > QinQ > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to 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	Click the drop-down menu to specify the administrative mode via which Double VLAN Tagging can be enabled or disabled. The default value for this is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Remove	Click Remove to delete the selected Ether Type.

Interface Status

The DVLAN Interface Summary page displays the assigned mode and Ethertype for each interface. To access this page, click **Switching > QinQ > Interface Summary**.

DVLAN Interface Summary

Interface	Interface Mode	Interface EtherType
ge0/1	Disable	0x8100
ge0/2	Disable	0x8100
ye0/3	Disable	0x8100
ge0/4	Disable	0x8100
ge0/5	Disable	0x8100
ye0/6	Disable	0x8100
ge0/7	Disable	0x8100
ge0/8	Disable	0x8100
ye0/9	Disable	0x8100
ge0/10	Disable	0x8100
ge0/11	Disable	0x8100
ye0/12	Disable	0x8100
ge0/13	Disable	0x8100
ge0/14	Disable	0x8100
ye0/15	Disable	0x8100
ge0/15	Disable	0x8100
LAG1	Disable	0x8100
LAG2	Disable	0x8100
LAG3	Disable	0x8100
LAG4	Disable	0x8100
LAG5	Disable	0x8100
LAG6	Disable	0x8100

Figure 3-107. Switching > QinQ > Interface Summary

The following table describes the items in the previous menu.

Table 3-104. Switching > QinQ > Interface Summary

Parameter	Description
Interface	Displays the physical interface for which data is being displayed.
Interface Mode	Displays the administrative mode via which Double VLAN Tagging can be enabled or disabled.

Table 3-104. Switching > QinQ > Interface Summary (Continued)

Parameter	Description
Interface EtherType	Displays the Interface EtherType configured.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.4.7 GARP

Status

The GARP status page displays the status for the GVRP and GMRP switches, as well as mode and timer information for each interface. To access this page, click **Switching > GARP > Status**.

GARP Status

Switch GVRP	Disable
Switch GMRP	Disable

Interface	Port GVRP Mode	Port GMRP Mode	Join Timer (centisees)	Leave Timer(centisees)	Leave All Timer (centisees)
ge1/1	Disable	Disable	20	60	1000
ge2/2	Disable	Disable	20	60	1000
ge3/3	Disable	Disable	20	60	1000
ge4/4	Disable	Disable	20	60	1000
ge5/5	Disable	Disable	20	60	1000
ge6/6	Disable	Disable	20	60	1000
ge7/7	Disable	Disable	20	60	1000
ge8/8	Disable	Disable	20	60	1000
ge9/9	Disable	Disable	20	60	1000
ge10/10	Disable	Disable	20	60	1000
ge11/11	Disable	Disable	20	60	1000
ge12/12	Disable	Disable	20	60	1000
ge13/13	Disable	Disable	20	60	1000
ge14/14	Disable	Disable	20	60	1000
ge15/15	Disable	Disable	20	60	1000
ge16/16	Disable	Disable	20	60	1000
LAG1	Disable	Disable	20	60	1000
LAG2	Disable	Disable	20	60	1000
LAG3	Disable	Disable	20	60	1000

Figure 3-108. Switching > GARP > Status

The following table describes the items in the previous menu.

Table 3-105. Switching > GARP > Status

Parameter	Description
Switch GVRP	Displays the GARP VLAN Registration Protocol administrative mode for this switch is enabled or disabled. The factory default is Disable.
Switch GMRP	Displays the GARP Multicast Registration Protocol administrative mode for this switch, enabled or disabled. The factory default is Disable.
Interface	Displays the Slot/Port of the interface.
Port GVRP Mode	Displays the GVRP administrative mode for the port is enabled or disabled. The factory default is Disable.

Table 3-105. Switching > GARP > Status (Continued)

Parameter	Description
Port GMRP Mode	Displays the GMRP administrative mode for the port is enabled or disabled. The factory default is Disable.
Join Timer (centi-secs)	Displays the time between the transmission of GARP PDUs registering (or re-registering) membership for a VLAN or multicast group in centiseconds. An instance of this timer exists for each GARP participant for each port. Permissible values are 10 to 100 centiseconds (0.1 to 1.0 seconds). The factory default is 20 centiseconds (0.2 seconds).
Leave Timer (centi-secs)	Displays the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds. This allows time for another station to assert registration for the same attribute in order to maintain uninterrupted service. An instance of this timer exists for each GARP participant for each port. Permissible values are 20 to 600 centiseconds (0.2 to 6.0 seconds). The factory default is 60 centiseconds (0.6 seconds).
Leave All Timer (centi-secs)	Displays 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. An instance of this timer exists for each GARP participant for each port. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are 200 to 6000 centiseconds (2 to 60 seconds). The factory default is 1000 centiseconds (10 seconds).
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Global Configuration

The GARP Switch Configuration page allows users to enable or disable the GVRP and GMRP modes. To access this page, click **Switching > GARP > Global Configuration**.

GARP Switch Configuration

GVRP Mode

GMRP Mode

Figure 3-109. Switching > GARP > Global Configuration

The following table describes the items in the previous menu.

Table 3-106. Switching > GARP > Global Configuration

Parameter	Description
GVRP Mode	Click drop-down to enable or disable the GARP VLAN Registration Protocol administrative mode for the switch by selecting enable or disable from the pull-down menu. The factory default is Disable.
GMRP Mode	Click the drop-down menu to enable or disable the GARP Multicast Registration Protocol administrative mode for the switch by selecting enable or disable from the pull-down menu. The factory default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Configuration

The GARP Port Configuration page allows users to configure the mode and timer settings for each interface. To access this page, click **Switching > GARP > Interface Configuration**.

GARP Port Configuration

The screenshot shows the GARP Port Configuration page with the following fields:

- Interface:** A dropdown menu with 'ge0/1' selected.
- Port GVRP Mode:** A dropdown menu with 'Disable' selected.
- Port GMRP Mode:** A dropdown menu with 'Disable' selected.
- GARP Timers:**
 - Leave Timer (centiseecs):** A text input field with '60' and a range '(20 to 600)'.
 - Join Timer (centiseecs):** A text input field with '20' and a range '(10 to 100)'.
 - Leave All Timer (centiseecs):** A text input field with '1000' and a range '(200 to 6000)'.
- Submit:** A button at the bottom right.

Figure 3-110. Switching > GARP > Interface Configuration

The following table describes the items in the previous menu.

Table 3-107. Switching > GARP > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the physical interface for which data is to be displayed or configured. It is possible to set the parameters for all ports by selecting 'All'.
Port GVRP Mode	Click the drop-down menu to enable or disable the GARP VLAN Registration Protocol administrative mode for the port by selecting enable or disable from the pull-down menu. If you select disable, the protocol will not be active and the Join Time, Leave Time and Leave All Time will have no effect. The factory default is Disable.
Port GMRP Mode	Click the drop-down menu to enable or disable the GARP Multicast Registration Protocol administrative mode for the port by selecting enable or disable from the pull-down menu. If you select disable, the protocol will not be active, and Join Time, Leave Time and Leave All Time have no effect. The factory default is Disable.
GARP Timers	

Table 3-107. Switching > GARP > Interface Configuration (Continued)

Parameter	Description
Leave Timer (centi-secs)	Enter a value to specify the time to wait after receiving an unregister request for a VLAN or multicast group before deleting the associated entry, in centiseconds. 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). The factory default is 60 centiseconds (0.6 seconds). An instance of this timer exists for each GARP participant for each port.
Join Timer (centi-secs)	Enter a value to 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.
Leave All Timer (centi-secs)	Enter a value to specify 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.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

3.4.8 Port Channel

Configuration

The Port Channel Configuration page allows users to configure port channel settings. To access this page, click **Switching > Port Channel > Configuration**.

Port Channel Configuration

Port Channel Interface	LAG1 ▾
Port Channel Name	ch1 (1 to 15 alphanumeric characters)
Link Trap	Disable ▾
Administrative Mode	Enable ▾
Link Status	Down
STP Mode	Enable ▾
Static Mode	Enable ▾
Load Balance	3 Src/Dest MAC, VLAN, EType, incoming port ▾
Port Channel Members	

Slot/Port	Participation	Membership Conflicts
ge0/1	Exclude ▾	
ge0/2	Exclude ▾	
ge0/3	Exclude ▾	
ge0/4	Exclude ▾	
ge0/5	Exclude ▾	
ge0/6	Exclude ▾	
ge0/7	Exclude ▾	
ge0/8	Exclude ▾	
ge0/9	Exclude ▾	
ge0/10	Exclude ▾	
ge0/11	Exclude ▾	

Figure 3-111. Switching > Port Channel > Configuration

The following table describes the items in the previous menu.

Table 3-108. Switching > Port Channel > Configuration

Parameter	Description
Port Channel Interface	Click the drop-down menu to select existing Port Channel or to create a new one. Use this pull-down menu to select one of the existing Port Channels, or select 'Create' to add a new one. There can be a maximum of 8 Port Channels.
Port Channel Name	Enter a value to specify the name you want assigned to the Port Channel. You may enter any string of 1 to 15 alphanumeric characters. A valid name has to be specified in order to create the Port Channel.
Link Trap	Click the drop-down menu to enable or disable the link trap function. The factory default is Disable, based on which the traps are to be sent.
Administrative Mode	Click the drop-down menu to enable or disable the function. 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	Displays the link status: up or down.

Table 3-108. Switching > Port Channel > Configuration (Continued)

Parameter	Description
STP Mode	Click the drop-down menu to enable or disable the Spanning Tree Protocol Administrative Mode associated with the Port Channel. The possible values are: <ul style="list-style-type: none"> • Disable - spanning tree is disabled for this Port Channel. • Enable - spanning tree is enabled for this Port Channel. The factory default is Enable.
Static Mode	Click the drop-down menu to enable or disable the Static Mode function. When the Port Channel is enabled it does not transmit or process received LAGPDUs i.e. the member ports do not transmit LAGPDUs and all the LAGPDUs it may receive are dropped. The factory default is Enable.
Load Balance	Click the drop-down menu to select the hashing algorithm for distribution of 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: <ol style="list-style-type: none"> 1. Source MAC, VLAN, Ethertype, and incoming port. 2. Destination MAC, VLAN, EtherType and incoming port. 3. Source/Destination MAC, VLAN, Ethertype, and incoming port. This is the factory default. 4. Source IP and Source TCP/UDP Port. 5. Destination IP and Destination TCP/UDP Port. 6. Source/Destination IP and source/destination TCP/UDP Port.
Port Channel Members	Displays a list of members of the Port Channel in Slot/Port form.
Slot/Port	Displays the Slot/Port identification of the Port Channel being configured. This field will not appear when a new Port Channel is being created.
Participation	Click the drop-down menu to exclude or include port participation. The default is exclude. There can be a maximum of 8 ports assigned to a Port Channel.
Membership Conflicts	Displays the membership state of other Port Channels. A port may only be a member of one Port Channel at a time. If the entry is blank, it is not currently a member of any Port Channel.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Status

The Port Channel Status page displays a summary of the details for each port channel. To access this page, click **Switching > Port Channel > Status**.

Port Channel Status

Port Channel	Port Channel Name	Port Channel Type	Admin Mode	Link State	STP Mode	Static Mode	Link Trap	Port Channel Members	Active Ports	Load Balance
LAG1	ch1	Static	Enable	Down	Enable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port
LAG2	ch2	Static	Enable	Down	Enable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port
LAG3	ch3	Static	Enable	Down	Enable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port
LAG4	ch4	Static	Enable	Down	Enable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port
LAG5	ch5	Static	Enable	Down	Enable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port
LAG6	ch6	Static	Enable	Down	Enable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port
LAG7	ch7	Static	Enable	Down	Enable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port
LAG8	ch8	Static	Enable	Down	Enable	Enable	Disable			3 Src/Dest MAC, VLAN, EType, incoming port

Refresh

Figure 3-112. Switching > Port Channel > Status

The following table describes the items in the previous menu.

Table 3-109. Switching > Port Channel > Status

Parameter	Description
Port Channel	Displays the Slot/Port identification of the Port Channel.
Port Channel Name	Displays the name of the Port Channel.
Port Channel Type	Displays the type of this Port Channel.
Admin Mode	Displays the Administrative Mode of the Port Channel, enable or disable.
Link State	Displays the link status: up or down.
STP Mode	Displays the Spanning Tree Protocol Administrative Mode associated with the Port Channel. The possible values are: <ul style="list-style-type: none"> • Disable - spanning tree is disabled for this Port Channel. • Enable - spanning tree is enabled for this Port Channel.
Static Mode	Displays the Static Mode of the Port Channel, enable or disable.
Link Trap	Displays the trap state policy for a status changes. The factory default is Enable.
Port Channel Members	Displays the ports that are members of the Port Channel, in Slot/Port notation. There can be a maximum of 8 ports assigned to a Port Channel.
Active Ports	Displays a listing of the ports that are actively participating members of this Port Channel, in Slot/Port notation. There can be a maximum of 8 ports assigned to a Port Channel.

Table 3-109. Switching > Port Channel > Status (Continued)

Parameter	Description
Load Balance	Displays the Load balance policy of the Port Channel. The possible values are: <ul style="list-style-type: none"> • Source MAC, VLAN, Ethertype, and source port • Destination MAC, VLAN, EtherType and source port • Source/Destination MAC, VLAN, Ethertype, and source port • Source IP and Source TCP/UDP Port • Destination IP and Destination TCP/UDP Port • Source/Destination IP and source/destination TCP/UDP Port
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.4.9 X-Ring Pro

Configuration

The X-Ring Pro Configuration page allows users to configure the settings for each ring ID. To access this page, click **Switching > X-Ring Pro > Configuration**.

X-Ring+ Configuration

The screenshot shows the configuration interface for X-Ring Pro. It includes a form with the following fields: Ring ID (text input), Mode (dropdown menu with 'Ring' selected), Interface 1 (dropdown menu with 'ge0/1' selected), and Interface 2 (dropdown menu with 'ge0/1' selected). Below the form is a table header with columns: Ring ID, Mode, Interface 1, Interface 2, and Master Ring. At the bottom of the form area are 'Create' and 'Delete' buttons.

Figure 3-113. Switching > X-Ring Pro > Configuration

The following table describes the items in the previous menu.

Table 3-110. Switching > X-Ring Pro > Configuration

Parameter	Description
Ring ID	Specifies a number ranging from 1 to 99 to identify a given X-Ring group.
Mode	Click the drop-down menu to select the mode of the X-Ring group. The value is either "Ring" or "Coupling". The default value is "Ring". <ul style="list-style-type: none"> • The X-Ring group denoted as mode "Ring" means this switch is connected to the other switches to form a ring topology. • The X-Ring group denoted as "Coupling" means this switch is used to inter-connect two X-Ring networks.
Interface 1	Click the drop-down menu to select the first member interface for the X-Ring group. The value is either physical port or LAG (Link-Aggregation-Group) port.

Table 3-110. Switching > X-Ring Pro > Configuration (Continued)

Parameter	Description
Interface 2	Click the drop-down menu to select the secondary member interface for the X-Ring group. <ul style="list-style-type: none"> For the X-Ring group denoted as "Ring", the value is either physical port or LAG (Link-Aggregation-Group) port. For the X-Ring group denoted as "Coupling", the value is physical port or LAG (Link-Aggregation-Group) port or "None". The value "None" implies that the X-Ring group is not created for coupling dual-homing application.
Ring ID	Displays the Ring ID.
Mode	Displays the configured mode for the selected ring.
Interface 1	Displays the configured interface port for the selected ring.
Interface 2	Displays the configured interface port for the selected ring.
Master Ring	Displays the selected master ring for the selected ring.
Create	Click Create to make a new X-Ring group in accordance to "Ring ID" and the other values specified on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Click Delete to remove a current X-Ring group in accordance to "Ring ID" specified on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Status

The X-Ring Pro Status page displays a summary of the details for each ring ID. To access this page, click **Switching > X-Ring Pro > Status**.

X-Ring+ Status

Ring ID	Mode	Operation State	Interface 1	Forward State	Interface 2	Forward State	Master Ring
Refresh							

Figure 3-114. Switching > X-Ring Pro > Status

The following table describes the items in the previous menu.

Table 3-111. Switching > X-Ring Pro > Status

Parameter	Description
Ring ID	Displays a number ranging from 1 to 99 to identify a given X-Ring group.
Mode	Displays the mode of the X-Ring group. The value is either "Ring" or "Coupling". The default value is "Ring". <ul style="list-style-type: none"> The X-Ring group denoted as mode "Ring" means it is a switch connected to the other switches to form a ring topology. The X-Ring group denoted as "Coupling" means it is a switch that is used to inter-connect two X-Ring networks.

Table 3-111. Switching > X-Ring Pro > Status (Continued)

Parameter	Description
Operation State	<p>Displays the run-time operation state of the X-Ring group.</p> <ul style="list-style-type: none"> For the X-Ring group denoted as “Ring”, the value is “Standby”, “Edge”, “Master” or “Transit”. For the ring topology, there would be exactly one switch stays in master state and one of two Ring interfaces is set in blocking state. For the X-Ring group denoted as “Coupling”, the value is “Disconnect”, “Backup”, or “Primary”. There would be maximum one coupling path stays in “Primary” to forward traffic between two X-Ring networks.
Interface 1	Displays the first member interface for the X-Ring group. The value is either physical port or LAG (Link-Aggregation-Group) port.
Interface 2	<p>Displays the secondary member interface for the X-Ring group.</p> <ul style="list-style-type: none"> For the X-Ring group denoted as “Ring”, the value is either physical port or LAG (Link-Aggregation-Group) port. For the X-Ring group denoted as “Coupling”, the value is physical port or LAG (Link-Aggregation-Group) port or “None”. The value “None” implies the X-Ring group is created not for coupling dual-homing application.
Forward State	<p>Displays the spanning tree state of the member interface of an X-Ring group. The value is “Discarding” or “Forwarding”.</p> <ul style="list-style-type: none"> Discarding - Discard traffic in both ingress and egress directions. Forwarding - Forward ingress traffic bases on the result of forwarding database lookup.
Master Ring	Displays the X-Ring network that is coupling connected by the X-Ring group denoted as “Coupling”. This field is required for the X-Ring coupling application only.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.4.10 Spanning Tree

Global Configuration/Status

The Spanning Tree Switch Configuration/Status page allows users to configure the settings for the spanning tree. To access this page, click **Switching > Spanning Tree > Global Con-figuration/Status**.

Spanning Tree Switch Configuration/Status

Spanning Tree Admin Mode Enable ▾

Force Protocol Version IEEE 802.1w ▾

Configuration Name (1 to 31 characters)

Configuration Revision Level (0 to 65535)

Configuration Digest Key

Configuration Format Selector

MST ID	VID	FID
0	1	1

Figure 3-115. Switching > Spanning Tree > Global Configuration/Status

The following table describes the items in the previous menu.

Table 3-112. Switching > Spanning Tree > Global Configuration/Status

Parameter	Description
Spanning Tree Admin Mode	Click to the drop-down menu to enable or disable the spanning tree operation.
Force Protocol Version	Click to the drop-down menu to specify the Force Protocol Version parameter for the switch, options: IEEE 802.1d, IEEE 802.1w and IEEE 802.1s.
Configuration Name	Enter the identifier used to identify the configuration currently being used. It may be up to 31 characters, default: MAC address.
Configuration Revision Level	Enter the identifier used to identify the configuration currently being used. The values allowed are between 0 and 65535 (default: 0).
Configuration Digest Key	Displays the identifier used to identify the configuration currently being used.
MST ID	Displays the table consisting of the MST instances (including the CST) and the corresponding VLAN IDs associated with each of them.
VID	Displays the table consisting of the VLAN IDs and the corresponding FID.
FID	Displays the table consisting of the FIDs and the corresponding VLAN IDs associated with each of them.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

CST Configuration/Status

The Spanning Tree CST Configuration/Status page allows users to configure bridge, BPDU, and hold counts. To access this page, click **Switching > Spanning Tree > CST Configuration/Status**.

Spanning Tree CST Configuration/Status

Bridge Priority	<input type="text" value="32768"/> (0 to 61440)
Bridge Max Age (secs)	<input type="text" value="20"/> (6 to 40)
Bridge Hello Time (secs)	2
Bridge Forward Delay (secs)	<input type="text" value="15"/> (4 to 30)
Spanning Tree Maximum Hops	<input type="text" value="20"/> (6 to 40)
BPDU Guard	<input type="button" value="Disable"/>
BPDU Filter	<input type="button" value="Disable"/>
Spanning Tree Tx Hold Count	<input type="text" value="5"/> (1 to 10)
Bridge Identifier	80:00:C0:00:C9:75:16:FF
Time Since Topology Change	0 day 18 hr 10 min 10 sec
Topology Change Count	0
Topology Change	False
Designated Root	80:00:C0:00:C9:75:16:FF
Root Path Cost	0
Root Port	00:00
Max Age (secs)	20
Forward Delay (secs)	15
Hold Time (secs)	6
CST Regional Root	80:00:C0:00:C9:75:16:FF
CST Path Cost	0

Figure 3-116. Switching > Spanning Tree > CST Configuration/Status

The following table describes the items in the previous menu.

Table 3-113. Switching > Spanning Tree > CST Configuration/Status

Parameter	Description
Bridge Priority	Enter the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 to 61440. It is set in multiples 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. If it is tried to be set to any value between 4096 and (2*4096-1) it will be set to 4096 and so on. The default priority is 32768.
Bridge Max Age (secs)	Enter the bridge max age in seconds for the Common and Internal Spanning tree (CST). The value lies between 6 to 40, with the value being 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)	Displays the bridge hello time in seconds for the Common and Internal Spanning tree (CST). According to IEEE 802.1Q-REV 2005 updating hello time is disallowed.
Bridge Forward Delay (secs)	Enter the time spent in "Listening and Learning" mode before forwarding packets. Bridge Forward Delay must be greater or equal to "(Bridge Max Age / 2) + 1". The time range is from 4 to 30 seconds. The default value is 15.
Spanning Tree Maximum Hops	Enter the maximum number of hops for the Spanning tree. The valid range is 6 to 40. Default value is 20.

Table 3-113. Switching > Spanning Tree > CST Configuration/Status (Continued)

Parameter	Description
Spanning Tree Tx Hold Count	Click the drop-down menu to configure the maximum number of BPDUs the bridge is allowed to send within the hello time window. The valid range is 1 to 10. The default value is 6.
BPDU Guard	Click the drop-down menu to enable or disable BPDU guard. The default is Disable.
BPDU Filter	Click the drop-down menu to enable or disable the BPDU Filter to filter the BPDU traffic on the edge ports. The possible values are Enable or Disable. The value is disabled by default.
Spanning Tree Tx Hold Count	Enter a value (1 to 10) to set the Tx holding counter.
Time Since Topology Change	Displays the time in seconds since the topology of the CST last changed.
Topology Change Count	Displays the number of times topology has changed for the CST.
Topology Change	Displays the value of the topology change parameter for the switch indicating if a topology change is in progress on any port assigned to the CST. It takes a value if True or False.
Designated Root	Displays the bridge identifier of the root bridge. It 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 the CST.
Root Port	Displays the port to access the Designated Root for the CST.
Max Age (secs)	Displays the path Cost to the Designated Root for the CST.
Forward Delay (secs)	Displays the derived value in seconds of the Root Port Bridge Forward Delay parameter.
Hold Time (secs)	Displays the minimum time in seconds between transmissions of Configuration BPDUs.
CST Regional Root	Displays the priority and base MAC address of the CST Regional Root.
CST Path Cost	Displays the path cost to the CST tree Regional Root.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

MST Configuration/Status

The Spanning Tree MST Configuration/Status page allows users to create MSTs and configure settings for each MST. To access this page, click **Switching > Spanning Tree > MST Configuration/Status**.

Spanning Tree MST Configuration/Status

The screenshot shows a web interface for configuring MST. It includes a dropdown menu for selecting an existing MST, a 'Create' button to add a new one, an input field for the MST ID (ranging from 1 to 4094), and a 'Submit' button.

Figure 3-117. Switching > Spanning Tree > MST Configuration/Status

The following table describes the items in the previous menu.

Table 3-114. Switching > Spanning Tree > MST Configuration/Status

Parameter	Description
MST	Click the drop-down menu to create a new MST or select an existing one to configure.
MST ID	Enter This is only visible when the select option of the MST ID select box is selected. The ID of the MST being created. Valid values for this are between 1 and 4094.
Priority	Enter the bridge priority for the MST instance selected. The value lies between 0 to 61440. The bridge priority is set in multiples 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. If it is tried to be set to any value between 4096 and $(2*4096-1)$ it will be set to 4096 and so on. The default priority is 32768.
Associated VLANs	Click the drop-down menu to add or delete an associated VLAN to this entry. Non-configured VLANs can be added to or deleted from the MST instance by selecting Add/Delete option and entering the VLAN ID in the VLAN ID - Individual/Range text-box.
Bridge Identifier	Displays 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 time in seconds since the topology of the selected MST instance last changed.
Topology Change Count	Displays the number of times topology has changed for the selected MST instance.
Topology Change	Displays the value of the topology change parameter for the switch indicating if a topology change is in progress on any port assigned to the selected MST instance. It takes a value if True or False.
Designated Root	Displays the bridge identifier of the root bridge. It 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	Displays the port to access the Designated Root for this MST instance.

Table 3-114. Switching > Spanning Tree > MST Configuration/Status (Continued)

Parameter	Description
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.
Delete Instance	Click Delete Instance to remove the selected MST instance. All VLANs associated with the instance are associated with the CST

CST Interface Configuration/Status

The Spanning Tree CST Port Configuration/Status page allows users to configure bridge, BPDU, and hold counts. To access this page, click **Switching > Spanning Tree > CST Interface Configuration/Status**.

Spanning Tree MST Port Configuration Status

No MSTs Available

Figure 3-118. Switching > Spanning Tree > CST Interface Configuration/Status

The following table describes the items in the previous menu.

Table 3-115. Switching > Spanning Tree > CST Interface Configuration/Status

Parameter	Description
Interface	Click the drop-down menu to select one of the physical or port channel interfaces associated with VLANs associated with the CST.
Port Priority	Enter the priority for a particular port within the CST. The port priority is set in multiples of 16. For example if the priority is attempted to be set to any value between 0 and 15, it will be set to 0. If it is tried to be set to any value between 16 and (2*16-1) it will be set to 16 and so on. The valid range is from 0 to 240. Default priority is 128.
Admin Edge Port	Click the drop-down menu to enable or disable the specification port of the Edge Port within the CIST. It takes a value of enable or disable, where the default value is disable.
Port Path Cost	Enter the 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 0 to 200000000. Enter '0' to set the path cost value automatically on the basis of Link Speed. Default value is 0.
External Port Path Cost	Displays the external Path Cost to a new value for the specified port in the spanning tree. It takes a value in the range of 0 to 200000000. Enter '0' to set the external path cost value automatically on the basis of Link Speed. Default value is 0.
BPDU Filter	Click the drop-down menu to enable or disable the BPDU Filter, filters the BPDU traffic on this port when STP is enabled on this port. The possible values are Enable or Disable. It is disabled by default.
BPDU Flood	Click the drop-down menu to enable or disable the BPDU Flood, floods the BPDU traffic arriving on this port when STP is disabled on this port. The possible values are Enable or Disable. It is disabled by default.

Table 3-115. Switching > Spanning Tree > CST Interface Configuration/Status (Continued)

Parameter	Description
Port Mode	Click the drop-down menu to enable or disable the Spanning Tree Protocol Administrative Mode associated with the port or port channel. The possible values are Enable or Disable. It is disabled by default.
Port Forwarding State	Displays the State of this port (Forwarding/Learning/Discarding/Manual forwarding/Not participating/Disabled). * indicates Loop inconsistent state. Refer to Loop Guard for more information.
Port Role	Displays 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	Displays the Root Bridge for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Designated Cost	Displays the path cost offered to the LAN by the Designated Port.
Designated Bridge	Displays the 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	Displays the 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	Displays 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	Click the drop-down menu to enable or disable the auto edge 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. It is disabled by default.
Edge Port	Displays the status of the edge port (enabled or disabled). It takes the value "Enabled" or "Disabled".
Point-to-point MAC	Displays the derived value of the point-to-point status.
Root Guard	Click the drop-down menu to enable or disable 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. It is disabled by default.
Loop Guard	Click the drop-down menu to enable or disable 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. It is disabled by default.
TCN Guard	Click the drop-down menu to enable or disable 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. It is disabled by default.
CST Regional Root	Displays the bridge identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
CST Path Cost	Displays the path cost to the CST Regional Root.

Table 3-115. Switching > Spanning Tree > CST Interface Configuration/Status (Continued)

Parameter	Description
Loop Inconsistent State	Displays the loop inconsistent state status for the port.
Transitions Into Loop Inconsistent State	Displays the number of times this interface has transitioned into loop inconsistent state.
Transitions Out Of Loop Inconsistent State	Displays the number of times this interface has transitioned out of loop inconsistent state.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.
Force	Click Force to push the port to send out 802.1w or 802.1d BPDUs.

MST Interface Configuration/Status

The Spanning Tree MST Port Configuration/Status page allows users to configure the set-tings for MST ports. To access this page, click **Switching > Spanning Tree > MST Interface Configuration/Status**.

Spanning Tree MST Port Configuration Status

No MSTs Available

Figure 3-119. Switching > Spanning Tree > MST Interface Configuration/Status

The following table describes the items in the previous menu.

Table 3-116. Switching > Spanning Tree > MST Interface Configuration/Status

Parameter	Description
MST ID	Click the drop-down menu to select one MST instance from existing MST instances.
Interface	Click the drop-down menu to select one of the physical or port channel interfaces associated with VLANs associated with the selected MST instance.
Port Priority	Enter the priority for a particular port within the selected MST instance. The port priority is set in multiples of 16. For example if the priority is attempted to be set to any value between 0 and 15, it will be set to 0. If it is tried to be set to any value between 16 and (2*16-1) it will be set to 16 and so on. The valid range is from 0 to 240. Default priority is 128.
Port Path Cost	Enter the variable to 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 0 to 200000000. Enter '0' to set the path cost value automatically on the basis of Link Speed. Default value is 0.
Auto-calculate Port Path Cost	Displays whether the path cost is automatically calculated (Enabled) or not (Disabled). Path cost will be calculated based on the link speed of the port if the configured value for Port Path Cost is zero.

Table 3-116. Switching > Spanning Tree > MST Interface Configuration/Status (Continued)

Parameter	Description
Port ID	Displays the port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Up Time Since Counters Last Cleared	Displays the time since the counters were last cleared, displayed in Days, Hours, Minutes, and Seconds.
Port Mode	Displays the Spanning Tree Protocol Administrative Mode associated with the port or port channel. The possible values are Enable or Disable.
Port Forwarding State	Displays the State of this port (Forwarding/Learning/Discarding). * indicates Loop inconsistent state. Refer to Loop Guard for more information.
Port Role	Displays 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	Displays the 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 the path cost offered to the LAN by the Designated Port.
Designated Bridge	Displays the 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	Displays the 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	Displays the parameter identifies whether the port is in a loop inconsistent state in the specified MST instance.
Transitions Into Loop Inconsistent State	Displays the number of times this interface has transitioned into loop inconsistent state.
Transitions Out Of Loop Inconsistent State	Displays the number of times this interface has transitioned out of loop inconsistent state.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Statistics

The Spanning Tree Statistics page displays received and transmitted BPDU information for STP, RSTP, and MSTP. To access this page, click **Switching > Spanning Tree > Statistics**.

Spanning Tree Statistics

Interface	ge0/1
STP BPDUs Received	0
STP BPDUs Transmitted	0
RSTP BPDUs Received	0
RSTP BPDUs Transmitted	0
MSTP BPDUs Received	0
MSTP BPDUs Transmitted	0

Figure 3-120. Switching > Spanning Tree > Statistics

The following table describes the items in the previous menu.

Table 3-117. Switching > Spanning Tree > Statistics

Parameter	Description
Interface	Click the drop-down menu to select one of the physical or port channel interfaces of the switch.
STP BPDUs Received	Displays the number of STP BPDUs received at the selected port.
STP BPDUs Transmitted	Displays the number of STP BPDUs transmitted from the selected port.
RSTP BPDUs Received	Displays the number of RSTP BPDUs received at the selected port.
RSTP BPDUs Transmitted	Displays the number of RSTP BPDUs transmitted from the selected port.
MSTP BPDUs Received	Displays the number of MSTP BPDUs received at the selected port.
MSTP BPDUs Transmitted	Displays the number of MSTP BPDUs transmitted from the selected port.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.4.11 Flow Control

The Flow Control page allows users to enable or disable the flow control mode. To access this page, click **Switching > Flow Control**.

Switch Configuration

Figure 3-121. Switching > Flow Control

The following table describes the items in the previous menu.

Table 3-118. Switching > Flow Control

Parameter	Description
802.3x Flow Control Mode	Click the drop-down menu to enable or disable this option by selecting the corresponding line on the pull-down entry field. The factory default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

3.5. Multicast

3.5.1 IGMP Snooping

Global Configuration and Status

The IGMP Snooping Global Configuration and Status page allows users to enable or disable admin mode and assign VLAN IDs for IGMP snooping. To access this page, click **Multicast > IGMP Snooping > Global Configuration and Status**.

IGMP Snooping Global Configuration and Status

Figure 3-122. Multicast > IGMP Snooping > Global Configuration and Status

The following table describes the items in the previous menu.

Table 3-119. Multicast > IGMP Snooping > Global Configuration and Status

Parameter	Description
Admin Mode	Click the drop-down menu to select the administrative mode for IGMP Snooping for the switch from the pull-down menu. The default is Disable.
Multicast Control Frame Count	Displays the number of multicast control frames that are processed by the CPU.
Interfaces Enabled for IGMP Snooping	Displays a list of all the interfaces currently enabled for IGMP Snooping.
Data Frames Forwarded by the CPU	Displays the number of data frames forwarded by the CPU.
VLAN IDs Enabled For IGMP Snooping	Enter the VLAN IDs enabled for IGMP snooping.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Configuration

The Snooping Interface Configuration page allows users to configure snooping settings for each interface. To access this page, click **Multicast > IGMP Snooping > Interface Configuration**.

IGMP Snooping Interface Configuration

Figure 3-123. Multicast > IGMP Snooping > Interface

Configuration The following table describes the items in the previous menu.

Table 3-120. Multicast > IGMP Snooping > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the single select box lists all physical, VLAN and LAG interfaces. Select the interface you want to configure.
Admin Mode	Click the drop-down menu to disable or enable the interface mode for the selected interface for IGMP Snooping for the switch from the pull-down menu. The default is Disable.

Table 3-120. Multicast > IGMP Snooping > Interface Configuration (Continued)

Parameter	Description
Group Membership Interval	Enter 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 value is 260 seconds. The configured value must be greater than the Max Response Time.
Max Response Time (Less Than Group Membership Interval)	Enter 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. The valid range is 1 to 25 seconds. 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	Enter the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite timeout, i.e. no expiration.
Fast Leave Admin Mode	Click the drop-down menu to enable or disable the Fast Leave mode for the a particular interface from the pull-down menu. The default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

VLAN Status

The IGMP Snooping VLAN Status displays the summary of the IGMP snooping configuration. To access this page, click **Multicast > IGMP Snooping > VLAN Status**.

IGMP Snooping VLAN Status

VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval (secs)	Max Response Time (secs)	Multicast Router Expiry Time (secs)
Refresh					

Figure 3-124. Multicast > IGMP Snooping > VLAN Status

The following table describes the items in the previous menu.

Table 3-121. Multicast > IGMP Snooping > VLAN Status

Parameter	Description
VLAN ID	Displays all VLAN IDs for which the IGMP Snooping mode is Enabled.
Admin Mode	Displays IGMP Snooping Mode for VLAN ID.
Fast Leave Admin Mode	Displays the Fast Leave Mode for VLAN ID.
Group Membership Interval (secs)	Displays the Group Membership Interval of IGMP Snooping for the specified VLAN ID. Valid range is 2 to 3600 seconds. Its value should be greater than maximum response time.

Table 3-121. Multicast > IGMP Snooping > VLAN Status (Continued)

Parameter	Description
Maximum Response Time (secs)	Displays the Maximum Response Time of IGMP Snooping for the specified VLAN ID. Valid range is 1 to 25 seconds. Its value should be less than group membership value.
Multicast Router Expiry Time (secs)	Displays the Multicast Router Expiry Time of IGMP Snooping for the specified VLAN ID. Valid range is 0 to 3600 seconds.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

VLAN Configuration

The IGMP Snooping VLAN Configuration page allows users to configure IGMP snooping VLAN settings. To access this page, click **Multicast > IGMP Snooping > VLAN Configuration**.

IGMP Snooping VLAN Configuration

VLAN ID	<input type="text" value="New Entry"/>	
VLAN ID	<input type="text"/>	(1 to 4093)
Admin Mode	Enable	
Fast Leave Admin Mode	<input type="text" value="Disable"/>	
Group Membership Interval	<input type="text" value="260"/>	((Max Response Time + 1) to 3600 secs)
Maximum Response Time	<input type="text" value="10"/>	(1 to 25 secs)
Multicast Router Expiry Time	<input type="text" value="0"/>	(0 to 3600 secs)

Figure 3-125. Multicast > IGMP Snooping > VLAN Configuration

The following table describes the items in the previous menu.

Table 3-122. Multicast > IGMP Snooping > VLAN Status

Parameter	Description
VLAN ID	Click the drop-down menu to select create or select a VLAN ID for IGMP Snooping.
VLAN ID	Enter the name of the VLAN ID. Appears when New Entry is selected in VLAN ID combo box. Specifies VLAN ID for which pre-configurable Snooping parameters are to be set.
Admin Mode	Displays the status of the mode for the IGMP Snooping entry.
Fast Leave Admin Mode	Click the drop-down menu to enable or disable the IGMP Snooping Fast Leave Mode for the specified VLAN ID. Fast Leave Admin Mode is disabled by default.
Group Membership Interval	Enter the value for group membership interval of IGMP Snooping for the specified VLAN ID. Valid range is 2 to 3600 seconds. The default value is 260 seconds. The configured value must be greater than the Max Response Time.
Maximum Response Time	Enter the value for maximum response time of IGMP Snooping for the specified VLAN ID. Valid range is 1 to 25 seconds. Its value should be less than Group Membership Interval value. Default value is 10 seconds.

Table 3-122. Multicast > IGMP Snooping > VLAN Status (Continued)

Parameter	Description
Multicast Router Expiry Time	Enter the value for multicast router expiry time of IGMP Snooping for the specified VLAN ID. Valid range is 0 to 3600 seconds. Default value is 0.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Click Delete to remove created entry.

Multicast Router Status

The IGMP Snooping Multicast Router Status displays the multicast router settings for each interface. To access this page, click **Multicast > IGMP Snooping > Multicast Router Status**.

IGMP Snooping Multicast Router Status

Figure 3-126. Multicast > IGMP Snooping > Multicast Router Status

The following table describes the items in the previous menu.

Table 3-123. Multicast > IGMP Snooping > Multicast Router Status

Parameter	Description
Interface	Click the drop-down menu to select a interface. Select the interface for which you want to display the status.
Multicast Router	Displays for the selected interface whether multicast router is enable or disabled.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Multicast Router Configuration

The IGMP Snooping Multicast Router Configuration page allows users to enable or disable the multicast router for each interface. To access this page, click **Multicast > IGMP Snooping > Multicast Router Configuration**.

IGMP Snooping Multicast Router Configuration

Figure 3-127. Multicast > IGMP Snooping > Multicast Router Configuration

The following table describes the items in the previous menu.

Table 3-124. Multicast > IGMP Snooping > Multicast Router Configuration

Parameter	Description
Interface	Click the drop-down menu to select an interface. Select the interface for which you want Multicast Router to be enabled.
Multicast Router	Click the drop-down menu to enable or disable Multicast Router on the selected interface.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Multicast Router VLAN Status

The IGMP Snooping Multicast Router VLAN Status displays the VLAN ID and multicast router status for each interface. To access this page, click **Multicast > IGMP Snooping > Multicast Router VLAN Status**.

IGMP Snooping Multicast Router VLAN Status

The screenshot shows a web interface for configuring Multicast Router VLAN Status. At the top, there is a form with a label 'Interface' and a dropdown menu currently showing 'ge0/1'. Below the form is a table with two columns: 'VLAN ID' and 'Multicast Router'. Below the table is a 'Refresh' button.

Figure 3-128. Multicast > IGMP Snooping > Multicast Router VLAN Status

The following table describes the items in the previous menu.

Table 3-125. Multicast > IGMP Snooping > Multicast Router VLAN Status

Parameter	Description
Interface	Click the drop-down menu to select an interface. Select the interface for which you want to display the status.
VLAN ID	Displays All VLAN IDs for which the Multicast Router Mode is Enabled.
Multicast Router	Displays the Multicast Router Mode for VLAN ID.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Multicast Router VLAN Configuration

The IGMP Snooping Multicast Router VLAN Configuration page allows users to configure the VLAN ID and multicast router status for each interface. To access this page, click **Multi-cast > IGMP Snooping > Multicast Router VLAN Configuration**.

IGMP Snooping Multicast Router VLAN Configuration

Figure 3-129. Multicast > IGMP Snooping > Multicast Router VLAN Configuration

The following table describes the items in the previous menu.

Table 3-126. Multicast > IGMP Snooping > Multicast Router VLAN Configuration

Parameter	Description
Interface	Click the drop-down menu to select an interface. Select the interface for which you want Multicast Router to be enabled.
VLAN ID	Enter a VLAN ID for which the Multicast Router Mode is to be Enabled or Disabled. Valid range is 1 to 4093.
Multicast Router	Click the drop-down menu to enable or disable the multicast router function. The value is enabled by default.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

IGMP Snooping Table

The MFDB IGMP Snooping Table displays the type, description, and interface for each MAC address. To access this page, click **Multicast > IGMP Snooping > IGMP Snooping Table**.

MFDB IGMP Snooping Table

Figure 3-130. Multicast > IGMP Snooping > IGMP Snooping Table

The following table describes the items in the previous menu.

Table 3-127. Multicast > IGMP Snooping > IGMP Snooping Table

Parameter	Description
MAC Address	Displays 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	Displays the type of the entry. Static entries are those that are configured by the user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	Displays the text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
Interface(s)	Displays the list of interfaces that are designated for forwarding (Fwd:).
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.
Clear Entries	Click Clear Entries to remove IGMP Snooping entries from the multicast forwarding database.

3.5.2 IGMP Snooping Querier

Configuration

The IGMP Snooping Querier Configuration page allows users to configure the IGMP snooping querier settings. To access this page, click **Multicast > IGMP Snooping Querier > Configuration**.

IGMP Snooping Querier Configuration

Snooping Querier Admin Mode	<input type="text" value="Disable"/>
Snooping Querier Address	<input type="text" value="0.0.0.0"/>
IGMP Version	<input type="text" value="2"/> (1 to 2)
Query Interval(secs)	<input type="text" value="60"/> (1 to 1800)
Querier Expiry Interval(secs)	<input type="text" value="60"/> (60 to 300)

Figure 3-131. Multicast > IGMP Snooping Querier > Configuration

The following table describes the items in the previous menu.

Table 3-128. Multicast > IGMP Snooping Querier > Configuration

Parameter	Description
Snooping Querier Admin Mode	Click the drop-down menu to enable or disable the administrative mode for IGMP Snooping for the switch from the pull-down menu. The default is disable.
Snooping Querier Address	Enter 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	Enter the IGMP protocol version used in periodic IGMP queries. IGMP queries.

Table 3-128. Multicast > IGMP Snooping Querier > Configuration (Continued)

Parameter	Description
Query Interval (secs)	Enter 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 (secs)	Enter 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.
Submit	click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

VLAN Configuration

The IGMP Snooping Querier VLAN Configuration page allows users to configure IGMP Snooping Querier VLAN settings. To access this page, click **Multicast > IGMP Snooping Querier > VLAN Configuration**.

IGMP Snooping Querier VLAN Configuration

The screenshot shows a configuration form for IGMP Snooping Querier VLAN. It includes a 'VLAN ID' field with a 'New Entry' dropdown menu, a 'Querier Election Participate Mode' dropdown menu set to 'Disable', and a 'Snooping Querier VLAN Address' text input field. Below the form are 'Submit' and 'Refresh' buttons.

Figure 3-132. Multicast > IGMP Snooping Querier > VLAN Configuration

The following table describes the items in the previous menu.

Table 3-129. Multicast > IGMP Snooping Querier > VLAN Configuration

Parameter	Description
VLAN ID	Selects the VLAN ID on which IGMP Snooping Querier is enabled.
VLAN ID	Appears when "New Entry" is selected in VLAN ID selection list. Specifies VLAN ID for which IGMP Snooping Querier is to be enabled. User can also set pre-configurable Snooping Querier parameters. The value ranges from 1 to 4093.
Querier Election Participate Mode	Enable or disable the IGMP Snooping Querier participate in election mode. When this mode is disabled, up on seeing other querier of same version in the VLAN, the snooping querier move to non-querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least IP address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state. The mode is enabled by default.
Snooping Querier VLAN Address	Enter the Snooping Querier Address to be used as source address in periodic IGMP queries sent on the specified VLAN.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Table 3-129. Multicast > IGMP Snooping Querier > VLAN Configuration (Continued)

Parameter	Description
Delete	Click Delete to disable Snooping Querier on the selected VLAN. This button is not visible when a VLAN is not selected.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

VLAN Configuration Summary

The IGMP Snooping Querier VLAN Configuration Summary page displays the participation mode and VLAN address for each VLAN ID. To access this page, click **Multicast > IGMP Snooping Querier > VLAN Configuration Summary**.

IGMP Snooping Querier VLAN Configuration Summary

VLAN ID	Querier Election Participate Mode	Snooping Querier VLAN Address
Refresh		

Figure 3-133. Multicast > IGMP Snooping Querier > VLAN Configuration Summary The following table describes the items in the previous menu.

Table 3-130. Multicast > IGMP Snooping Querier > VLAN Configuration Summary

Parameter	Description
VLAN ID	Displays the VLAN ID on which IGMP Snooping Querier is administratively enabled.
Querier Election Participate Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, upon seeing a query of the same version in the VLAN, the snooping querier moves to non-querier state. Only when this mode is enabled, the snooping querier will participate in querier election where the least IP address will win the querier election and 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.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

VLAN Status

The IGMP Snooping Querier VLAN Status displays the operation and last querier status for each VLAN ID. To access this page, click **Multicast > IGMP Snooping Querier > VLAN Status**.

IGMP Snooping Querier VLAN Status

VLAN ID	Operational State	Operational Version	Last Querier Address	Last Querier Version	Operational Max Response Time(secs)
Refresh					

Figure 3-134. Multicast > IGMP Snooping Querier > VLAN Status

The following table describes the items in the previous menu.

Table 3-131. Multicast > IGMP Snooping Querier > VLAN Status

Parameter	Description
VLAN ID	Displays the VLAN ID on which IGMP Snooping Querier is administratively enabled and VLAN exists in the VLAN database.
Operational State	Displays the operational state of the IGMP Snooping Querier on a VLAN. It can be in any of the following states: <ul style="list-style-type: none"> Querier - 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, it moves to non-querier mode. Non-Querier - Snooping switch is in Non-Querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch will move into querier mode. Disabled - Snooping Querier is not operational on the VLAN. The Snooping Querier moves to disabled mode when IGMP Snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.
Operational Version	Displays the operational IGMP protocol version of the 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 (secs)	Displays maximum response time to be used in the queries that are sent by the Snooping Querier.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.5.3 MLD Snooping

Configuration and Status

The MLD Snooping Configuration and Status page allows users to enable or disable admin mode, and enable VLAN IDs for MLD snooping. To access this page, click **Multicast > MLD Snooping > Configuration and Status**.

MLD Snooping Configuration and Status

The screenshot shows a configuration page for MLD Snooping. It contains a form with the following elements:

- Admin Mode:** A drop-down menu currently set to "Disable".
- Multicast Control Frame Count:** A text input field containing the value "U".
- Interfaces Enabled for MLD Snooping:** A text input field that is currently empty.
- Data Frames Forwarded by the CPU:** A text input field containing the value "0".
- VLAN IDs Enabled for MLD Snooping:** A text input field that is currently empty.

At the bottom of the form, there are two buttons: "Submit" and "Refresh".

Figure 3-135. Multicast > MLD Snooping > Configuration and Status

The following table describes the items in the previous menu.

Table 3-132. Multicast > MLD Snooping > Configuration and Status

Parameter	Description
Admin Mode	Click the drop-down menu to enable or disable the administrative mode for MLD Snooping for the switch. The default is Disable.
Multicast Control Frame Count	Displays the number of multicast control frames that are processed by the CPU.
Interfaces Enabled for MLD Snooping	Displays all the interfaces currently enabled for MLD Snooping.
Data Frames Forwarded by the CPU	Displays the number of data frames forwarded by the CPU.
VLAN IDs Enabled For MLD Snooping	Displays VLAN IDs enabled for MLD snooping.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Configuration

The MLD Snooping Interface Configuration page allows users to configure the settings for MLD snooping. To access this page, click **Multicast > MLD Snooping > Interface Configuration**.

MLD Snooping Interface Configuration

The screenshot shows a configuration form with the following fields and values:

- Interface: ge0/1
- Admin Mode: Disable
- Group Membership Interval(secs): 260 (range: 2 to 3600 seconds)
- Max Response Time(secs)(Less Than Group Membership Interval): 10 (range: 1 to 65 seconds)
- Multicast Router Present Expiration Time(secs): 0 (range: 0 to 3600 seconds)
- Fast Leave Admin Mode: Disable

A Submit button is located at the bottom center of the form.

Figure 3-136. Multicast > MLD Snooping > Interface Configuration

The following table describes the items in the previous menu.

Table 3-133. Multicast > MLD Snooping > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the single select box lists all physical, VLAN and LAG interfaces. Select the interface you want to configure.
Admin Mode	Click the drop-down menu to enable or disable the interface mode for the selected interface for MLD Snooping for the switch. The default is Disable.
Group Membership Interval (secs)	Enter 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 configured value must be greater than Max Response Time. The default is 260 seconds.
Max Response Time (secs) (Less Than Group Membership Interval)	Enter 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 (secs)	Enter the amount of time you want the switch to wait to receive a query on an interface before removing it from the list of interfaces with multicast routers attached. Enter a value between 0 and 3600 seconds. The default is 0 seconds. A value of zero indicates an infinite timeout, i.e. no expiration.
Fast Leave Admin Mode	Enter the Fast Leave mode for a particular interface from the pull-down menu. The default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

VLAN Status

The MLD Snooping VLAN Status page displays the summary of the MLD snooping configuration for VLAN. To access this page, click **Multicast > MLD Snooping > VLAN Status**.

MLD Snooping VLAN Status

VLAN ID	Admin Mode	Fast Leave Admin Mode	Group Membership Interval (secs)	Max Response Time (secs)	Multicast Router Expiry Time (secs)
<input type="button" value="Refresh"/>					

Figure 3-137. Multicast > MLD Snooping > VLAN Status

The following table describes the items in the previous menu.

Table 3-134. Multicast > MLD Snooping > VLAN Status

Parameter	Description
VLAN ID	Displays all VLAN IDs for which the MLD Snooping mode is Enabled.
Admin Mode	Displays MLD Snooping Mode for VLAN ID.
Fast Leave Admin Mode	Displays fast Leave Mode for VLAN ID.
Group Membership Interval (secs)	Displays Group Membership Interval of MLD Snooping for the specified VLAN ID. Valid range is 2 to 3600.
Maximum Response Time (secs)	Displays Maximum Response Time of MLD Snooping for the specified VLAN ID. Valid range is 1 to 3599. Its value should be greater than group membership interval value.
Multicast Router Expiry Time (secs)	Displays Multicast Router Expiry Time of MLD Snooping for the specified VLAN ID. Valid range is 0 to 3600.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

VLAN Configuration

The MLD Snooping VLAN Configuration page allows users to configure MLD snooping VLAN settings. To access this page, click **Multicast > MLD Snooping > VLAN Configuration**.

MLD Snooping VLAN Configuration

VLAN ID	<input type="button" value="New Entry"/>
VLAN ID	<input type="text" value=""/> (1 to 4093)
Admin Mode	<input checked="" type="checkbox"/> Enable
Fast Leave Admin Mode	<input type="button" value="Disable"/>
Group Membership Interval	<input type="text" value="260"/> (2 to 3600 secs)
Maximum Response Time	<input type="text" value="10"/> (1 to 65 secs)
Multicast Router Expiry Time	<input type="text" value="0"/> (0 to 3600 secs)
<input type="button" value="Submit"/>	

Figure 3-138. Multicast > MLD Snooping > VLAN Configuration

The following table describes the items in the previous menu.

Table 3-135. Multicast > MLD Snooping > VLAN Configuration

Parameter	Description
VLAN ID	Click the drop-down menu to specify the list of VLAN IDs for which MLD Snooping is enabled.
VLAN ID	Enter a value for the VLAN ID. Appears when "New Entry" is selected in VLAN ID combo box. Specifies VLAN ID for which pre-configurable Snooping parameters are to be set.
Admin Mode	Displays the MLD Snooping status for the specified VLAN ID.
Fast Leave Admin Mode	Click the drop-down menu to enable or disable the MLD Snooping Fast Leave Mode for the specified VLAN ID.
Group Membership Interval	Enter the value for group membership interval of MLD Snooping for the specified VLAN ID. Valid range is (Maximum Response Time + 1) to 3600.
Maximum Response Time	Enter the value for maximum response time of MLD Snooping for the specified VLAN ID. Valid range is 1 to (Group Membership Interval - 1). Its value should be less than group membership interval value.
Multicast Router Expiry Time	Enter the value for multicast router expiry time of MLD Snooping for the specified VLAN ID. Valid range is 0 to 3600.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Click Delete to remove the switch with the default values.

Multicast Router Status

The MLD Snooping Multicast Router Status displays the multicast router settings for each interface. To access this page, click **Multicast > MLD Snooping > Multicast Router Status**.

MLD Snooping Multicast Router Status

Interface ge0/1 ▾

Multicast Router Disable

Figure 3-139. Multicast > MLD Snooping > Multicast Router Status

The following table describes the items in the previous menu.

Table 3-136. Multicast > MLD Snooping > Multicast Router Status

Parameter	Description
Interface	Click the drop-down menu to select the single select box lists all physical and LAG interfaces. Select the interface for which you want to display the status.
Multicast Router	Displays the multicast router status (enable or disable).
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Multicast Router Configuration

The MLD Snooping Multicast Router Configuration page allows users to enable or disable the multicast router for each interface. To access this page, click **Multicast > MLD Snooping > Multicast Router Configuration**.

MLD Snooping Multicast Router Configuration

The screenshot shows a configuration page with a form containing two dropdown menus. The first dropdown is labeled 'Interface' and has 'ge0/1' selected. The second dropdown is labeled 'Multicast Router Mode' and has 'Disable' selected. Below the form is a 'Submit' button.

Figure 3-140. Multicast > MLD Snooping > Multicast Router

Configuration The following table describes the items in the previous menu.

Table 3-137. Multicast > MLD Snooping > Multicast Router Configuration

Parameter	Description
Interface	Click the drop-down menu to select an interface. Select the interface for which you want Multicast Router to be enabled.
Multicast Router	Click the drop-down menu to enable or disable Multicast Router on the selected interface.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Multicast Router VLAN Status

The MLD Snooping Multicast Router VLAN Status displays the VLAN ID and multicast router status for each interface. To access this page, click **Multicast > MLD Snooping > Multicast Router VLAN Status**.

MLD Snooping Multicast Router VLAN Status

Figure 3-141. Multicast > MLD Snooping > Multicast Router VLAN Status

The following table describes the items in the previous menu.

Table 3-138. Multicast > MLD Snooping > Multicast Router VLAN Status

Parameter	Description
Interface	Click the drop-down menu to select a Slot/Port. Select the interface for which you want to display the status.
VLAN ID	Displays all VLAN IDs for which the Multicast Router Mode is Enabled.
Multicast Router	Displays the Multicast Router Mode for VLAN ID.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Multicast Router VLAN Configuration

The MLD Snooping Multicast Router VLAN Configuration page allows users to configure the VLAN ID and multicast router status for each interface. To access this page, click **Multicast > MLD Snooping > Multicast Router VLAN Configuration**.

MLD Snooping Multicast Router VLAN Configuration

Figure 3-142. Multicast > MLD Snooping > Multicast Router VLAN

Configuration The following table describes the items in the previous menu.

Table 3-139. Multicast > MLD Snooping > Multicast Router VLAN Configuration

Parameter	Description
Interface	Click the drop-down menu to select a Slot/Port. Select the interface for which you want Multicast Router to be enabled.
VLAN ID	Enter the VLAN ID for the Multicast Router Mode. Valid range is from 1 to 4093.

Table 3-139. Multicast > MLD Snooping > Multicast Router VLAN Configuration (Continued)

Parameter	Description
Multicast Router	Click the drop-down menu to enable or disable the VLAN ID, multicast router may be enabled or disabled using this.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

MLD Snooping Table

The MFDB MLD Snooping Table displays the type, description, and interface for each MAC address. To access this page, click **Multicast > MLD Snooping > MLD Snooping Table**.

MFDB MLD Snooping Table

MAC Address	Type	Description	Interface(s)
Refresh			

Figure 3-143. Multicast > MLD Snooping > MLD Snooping Table

The following table describes the items in the previous menu.

Table 3-140. Multicast > MLD Snooping > MLD Snooping Table

Parameter	Description
MAC Address	Displays 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	Displays the entry type. Static entries are those that are configured by the user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	Displays the text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
Interface(s)	Displays the list of interfaces that are designated for forwarding (Fwd:).
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.5.4 MLD Snooping Querier

Configuration

The MLD Snooping Querier Configuration page allows users to configure the MLD snooping querier settings. To access this page, click **Multicast > MLD Snooping Querier > Configuration**.

MLD Snooping Querier Configuration

Snooping Querier Admin Mode	<input type="text" value="Disable"/>
Snooping Querier Address	<input type="text" value="::"/>
MLD Version	<input type="text" value="1"/>
Query Interval(secs)	<input type="text" value="50"/> (1 to 1800)
Querier Expiry Interval(secs)	<input type="text" value="50"/> (60 to 300)

Figure 3-144. Multicast > MLD Snooping Querier > Configuration

The following table describes the items in the previous menu.

Table 3-141. Multicast > MLD Snooping Querier > Configuration

Parameter	Description
Snooping Querier Admin Mode	Click the drop-down menu to enable or disable the administrative mode for MLD Snooping for the switch from the pull-down menu. The default is disable.
Snooping Querier Address	Enter 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	Enter the MLD protocol version used in periodic MLD queries. MLD queries.
Query Interval (secs)	Enter 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 (secs)	Enter 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.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

VLAN Configuration

The MLD Snooping Querier VLAN Configuration page allows users to configure MLD Snooping Querier VLAN settings. To access this page, click **Multicast > MLD Snooping Querier > VLAN Configuration**.

MLD Snooping Querier VLAN Configuration

Figure 3-145. Multicast > MLD Snooping Querier > VLAN Configuration

The following table describes the items in the previous menu.

Table 3-142. Multicast > MLD Snooping Querier > VLAN Configuration

Parameter	Description
VLAN ID	Click the drop-down menu to select an existing configuration or create a new one.
VLAN ID	Enter a value for the VLAN ID. Appears when "New Entry" is selected in VLAN ID selection list. Specifies VLAN ID for which MLD Snooping Querier is to be enabled. User can also set pre-configurable Snooping Querier parameters.
Querier Election Participate Mode	Click the drop-down menu to enable or disable the MLD Snooping Querier participate. When this mode is disabled, up on seeing other querier of same version in the VLAN, the snooping querier move to non-querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least IP address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
Snooping Querier VLAN Address	Enter the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Delete	Click Delete to remove a Snooping Querier on the selected VLAN. This button is not visible when a VLAN is not selected.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

VLAN Configuration Summary

The MLD Snooping Querier VLAN Configuration Summary page displays the participation mode and VLAN address for each VLAN ID. To access this page, click **Multicast > MLD Snooping Querier > VLAN Configuration Summary**.

MLD Snooping Querier VLAN Configuration Summary

VLAN ID	Querier Election Participate Mode	Snooping Querier VLAN Address
Refresh		

Figure 3-146. Multicast > MLD Snooping Querier > VLAN Configuration Summary The following table describes the items in the previous menu.

Table 3-143. Multicast > MLD Snooping Querier > VLAN Configuration Summary

Parameter	Description
VLAN ID	Displays 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, upon seeing a query of the same version in the vlan, the snooping querier move to non-querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least IP address will win the querier election and 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 MLD queries sent on the specified VLAN.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

VLAN Status

The MLD Snooping Querier VLAN Status displays the operation and last querier status for each VLAN ID. To access this page, click **Multicast > MLD Snooping Querier > VLAN Status**.

MLD Snooping Querier VLAN Status

VLAN ID	Querier Operational State	Snooping Protocol Operational Version	Last Querier Address	Last Querier Version	Querier Operational Max Response Time (secs)
Refresh					

Figure 3-147. Multicast > MLD Snooping Querier > VLAN Status

The following table describes the items in the previous menu.

Table 3-144. Multicast > MLD Snooping Querier > VLAN Status

Parameter	Description
VLAN ID	Displays the VLAN ID on which MLD Snooping Querier is administratively enabled and VLAN exists in the VLAN database.
Operational State	Displays the operational state of the MLD Snooping Querier on a VLAN. It can be in any of the following states: <ul style="list-style-type: none"> Querier - 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, it moves to non-querier mode. Non-Querier - Snooping switch is in Non-Querier mode in the VLAN. If the querier expiry interval timer expires, the snooping switch will move into querier mode. Disabled - Snooping Querier is not operational on the VLAN. The Snooping Querier moves to disabled mode when MLD Snooping is not operational on the VLAN or when the querier address is not configured or the network management address is also not configured.
Operational Version	Displays the operational MLD protocol version of the 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 maximum response time to be used in the queries that are sent by the Snooping Querier.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.5.5 L2 Multicast Table

L2 Multicast Groups

The Multicast Forwarding Database holds 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 this page, click **Multi-cast > L2 Multicast Table > L2 Multicast Groups**.

Multicast Forwarding Database Table

MAC Address	Component	Type	Description	Interface(s)	Forwarding Interface(s)
<input style="width: 50%; border: none;" type="button" value="Refresh"/>					

Figure 3-148. Multicast > L2 Multicast Table > L2 Multicast Groups

The following table describes the items in the previous menu.

Table 3-145. Multicast > L2 Multicast Table > L2 Multicast Groups

Parameter	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-digit hexadecimal numbers are the VLAN ID and the remaining numbers are the MAC address. Then click on the "Search" button. If the address exists, that entry will be displayed. An exact match is required.
MAC Address	Displays the multicast MAC address for which you requested data.
Component	Displays the component that is responsible for this entry in the Multicast Forwarding Database. Possible values are IGMP Snooping, MLD Snooping, GMRP, and Static Filtering.
Type	Displays the entry type. 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	Displays the text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
Interface(s)	Displays the list of interfaces that are designated for forwarding (Fwd:) for the selected address.
Forwarding Interface(s)	Displays the resultant forwarding list is derived from combining all the forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.
Search	Click Search to initiate a search function based on the values in MAC address field.
Refresh	Refresh the data on the screen with the present state of the data in the switch.

L2 Multicast Statistics

The Multicast Forwarding Database Statistics page display the summary of MFDB table entries. To access this page, click **Multicast > L2 Multicast Table > L2 Multicast Statistics**.

Multicast Forwarding Database Statistics

Max MFDB Table Entries	1024
Most MFDB Entries Since Last Reset	0
Current Entries	0

Refresh

Figure 3-149. Multicast > L2 Multicast Table > L2 Multicast Statistics

The following table describes the items in the previous menu.

Table 3-146. Multicast > L2 Multicast Table > L2 Multicast Statistics

Parameter	Description
Max MFDB Table Entries	Displays the maximum number of entries that the Multicast Forwarding Database table can hold.
Most MFDB Entries Since Last Reset	Displays the largest number of entries that have been present in the Multicast Forwarding Database table since last reset. This value is also known as the MFDB high-water mark.
Current Entries	Displays the current number of entries in the Multicast Forwarding Database table.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.5.6 GMRP Table

GMRP Table

The MFDB GMRP Table displays all of the entries in the Multicast Forwarding Database that were created for the GARP Multicast Registration Protocol. To access this page, click **Multi-cast > GMRP Table**.

MFDB GMRP Table

MAC address	Type	Description	Interface(s)
Refresh			

Figure 3-150. Multicast > GMRP Table

The following table describes the items in the previous menu.

Table 3-147. Multicast > GMRP Table

Parameter	Description
MAC Address	Displays a VLAN ID - multicast MAC address pair for which the switch has forwarding and or filtering information. The format is as follows: 8 two-digit hexadecimal numbers, separated by colons, for example 00:01:23:45:67:89:AB:CD.
Type	Displays the type of the entry. Static entries are those that are configured by the user. Dynamic entries are added to the table as a result of a learning process or protocol.
Description	Displays the text description of this multicast table entry. Possible values are Management Configured, Network Configured and Network Assisted.
Interface(s)	Displays the list of interfaces that are designated for forwarding.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.6. Security

3.6.1 Denial of Service Protection

The Denial of Service Configuration page allows users to enable or disable denial of service settings. To access this page, click **Security > Denial of Service Protection**.

Denial of Service Configuration

Denial of Service L4 Port	Disable ▾
Denial of Service SIP=DIP	Disable ▾
Denial of Service SMAC=DMAC	Disable ▾
Denial of Service TCP Flag	Disable ▾
Denial of Service TCP Fragment	Disable ▾

Figure 3-151. Security > Denial of Service Protection

The following table describes the items in the previous menu.

Table 3-148. Security > Denial of Service Protection

Parameter	Description
Denial of Service SIP=DIP	Click the drop-down menu to enable or disable the option by selecting the corresponding line on the pull-down 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 Disable.
Denial of Service SMAC=DMAC	Click the drop-down menu to enable or disable the option by selecting the corresponding line on the pull-down 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 Disable.
Denial of Service TCP Flag	Click the drop-down menu to enable or disable the option by selecting the corresponding line on the pull-down entry field. Enabling TCP Flag DoS prevention causes the switch to drop packets that have TCP flag SYN set and TCP source port less than 1024 or TCP control flags set to 0 and TCP sequence number set to 0 or TCP flags FIN, URG, and PSH set and TCP sequence number set to 0 or both TCP flags SYN and FIN set. The factory default is Disable.
Denial of Service TCP Fragment	Click the drop-down menu to enable or disable the option by selecting the corresponding line on the pull-down 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 Disable.
Denial of Service L4 Port	Click the drop-down menu to enable or disable the option by selecting the corresponding line on the pull-down entry field. Enabling L4 Port DoS prevention causes the switch to drop packets that have TCP/UDP source port equal to TCP/UDP destination port. The factory default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

3.6.2 Port Access Control

Configuration

The Port Access Control Configuration page allows users to enable or disable port access settings. To access this page, click **Security > Port Access Control > Configuration**.

Port Access Control Configuration

Administrative Mode	Disable ▾
VLAN Assignment Mode	Disable ▾
Dynamic VLAN Creation Mode	Disable ▾
Monitor Mode	Disable ▾

Submit

Figure 3-152. Security > Port Access Control > Configuration

The following table describes the items in the previous menu.

Table 3-149. Security > Port Access Control > Configuration

Parameter	Description
Administrative Mode	Click the drop-down menu to enable or disable the administration mode. By default Administrative Mode is Disabled.
VLAN Assignment Mode	Click the drop-down menu to enable or disable the VLAN Assignment mode. The default value is Disable.
Dynamic VLAN Creation Mode	Click the drop-down menu to enable or disable the Dynamic VLAN Creation Mode. The default value is Disable.
Monitor Mode	Click the drop-down menu to enable or disable the Monitor Mode. The default value is Disable. The feature monitors the dot1x authentication process and helps in diagnosis the authentication failure cases.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Cancel	Click Cancel to discard the changes made on the page.

Port Configuration

The Port Access Control Port Configuration page allows users to configure port access control. To access this page, click **Security > Port Access Control > Port Configuration**.

Port Access Control Port Configuration

Interface	ge0/1	
Control Mode	Auto	
Quiet Period (secs)	50	(0 to 65535)
Transmit Period (secs)	30	(1 to 65535)
Guest VLAN ID	0	(0 to 4093)
Guest VLAN Period (secs)	30	(1 to 600)
Unauthenticated VLAN ID	0	(0 to 4093)
Supplicant Timeout (secs)	30	(1 to 65535)
Server Timeout (secs)	30	(1 to 65535)
Maximum Requests	2	(1 to 10)
Re-authentication Period (secs)	3600	(1 to 65535)
Re-authentication Enabled	False	
Maximum Users	16	(1 to 16)

Submit Refresh Initialize Re-Authenticate

Figure 3-153. Security > Port Access Control > Port Configuration

The following table describes the items in the previous menu.

Table 3-150. Security > Port Access Control > Port Configuration

Parameter	Description
Interface	Click the drop-down menu to select the port to be configured. 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.
Control Mode	Click the drop-down menu to select control mode options. The control mode is only set if the link status of the port is link up. The options are: <ul style="list-style-type: none"> Auto: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. Force Authorized: The authenticator PAE unconditionally sets the controlled port to authorized. Force Unauthorized: The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized. MAC Based: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.
Quiet Period (secs)	Enter the quiet period for the selected port. This command sets 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 must be a number in the range of 0 and 65535. A quiet period value of 0 means that the authenticator state machine will never acquire a supplicant. The default value is 60. Changing the value will not change the configuration until the Submit button is pressed.

Table 3-150. Security > Port Access Control > Port Configuration (Continued)

Parameter	Description
Transmit Period (secs)	Enter 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. Changing the value will not change the configuration until the Submit button is pressed.
Guest VLAN ID	Enter the Guest VLAN ID for the interface. The valid range is 0 to 4093. The default value is 0. Changing the value will not change the configuration until the Submit button is pressed. Enter 0 to clear the Guest VLAN ID on the interface.
Guest VLAN Period (secs)	Enter 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 and 300. The default value is 90. Changing the value will not change the configuration until the Submit button is pressed.
Unauthenticated VLAN ID	Enter the Unauthenticated VLAN ID for the selected port. The valid range is 0 to 4093. The default value is 0. Changing the value will not change the configuration until the Submit button is pressed. Enter 0 to clear the Unauthenticated VLAN ID on the interface.
Supplicant Timeout (secs)	Enter the 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 must be a value in the range of 1 and 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.
Server Timeout (secs)	Enter the 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 must be a value in the range of 1 and 65535. The default value is 30. Changing the value will not change the configuration until the Submit button is pressed.
Maximum Requests	Enter the 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 must be in the range of 1 and 10. The default value is 2. Changing the value will not change the configuration until the Submit button is pressed.
Re-authentication Period (secs)	Enter the re-authentication period for the selected port. The re-authentication period is the value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The re-authentication period must be a value in the range of 1 and 65535. The default value is 3600. Changing the value will not change the configuration until the Submit button is pressed.
Re-authentication Enabled	Click the drop-down menu to set the policy to True or False. If the value is 'true' re-authentication will occur. Otherwise, re-authentication will not be allowed. The default value is false. Changing the selection will not change the configuration until the Submit button is pressed.

Table 3-150. Security > Port Access Control > Port Configuration (Continued)

Parameter	Description
Maximum Users	Enter 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 the range of 1 to 16. The default value is 16. Changing the value will not change the configuration until the Submit button is pressed.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.
Initialize	Click Initialize to begin the initialization sequence on the selected port. This button is only selectable if the control mode is 'auto' or 'MAC-based'. 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. Dot1x must be enabled for this command to succeed.
Re-Authenticate	Click Re-Authenticate to begin the re-authentication sequence on the selected port. This button is only selectable if the control mode is 'auto' or 'MAC-based'. 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. Dot1x must be enabled for this command to succeed.

PAE Capability Configuration

The Port Access Control PAE Capability Configuration page allows users to assign PAE capabilities for each interface. To access this page, click **Security > Port Access Control > PAE Capability Configuration**.

Port Access Control PAE Capability Configuration

The screenshot shows a web interface for configuring PAE capabilities. It features a form with two dropdown menus. The first dropdown, labeled 'Interface', is set to 'ge0/1'. The second dropdown, labeled 'PAE Capabilities', is set to 'Authenticator'. Below the form are two buttons: 'Submit' and 'Refresh'.

Figure 3-154. Security > Port Access Control > PAE Capability

Configuration The following table describes the items in the previous menu.

Table 3-151. Security > Port Access Control > PAE Capability Configuration

Parameter	Description
Interface	Click the drop-down menu to select the port to be configured. 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.
PAE Capabilities	Click the drop-down menu to select an option for the Port Access Entity (PAE) configuration. The options are: <ul style="list-style-type: none"> • authenticator: Port Access Entity (PAE) is set to Authenticator. • supplicant: Port Access Entity (PAE) is set to Supplicant.

Table 3-151. Security > Port Access Control > PAE Capability Configuration (Continued)

Parameter	Description
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Supplicant Port Configuration

The Port Access Control Supplicant Port Configuration page allows users to configure the port access control settings for supplicant ports. To access this page, click **Security > Port Access Control > Supplicant Port Configuration**.

Port Access Control Supplicant Port Configuration

The screenshot shows a configuration form with the following fields and values:

- Interface: ge0/1 (dropdown)
- Control Mode: Auto (dropdown)
- User Name: admin (dropdown)
- Start Period (secs): 30 (range: 1 to 65535)
- Hold Period (secs): 60 (range: 1 to 65535)
- Authentication Period (secs): 30 (range: 1 to 65535)
- Maximum Requests: 3 (range: 1 to 10)

Buttons: Submit, Refresh

Figure 3-155. Security > Port Access Control > Supplicant Port Configuration

The following table describes the items in the previous menu.

Table 3-152. Security > Port Access Control > Supplicant Port Configuration

Parameter	Description
Interface	Click the drop-down menu to select the port to be configured. 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.
Control Mode	Click the drop-down menu to select an option for control mode. The options are: <ul style="list-style-type: none"> Force-unauthorized: The Supplicant port access entity (PAE) unconditionally sets the controlled port to unauthorized. Auto: The Supplicant PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. Force-authorized: The Supplicant PAE unconditionally sets the controlled port to authorized.
User Name	Enter the users that will have access to the specified port. The possible values are admin and guest.

Table 3-152. Security > Port Access Control > Supplicant Port Configuration (Continued)

Parameter	Description
Start Period (secs)	Enter the start period for the selected port. This command sets the value, in seconds, of the timer used by the Supplicant state machine on this port to define periods of time after which it will send start message again on Authenticator absence. The start period must be a number in the range of 1 and 65535. The default value is 30 seconds. Changing the value will not change the configuration until the Submit button is pressed.
Held Period (secs)	Enter the Held period for the selected port. The held period is the value, in seconds, of the timer used by the supplicant state machine on the specified port to determine when to send the next EAPOL start frame to the Authenticator on previous authentication failure. The Held period must be a number in the range of 1 and 65535. The default value is 60 seconds. Changing the value will not change the configuration until the Submit button is pressed.
Authentication Period (secs)	Enter the Authentication period for the selected port. The Authentication period is the value, in seconds, of the timer used by the supplicant backend state machine on the specified port to determine the timeout value for the EAPOL messages that are sent out to the Authenticator. The Authentication period must be a number in the range of 1 and 65535. The default value is 30 seconds. Changing the value will not change the configuration until the Submit button is pressed.
Maximum Requests	Enter the Maximum start messages that can be sent on the selected port. The maximum start request value is the maximum number of start messages to be sent continuously to detect the presence/absence of the Authenticator. The maximum start requests value must be in the range of 1 and 10. The default value is 3.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Port Status

The Port Access Control Port Status page displays port access information for each interface. To access this page, click **Security > Port Access Control > Port Status**.

Port Access Control Port Status

Interface	ge0/1
Protocol Version	Version1
PAE Capabilities	Supplicant
Control Mode	Auto
Supplicant PAE State	Initialize
Backend State	Request
Maximum Start Messages	3
Start Period (secs)	30
Held Period (secs)	60
Authentication Period (secs)	30

Figure 3-156. Security > Port Access Control > Port Status

The following table describes the items in the previous menu.

Table 3-153. Security > Port Access Control > Port Status

Parameter	Description
Interface	Click the drop-down menu to select 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.
Protocol Version	Displays the field displays the protocol version associated with the selected port. The only possible value is Version1, corresponding to the first version of the 802.1x specification. This field is not configurable.
PAE Capabilities	Displays the port access entity (PAE) functionality of the selected port. Possible values are "Authenticator" or "Supplicant". This field is not configurable.
Control Mode	<p>Displays the configured control mode for the specified port. Options are:</p> <ul style="list-style-type: none"> ● Force unauthorized: The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized. ● Force authorized: The authenticator PAE unconditionally sets the controlled port to authorized. ● Auto: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. ● MAC based: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on per supplicant basis.
Authenticator PAE State	<p>Displays the current state of the authenticator PAE state machine. This field is present only when the port control mode for the selected interface is not MAC-based. Possible values are:</p> <ul style="list-style-type: none"> ● Initialize ● Disconnected ● Connecting ● Authenticating ● Authenticated ● Aborting ● Held ● ForceAuthorized ● ForceUnauthorized

Table 3-153. Security > Port Access Control > Port Status (Continued)

Parameter	Description
Backend State	<p>Displays the current state of the backend authentication state machine. This field is present only when the port control mode for the selected interface is not MAC-based. Possible values are:</p> <ul style="list-style-type: none"> ● Request ● Response ● Success ● Fail ● Timeout ● Initialize ● Idle
Quiet Period	<p>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.</p>
Transmit Period	<p>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.</p>
Guest VLAN ID	<p>Displays the Guest VLAN ID configured on the interface. The valid range is (0 to 4093).</p>
Guest VLAN Period	<p>Displays the guest VLAN period for the selected port. The guest VLAN period is the value, in seconds, of the timer used by the GuestVLAN Authentication. The guest VLAN timeout must be a value in the range of 1 and 300.</p>
Supplicant Timeout	<p>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.</p>
Server Timeout	<p>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.</p>
Maximum Requests	<p>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.</p>
VLAN Assigned	<p>Displays the VLAN ID assigned to the selected interface by the Authenticator. This field is displayed only when the port control mode of the selected interface is not mac-based. This field is not configurable.</p>

Table 3-153. Security > Port Access Control > Port Status (Continued)

Parameter	Description
VLAN Assigned Reason	<p>Displays reason for the VLAN ID assigned by the authenticator to the selected interface. This field is displayed only when the port control mode of the selected interface is not mac-based. This field is not configurable. Possible values are:</p> <ul style="list-style-type: none"> ● Radius ● Unauth ● Default ● Not Assigned
Reauthentication Period	<p>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.</p>
Reauthentication Enabled	<p>Displays if reauthentication is enabled on the selected port. The possible values are 'true' and 'false'. If the value is 'true' reauthentication will occur. Otherwise, reauthentication will not be allowed.</p>
Key Transmission Enabled	<p>Displays if key transmission is enabled on the selected port. This is not a configurable field. The possible values are 'true' and 'false'. If the value is 'false' key transmission will not occur. Otherwise Key transmission is supported on the selected port.</p>
Control Direction	<p>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). This field is not configurable on some platforms.</p>
Maximum Users	<p>Displays the maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. The maximum users value is in the range of (1 to 16).</p>
Unauthenticated VLAN ID	<p>Displays the Unauthenticated VLAN ID for the selected port. The valid range is (0 to 4093).</p>
Session Timeout	<p>Displays Session Timeout set by the Radius Server for the selected port. This field is displayed only when the port control mode of the selected port is not mac-based.</p>
Session Termination Action	<p>Displays Termination Action set by the Radius Server for the selected port. This field is displayed only when the port control mode of the selected port is not mac-based. Possible values are:</p> <ul style="list-style-type: none"> ● Default ● Reauthenticate <p>If the termination action is 'default' then at the end of the session, the client details are initialized. Otherwise re-authentication is attempted.</p>
Refresh	<p>Click Refresh to update the data on the screen with the present state of the data in the switch.</p>

Port Summary

The Port Access Control Port Summary page displays the summary of port access control for each interface. To access this page, click **Security > Port Access Control > Port Summary**.

Port Access Control Port Summary

Interface	Control Mode	Operating Control Mode	Re-authentication Enabled	Port Status
ge0/1	Auto	Auto		Authorized
ge0/2	Auto	N/A	FALSE	N/A
ge0/3	Auto	N/A	FALSE	N/A
ge0/4	Auto	N/A	FALSE	N/A
ge0/5	Auto	N/A	FALSE	N/A
ge0/6	Auto	N/A	FALSE	N/A
ge0/7	Auto	N/A	FALSE	N/A
ge0/8	Auto	Auto	FALSE	Authorized
ge0/9	Auto	N/A	FALSE	N/A
ge0/10	Auto	N/A	FALSE	N/A
ge0/11	Auto	N/A	FALSE	N/A
ge0/12	Auto	N/A	FALSE	N/A
ge0/13	Auto	N/A	FALSE	N/A
ge0/14	Auto	N/A	FALSE	N/A
ge0/15	Auto	N/A	FALSE	N/A

Figure 3-157. Security > Port Access Control > Port Summary

The following table describes the items in the previous menu.

Table 3-154. Security > Port Access Control > Port Summary

Parameter	Description
Interface	Displays the port whose settings are displayed in the current table row.
Control Mode	<p>Displays the configured control mode for the port. Possible values are:</p> <ul style="list-style-type: none"> Auto: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server. Force Authorized: The authenticator PAE unconditionally sets the controlled port to authorized. Force Unauthorized: The authenticator port access entity (PAE) unconditionally sets the controlled port to unauthorized. MAC-based: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator, and the authentication server on a per supplicant basis.

Table 3-154. Security > Port Access Control > Port Summary (Continued)

Parameter	Description
Operating Control Mode	Displays the control mode under which the port is actually operating. Possible values are: <ul style="list-style-type: none"> • Auto • Force Authorized • Force Unauthorized • MAC-based • N/A: If the port is in detached state it cannot participate in port access control.
Re-authentication Enabled	Displays the re-authentication enabled policy. The possible values are 'true' and 'false'. If the value is 'true', re-authentication will occur. Otherwise, re-authentication will not be allowed.
Port Status	Displays the authorization status of the specified port. The possible values are 'Authorized', 'Unauthorized' and 'N/A'. If the port is in detached state, the value will be 'N/A' since the port cannot participate in port access control.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Statistics

The Port Access Control Statistics page displays received and transmitted frames. To access this page, click **Security > Port Access Control > Statistics**.

Port Access Control Statistics

Interface	
Supplicant Port Access Control Statistics	0/0/1 ▾
EAPOL Frames Received	0
EAPOL Frames Transmitted	0
EAPOL Start Frames Transmitted	0
EAPOL Logoff Frames Transmitted	0
Last EAPOL Frame Version	0
Last EAPOL Frame Source	nn:nn:nn:nn:nn:nn
EAP Response/Id Frames Transmitted	0
EAP Response Frames Transmitted	0
EAP Request/Id Frames Received	0
EAP Request Frames Received	0
Invalid EAPOL Frames Received	0
EAPOL Length Error Frames Received	0

Figure 3-158. Security > Port Access Control > Statistics

The following table describes the items in the previous menu.

Table 3-155. Security > Port Access Control > Statistics

Parameter	Description
Interface	Click the drop-down menu to select 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. The statistics will be displayed for an Authenticator or a Supplicant depending upon whether the port is a Supplicant or an Authenticator.
Authenticator Port Access Control Statistics: If the Port is an Authenticator.	
EAPOL Frames Received	Displays the number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	Displays the number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	Displays the number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	Displays the number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	Displays the protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	Displays the source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	Displays the number of EAP response/identity frames that have been received by this authenticator.
EAP Response Frames Received	Displays the number of valid EAP response frames (other than response/identity frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	Displays the number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	Displays the number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	Displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAPOL Length Error Frames Received	Displays the number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
Supplicant Port Access Control Statistics: If the Port is a Supplicant.	
EAPOL Frames Received	Displays the number of valid EAPOL frames of any type that have been received by this supplicant.
EAPOL Frames Transmitted	Displays the number of EAPOL frames of any type that have been transmitted by this supplicant.
EAPOL Start Frames Received	Displays the number of EAPOL start frames that have been received by this supplicant.

Table 3-155. Security > Port Access Control > Statistics (Continued)

Parameter	Description
EAPOL Logoff Frames Received	Displays the number of EAPOL logoff frames that have been received by this supplicant.
Last EAPOL Frame Version	Displays the protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	Displays the source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames Received	Displays the number of EAP response/identity frames that have been received by this supplicant.
EAP Response Frames Received	Displays the number of valid EAP response frames (other than response/identity frames) that have been received by this supplicant.
EAP Request/Id Frames Transmitted	Displays the number of EAP request/identity frames that have been transmitted by this supplicant.
EAP Request Frames Transmitted	Displays the number of EAP request frames (other than request/identity frames) that have been transmitted by this supplicant.
Invalid EAPOL Frames Received	Displays the number of EAPOL frames that have been received by this supplicant in which the frame type is not recognized.
EAPOL Length Error Frames Received	Displays the number of EAPOL frames that have been received by this supplicant in which the frame type is not recognized.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.
Clear	Click Clear to reset the statistics for the selected port. There is no confirmation prompt. When this button is pressed, the stats are immediately cleared.
Clear All	Click Clear All to reset all statistics for all ports to 0. There is no confirmation prompt. When this button is pressed, the stats are immediately cleared.

Client Summary

The Port Access Control Client Summary page displays details of port access for each interface. To access this page, click **Security > Port Access Control > Client Summary**.

Port Access Control Client Summary

Interface	Logical Interface	User Name	Supp MAC Address	Session Time	Filter ID
<input type="button" value="Refresh"/>					

Figure 3-159. Security > Port Access Control > Client Summary

The following table describes the items in the previous menu.

Table 3-156. Security > Port Access Control > Client Summary

Parameter	Description
Interface	Displays the dot1x Physical Port.
Logical Interface	Displays the dot1x Logical Port.
User Name	Displays this field displays the User Name representing the identity of the supplicant device.
Supp MAC Address	Displays this field displays supplicant's device MAC Address.
Session Time	Displays this field displays the time since the supplicant as logged in seconds.
Filter ID	Displays this field displays policy filter ID assigned by the authenticator to the supplicant device.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Client Detail

The Client Detail page displays details for successfully authorized clients on selected ports. To access this page, click **Security > Port Access Control > Client Detail**.

Port Access Control Client Detail

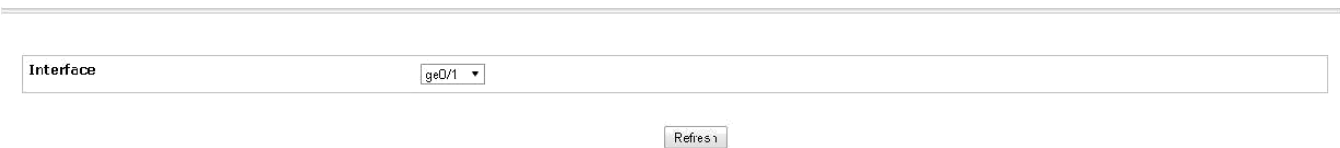


Figure 3-160. Security > Port Access Control > Client Detail

The following table describes the items in the previous menu.

Table 3-157. Security > Port Access Control > Client Detail

Parameter	Description
Interface	Click the drop-down menu to select a field lists all the physical ports.
Following are the details shown only for successfully authorized clients on selected Port above.	
Logical Interface	Displays the dot1x Logical Port.
User Name	Displays the User Name representing the identity of the supplicant device.
Supplicant MAC Address	Displays the supplicant's device MAC Address.
Session Time	Displays the time since the supplicant as logged in seconds.
Filter ID	Displays policy filter ID assigned by the authenticator to the supplicant device.
VLAN ID Associated	Displays VLAN ID assigned by the authenticator to the supplicant device.
Dot1x Logical Port VLAN Assignment	Displays reason for the VLAN ID assigned by the authenticator to the supplicant device.

Table 3-157. Security > Port Access Control > Client Detail (Continued)

Parameter	Description
Session Timeout	Displays Session Timeout set by the Radius Server to the supplicant device.
Termination Action	Displays Termination Action set by the Radius Server to the supplicant device.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Privileges

The Port Access Privileges page allows users to grant port access to selected users. To access this page, click **Security > Port Access Control > Privileges**.

Port Access Privileges

Figure 3-161. Security > Port Access Control > Privileges

The following table describes the items in the previous menu.

Table 3-158. Security > Port Access Control > Privileges

Parameter	Description
Interface	Click the drop-down menu to select the port to configure.
Users	Select the users that have access to the specified port or ports.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Summary

The Port Access Summary page displays the summary of port access for each interface. To access this page, click **Security > Port Access Control > Summary**.

Port Access Summary

Interface	Users
ge0/1	admin user
ge0/2	admin user
ge0/3	admin user
ge0/4	admin user
ge0/5	admin user
ge0/6	admin user
ge0/7	admin user
ge0/8	admin user
ge0/9	admin user
ge0/10	admin user
ge0/11	admin user
ge0/12	admin user
ge0/13	admin user
ge0/14	admin user
ge0/15	admin user
ge0/15	admin user

Figure 3-162. Security > Port Access Control > Summary

The following table describes the items in the previous menu.

Table 3-159. Security > Port Access Control > Summary

Parameter	Description
Interface	Displays the port in Slot/Port format.
Users	Displays the type of users with port access.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

History Log Summary

The Port Access Control History Log Summary page displays the summary of history logs for each interface. To access this page, click **Security > Port Access Control > History Log Summary**.

Port Access Control History Log Summary

Interface	Time Stamp	VLAN Assigned	VLAN Assigned Reason	Supp MAC Address	Filter Name	Auth Status	Reason
-----------	------------	---------------	----------------------	------------------	-------------	-------------	--------

Refresh Clear

Figure 3-163. Security > Port Access Control > History Log Summary

The following table describes the items in the previous menu.

Table 3-160. Security > Port Access Control > History Log Summary

Parameter	Description
Interface	Click the drop-down menu to select all the interfaces exist in the history log table. When the selection is changed, a screen refresh will occur causing all fields to be updated for the newly selected interface or all interfaces.
Following are the details shown for successful and unsuccessful authentication clients on selected port above.	
Interface	Displays on the page only if 'all' option is being selected in the above 'Interface' combo field. It indicates the interface number on which the authentication event took place.
Time Stamp	Displays the absolute time (in "Month Day Year Time" format) when the authentication event took place.
VLAN Assigned	Displays the VLAN ID assigned by the authenticator.
VLAN Assigned Reason	Displays the reason for the VLAN ID assigned by the authenticator to the supplicant device.
Supplicant MAC Address	Displays the supplicant's device MAC Address.
Filter Name	Displays the policy filter name assigned by the authenticator to the supplicant device.
Auth Status	Displays the authentication status of the client/port (Authorized or Unauthorized).
Reason	Displays the exact reason for the successful or unsuccessful authentication.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.
Clear	Click Clear to remove all the history log entries for the given interface.

3.6.3 DHCP Snooping

Configuration

The DHCP Snooping Configuration page allows users to enable or disable DHCP snooping mode and MAC and violation. To access this page, click **Security > DHCP Snooping > Configuration**.

DHCP Snooping Configuration

DHCP Snooping Mode:

MAC Address Validation:

Figure 3-164. Security > DHCP Snooping > Configuration

The following table describes the items in the previous menu.

Table 3-161. Security > DHCP Snooping > Configuration

Parameter	Description
DHCP Snooping Mode	Click the drop-down menu to enable or disable the DHCP Snooping feature. The factory default is Disable.
MAC Address Validation	Click the drop-down menu to enable or disable the validation of sender MAC Address for DHCP Snooping. The factory default is Enable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

VLAN Configuration

The DHCP Snooping VLAN Configuration page allows users to enable or disable DHCP snooping mode for each VLAN ID. To access this page, click **Security > DHCP Snooping > VLAN Configuration**.

DHCP Snooping VLAN Configuration

VLAN ID:

DHCP Snooping Mode:

Figure 3-165. Security > DHCP Snooping > VLAN Configuration

The following table describes the items in the previous menu.

Table 3-162. Security > DHCP Snooping > VLAN Configuration

Parameter	Description
VLAN ID	Select the VLAN for which information to be displayed or configured for DHCP Snooping Application.
DHCP Snooping Mode	Click the drop-down menu to enable or disable the DHCP Snooping feature on selected VLAN. The factory default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Configuration

The DHCP Snooping Interface Configuration page allows users to configure DHCP snooping settings for each interface. To access this page, click **Security > DHCP Snooping > Interface Configuration**.

DHCP Snooping Interface Configuration

Figure 3-166. Security > DHCP Snooping > Interface Configuration

The following table describes the items in the previous menu.

Table 3-163. Security > DHCP Snooping > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the interface for which data is to be displayed or configured.
Trust State	Click the drop-down menu to enable or disable the DHCP snooping trust state. The factory default is Disable.
Logging Invalid Packets	Click the drop-down menu to enable or disable the DHCP snooping application to log invalid packets on this interface. The factory default is Disable.
Rate Limit	Enter the value to specify the DHCP Snooping purpose. If the incoming rate of DHCP packets exceeds the value of this object for consecutively burst interval seconds, the port will be shutdown. The range of Rate Limit is 0 to 300.
No Limit	Click the box to specify no Rate Limit. If the rate limit is -1 burst interval has no meaning, hence it is disabled.
Burst Interval	Enter the value to specify the burst interval value for rate limiting purpose on this interface. If the rate limit is None, then burst interval has no meaning. The range of Burst Interval is 1 to 15.

Table 3-163. Security > DHCP Snooping > Interface Configuration

Parameter	Description
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Binding Configuration

The DHCP Snooping Binding Configuration page allows users to configure MAC and IP addresses and VLAN IDs for each interface. To access this page, click **Security > DHCP Snooping > Binding Configuration**.

DHCP Snooping Binding Configuration

The screenshot displays the DHCP Snooping Binding Configuration interface. At the top, there is a form with the following fields:

- Interface:** A dropdown menu showing 'ge0/1'.
- MAC address:** A text input field containing '00:00:30:00:00:00'.
- VLAN ID:** A dropdown menu showing '1'.
- IP Address:** A text input field containing '0.0.0.0'.

 Below the form is an 'Add' button. Underneath, there are two sections:

- Static Binding List:** A table with columns: Interface, MAC address, VLAN ID, IP Address, and Remove. Below the table is a 'Page' dropdown set to '1' and a 'Submit' button.
- Dynamic Binding List:** A table with columns: Interface, MAC address, VLAN ID, IP Address, and Lease Time. Below the table is a 'Page' dropdown set to '1', a 'Clear All' button, and a 'Refresh' button.

Figure 3-167. Security > DHCP Snooping > Binding Configuration

The following table describes the items in the previous menu.

Table 3-164. Security > DHCP Snooping > Binding Configuration

Parameter	Description
Interface	Click the drop-down menu to select the interface to add a binding into the DHCP snooping database.
MAC Address	Enter a MAC address for the binding to be added. This is the key value to the binding database.
VLAN ID	Click the drop-down menu to select the VLAN from the list for the binding rule. The range of the VLAN ID is 1 to 4093.
IP Address	Enter a valid IP Address for the binding rule.
Add	Click Add to create a DHCP snooping binding entry into the database.

Table 3-164. Security > DHCP Snooping > Binding Configuration (Continued)

Parameter	Description
Static Binding List	<p>Displays all the DHCP snooping static binding entries page by page. Ex: Page 1 displays first 15 available static entries. Page 2 displays Next 15 available static entries.</p> <ul style="list-style-type: none"> ● Interface - Interface ● MAC Address - MAC address ● VLAN ID - VLAN Identifier ● IP Address - IP address ● Remove - This is to be selected to remove the particular binding entry ● Page - Lists the Number of Pages the static binding entries occupied. Select the Page Number from this list to display the particular Page entries.
Page	Click the drop-down menu to list the Number of Pages the dynamic binding entries occupies. Select the Page Number from this list to display the particular Page entries.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Dynamic Binding List	<p>Displays all the DHCP snooping dynamic binding entries page by page. Ex: Page 1 displays first available up to 15 dynamic entries. Page 2 displays Next available up to 15 dynamic entries.</p> <ul style="list-style-type: none"> ● Interface - Interface ● MAC Address - MAC address ● VLAN ID - VLAN Identifier ● IP Address - IP address ● Lease Time- This is the remaining Lease time for the Dynamic entries ● Page - Lists the Number of Pages the dynamic binding entries occupied. Select the Page Number from this list to display the particular Page entries.
Clear All	Click Clear All to delete all DHCP Snooping binding entries.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Persistent Configuration

The DHCP Snooping Persistent Configuration page allows users to set up remote configuration for persistent DHCP snooping. To access this page, click **Security > DHCP Snooping > Persistent Configuration**.

DHCP Snooping Persistent Configuration

Figure 3-168. Security > DHCP Snooping > Persistent Configuration

The following table describes the items in the previous menu.

Table 3-165. Security > DHCP Snooping > Persistent Configuration

Parameter	Description
Store	Click the radio button to specify remote or local snooping database storage. <ul style="list-style-type: none"> Local - Check the Local Checkbox to disable the Remote objects like Remote File Name and Remote IP Address. Remote - Check the Remote Checkbox to Enable the Remote objects like Remote File Name and Remote IP Address.
Remote IP Address	Enter the Remote IP Address on which the snooping database will be stored when Remote checkbox is selected.
Remote File Name	Enter the remote file name to store the database when Remote checkbox is selected. Range is 1 to 32 characters and can contain only alphanumeric, dash, dot or underscore characters.
Write Delay	Enter the maximum write time to write the database into local or remote. The range of Write Delay is 15 to 86400.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Statistics

The DHCP Snooping Statistics page displays the list of DHCP snooping enabled interfaces. To access this page, click **Security > DHCP Snooping > Statistics**.

DHCP Snooping Statistics

No DHCP Snooping Enabled Interfaces Found

Figure 3-169. Security > DHCP Snooping > Statistics

The following table describes the items in the previous menu.

Table 3-166. Security > DHCP Snooping > Statistics

Parameter	Description
Interface	Displays the untrusted and snooping enabled interface for which statistics to be displayed.
MAC Verify Failures	Displays number of packets that were dropped by DHCP Snooping as there is no matching DHCP Snooping binding entry found.
Client Ifc Mismatch	Displays the number of DHCP messages that are dropped based on source MAC address and client HW address verification.
DHCP Server Msgs Received	Displays the number of Server messages that are dropped on an untrusted port.
Clear Statistics	Click Clear Statistics to reset all interfaces statistics.

DHCP L2 Relay

Global Configuration

The DHCP L2 Relay Global Configuration page allows users to enable or disable DHCP L2 Relay Mode. To access this page, click **Security > DHCP Snooping > DHCP L2 Relay > Global Configuration**.

DHCP L2 Relay Global Configuration

Figure 3-170. Security > DHCP Snooping > DHCP L2 Relay > Global Configuration The following table describes the items in the previous menu.

Table 3-167. Security > DHCP Snooping > DHCP L2 Relay > Global Configuration

Parameter	Description
DHCP L2 Relay Mode	Click the drop-down menu to enable or disable the DHCP L2 Relay feature. The factory default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Configuration

The DHCP L2 Relay Interface Configuration page allows users to enable or disable the DHCP L2 relay mode and relay trust mode for each interface. To access this page, click **Security > DHCP Snooping > DHCP L2 Relay > Interface Configuration**.

DHCP L2 Relay Interface Configuration

Figure 3-171. Security > DHCP Snooping > DHCP L2 Relay > Interface Configuration

The following table describes the items in the previous menu.

Table 3-168. Security > DHCP Snooping > DHCP L2 Relay > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the interface for which data is to be displayed or configured.
DHCP L2 Relay Mode	Click the drop-down menu to enable or disable L2 Relay mode on selected interface. The factory default is Disable.
DHCP L2 Relay Trust Mode	Click the drop-down menu to enable or disable the L2 relay. If this is Enabled, DHCP L2 Relay application considers selected port as L2 Relay trusted. The factory default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

VLAN Configuration

The DHCP L2 Relay VLAN Configuration page allows users to enable or disable DHCP L2 relay mode and circuit ID, and assign a remote ID for each VLAN ID. To access this page, click **Security > DHCP Snooping > DHCP L2 Relay > VLAN Configuration**.

DHCP L2 Relay VLAN Configuration

Figure 3-172. Security > DHCP Snooping > DHCP L2 Relay > VLAN Configuration

The following table describes the items in the previous menu.

Table 3-169. Security > DHCP Snooping > DHCP L2 Relay > VLAN Configuration

Parameter	Description
VLAN ID	Click the drop-down menu to select the VLAN for which data is to be displayed or configured.
DHCP L2 Relay Mode	Click the drop-down menu to enable or disable the DHCP L2 Relay feature on selected VLAN. The factory default is Disable.
DHCP L2 Relay Circuit-Id	Click the drop-down menu to enable or disable the DHCP Circuit-Identifier feature on selected VLAN. The factory default is Disable.
DHCP L2 Relay Remote-Id	Enter the DHCP Remote-Identifier string on selected VLAN. The factory default is NULL string. Range is 0 to 33 characters.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Interface Statistics

The DHCP L2 Relay Interface Statistics page displays the DHCP L2 relay statistics for trusted and untrusted server and client messages. To access this page, click **Security > DHCP Snooping > DHCP L2 Relay > Interface Statistics**.

DHCP L2 Relay Interface Statistics

Interface	Value
Untrusted Server Messages With Option-82	0
Untrusted Client Messages With Option-82	0
Trusted Server Messages Without Option-82	0
Trusted Client Messages Without Option-82	0

Refresh Clear ClearAll

Figure 3-173. Security > DHCP Snooping > DHCP L2 Relay > Interface Statistics The following table describes the items in the previous menu.

Table 3-170. Security > DHCP Snooping > DHCP L2 Relay > Interface Statistics

Parameter	Description
Interface	Click the drop-down menu to select the DHCP L2 Relay enabled interface for which statistics to be displayed.
Untrusted Server Messages with Option-82	Displays the number of DHCP Reply packets received with Option-82 on untrusted DHCP L2 Relay interface.
Untrusted Client Messages with Option-82	Displays the number of DHCP Request packets received with Option-82 on untrusted DHCP L2 Relay interface.

Table 3-170. Security > DHCP Snooping > DHCP L2 Relay > Interface Statistics (Continued)

Parameter	Description
Trusted Server Messages without Option-82	Displays the number of DHCP Reply packets received without Option-82 on untrusted DHCP L2 Relay interface.
Trusted Client Messages without Option-82	Displays the number of DHCP Request packets received without Option-82 on untrusted DHCP L2 Relay interface.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.
Clear	Click Clears to refresh the statistics for the selected interface.
ClearAll	Click Clear All to refresh the statistics for all the interfaces.

Dynamic ARP Inspection

Global Configuration

The Dynamic ARP Inspection Global Configuration page allows users to enable or disable validation of source and destination MACs and IP. To access this page, click **Security > DHCP Snooping > Dynamic ARP Inspection > Global Configuration**.

Dynamic ARP Inspection Global Configuration

Validate Source MAC	Disable ▾
Validate Destination MAC	Disable ▾
Validate IP	Disable ▾

Submit

Figure 3-174. Security > DHCP Snooping > Dynamic ARP Inspection > Global Configuration

The following table describes the items in the previous menu.

Table 3-171. Security > DHCP Snooping > Dynamic ARP Inspection > Global Configuration

Parameter	Description
Validate Source MAC	Click the drop-down menu to enable or disable the DAI Source MAC Validation Mode for the switch. If you select Enable, Sender MAC validation for the ARP packets will be enabled. The factory default is Disable.
Validate Destination MAC	Click the drop-down menu to enable or disable 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 factory default is Disable.
Validate IP	Click the drop-down menu to enable or disable the DAI IP Validation Mode for the switch. If you select Enable, IP Address validation for the ARP packets will be enabled. The factory default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

VLAN Configuration

The Dynamic ARP Inspection VLAN Configuration page allows users to configure the dynamic ARP inspection VLAN. To access this page, click **Security > DHCP Snooping > Dynamic ARP Inspection > VLAN Configuration**.

Dynamic ARP Inspection VLAN Configuration

Figure 3-175. Security > DHCP Snooping > Dynamic ARP Inspection > VLAN Configuration

The following table describes the items in the previous menu.

Table 3-172. Security > DHCP Snooping > Dynamic ARP Inspection > VLAN Configuration

Parameter	Description
VLAN ID	Click the drop-down menu to select the DAI Capable VLANs for which information has to be displayed or configured.
Dynamic ARP Inspection	Click the drop-down menu to enable or disable the Dynamic ARP Inspection. If this object is set to 'Enable' Dynamic ARP Inspection is enabled. If this object is set to 'Disable', Dynamic ARP Inspection is disabled. The factory default is Disable.
Logging Invalid Packets	Click the drop-down menu to set the Dynamic ARP Inspection logging policy. If this object is set to 'Enable' it will log the Invalid ARP Packets information. If this object is set to 'Disable', Dynamic ARP Inspection logging is disabled. The factory default is Enable.
ARP ACL Name	Enter the name of 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 up to 31 alphanumeric characters.
Static Flag	Click the drop-down menu to select the ARP packet validation using the DHCP snooping database in case ARP ACL rules don't match. If the flag is enabled then the ARP Packet will be validated by the ARP ACL Rules only. If the flag is disabled then the ARP Packet needs further validation by using the DHCP Snooping entries. The factory default is Disable.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Interface Configuration

The Dynamic ARP Inspection Interface Configuration page allows users to enable or disable trust rate for each interface, and assign rate limits and burst intervals. To access this page, click **Security > DHCP Snooping > Dynamic ARP Inspection > Interface Configuration**.

Dynamic ARP Inspection Interface Configuration

The screenshot shows a configuration form with the following fields and values:

- Interface:** ge0/1
- Trust State:** Disable
- Rate Limit:** 15 (0 to 300) pps
- Burst Interval:** 1 (1 to 15) seconds

Buttons: Submit, Refresh

Figure 3-176. Security > DHCP Snooping > Dynamic ARP Inspection > Interface Configuration

The following table describes the items in the previous menu.

Table 3-173. Security > DHCP Snooping > Dynamic ARP Inspection > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the physical interface for which data is to be displayed or configured.
Trust State	Click the drop-down menu to enable or disable the trust state--indicates whether the interface is trusted for Dynamic ARP Inspection purpose. If this object is set to 'Enable', the interface is trusted. ARP packets coming to this interface will be forwarded without checking. If this object is set to 'Disable', the interface is not trusted. ARP packets coming to this interface will be subjected to ARP inspection. The factory default is Disable.
Rate Limit	Enter a variable for the rate limit value for Dynamic ARP Inspection purpose. If the incoming rate of ARP packets exceeds the value of this object for consecutively burst interval seconds, ARP packets will be dropped. If this value is -1 there is no limit. The Range is 0 to 300 pps. The factory default is 15pps (packets per second).
No Limit	Enter a value to specify the value of Rate Limit will be configured to -1. If the rate limit is -1 burst interval has no meaning, hence it is disabled.
Burst Interval	Enter a value to specify the burst interval value for rate limiting purpose on this interface. The Range is 1 to 15 seconds. If the rate limit is -1 burst interval has no meaning. The factory default is 1 second.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

ARP ACL Configuration

The Dynamic ARP Inspection ARP ACL Configuration page allows users to assign ARP ACL names. To access this page, click **Security > DHCP Snooping > Dynamic ARP Inspection > ARP ACL Configuration**.

Dynamic ARP Inspection ARP ACL Configuration

Figure 3-177. Security > DHCP Snooping > Dynamic ARP Inspection > ARP ACL Configuration

The following table describes the items in the previous menu.

Table 3-174. Security > DHCP Snooping > Dynamic ARP Inspection > ARP ACL Configuration

Parameter	Description
ARP ACL Name	Enter a value to create New ARP ACL for DAI. The name can contain up to 31 alphanumeric characters).
ARP ACL Name	Displays the configured ARP ACL name.
Remove	Click Remove to delete the particular ACLs which you want to delete.
Add	Click Add to add a new ARP ACL entry.
Delete	Click Delete to remove the entry selected using checkbox under Remove field.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

ARP ACL Rule Configuration

The ACL Rule Configuration displays the rules for selected ARP ACLs. To access this page ARP ACL Rule Configuration, click **Security > DHCP Snooping > Dynamic ARP Inspection > ARP ACL Rule Configuration**.

Dynamic ARP Inspection ARP ACL Rule Configuration

Figure 3-178. Security > DHCP Snooping > Dynamic ARP Inspection > ARP ACL Rule Configuration

The following table describes the items in the previous menu.

Table 3-175. Security > DHCP Snooping > Dynamic ARP Inspection > ARP ACL Rule Configuration

Parameter	Description
ARP ACL Name	Displays the ARP ACL for which information want to be displayed or configured.
Sender IP Address	Displays the Sender IP address match value for the ARP ACL.
Sender MAC Address	Displays the Sender MAC Address state. This is used to create new Rule for the Selected ARP ACL. This indicates Sender MAC address match value for the ARP ACL.
List of ARP ACL Rules	
Sender IP Address	Displays the configured Sender IP address.
Sender MAC Address	Displays the configured Sender MAC address.
Remove	Click Remove to delete the selected the particular ACL Rules.
Add	Click Add to create a new ACL Rule.
Delete	Click Delete to remove the entry selected using checkbox under Remove field.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Statistics

The Statistics page displays the statistics per VLAN. To access this page, click **Security > DHCP Snooping > Dynamic ARP Inspection > Statistics**.

Dynamic ARP Inspection Statistics

No DAI enabled VLANs found

Figure 3-179. Security > DHCP Snooping > Dynamic ARP Inspection > Statistics The following table describes the items in the previous menu.

Table 3-176. Security > DHCP Snooping > Dynamic ARP Inspection > Statistics

Parameter	Description
VLAN ID	Click the drop-down menu to select the DAI enabled VLAN ID for which statistics to be displayed.
DHCP Drops	Displays the number of ARP packets that were dropped by DAI as there is no matching DHCP Snooping binding entry found.
ACL Drops	Displays the number of ARP packets that were dropped by DAI as there is no matching ARP ACL rule found for this VLAN and the static flag is set on this VLAN.
DHCP Permits	Displays the number of ARP packets that were forwarded by DAI as there is a matching DHCP Snooping binding entry found.

Table 3-176. Security > DHCP Snooping > Dynamic ARP Inspection > Statistics (Continue)

Parameter	Description
ACL Permits	Displays the number of ARP packets that were permitted by DAI as there is a matching ARP ACL rule found for this VLAN.
Bad Source MAC	Displays the number of ARP packets that were dropped by DAI as the sender MAC address in ARP packet didn't match the source MAC in ethernet header.
Bad Dest MAC	Displays the number of ARP packets that were dropped by DAI as the target MAC address in ARP reply packet didn't match the destination MAC in ethernet header.
Invalid IP	Displays the number of ARP packets that were dropped by DAI as the sender IP address in ARP packet or target IP address in ARP reply packet is invalid. Invalid addresses include 0.0.0.0, 255.255.255.255, IP multicast addresses, class E addresses (240.0.0.0/4), loopback addresses (127.0.0.0/8).
Forwarded	Displays the number of valid ARP packets forwarded by DAI.
Dropped	Displays the number of invalid ARP packets dropped by DAI.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.6.4 Protected Ports

Configuration

The Protected Ports Configuration page allows users to create a group, assign a group ID and name, and select protected ports to belong to the group. To access this page, click **Security > Protected Ports > Configuration**.

Protected Ports Configuration

The screenshot displays the 'Protected Ports Configuration' interface. It includes a 'Group ID' dropdown menu set to '0', a 'Group Name' text input field with a '(0 to 32 characters)' label, and a 'Protected Port(s)' list containing 'ge0/1', 'ge0/2', 'ge0/3', and 'ge0/4'. At the bottom, there are 'Add Port(s)' and 'Delete Port(s)' buttons.

Figure 3-180. Security > Protected Ports > Configuration

The following table describes the items in the previous menu.

Table 3-177. Security > Protected Ports > Configuration

Parameter	Description
Group ID	Click the drop-down menu to select the group ID. Traffic can flow between protected ports belonging to different groups, but not within the same group. The selection box lists all the possible protected port Group IDs supported for the current platform. The valid range of the Group ID is 0 to 2.
Group Name	Enter the name associated with the protected ports group used for identification purposes. It can be up to 64 characters long, including blanks. The default is blank. Setting the group name to blank will delete the previously configured name. This field is optional.
Protected Port(s)	Select a physical port entry. The protected ports are highlighted to differentiate between them. No traffic forwarding is possible between two protected ports. If left unconfigured, the default state is unprotected.
Add Port(s)	Click Add to create a new group entry.
Delete Port(s)	Click Delete Port to remove the highlighted ports from the protected ports group.

Status

The Protected Ports Summary page displays the summary of the groups created. To access this page, click **Security > Protected Ports > Status**.

Protected Ports Summary

Group ID	Group Name	Protected Port(s)
0		
1		
2		

Figure 3-181. Security > Protected Ports > Status

The following table describes the items in the previous menu.

Table 3-178. Security > Protected Ports > Status

Parameter	Description
Group ID	Displays the Group ID. Traffic can flow between protected ports belonging to different groups, but not within the same group. The valid range of the Group ID is 0 to 2.
Group Name	Displays the alphanumeric string associated with a Group ID.
Protected Port(s)	Displays the list consisting of all the protected ports. It is to be noted that no traffic forwarding is possible between two protected ports of a same group, but traffic can flow between protected ports of different groups.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.7. QoS

3.7.1 Access Control Lists

IP Access Control Lists

IP Access Control Lists are lists of IP access permissions.

Configuration

The Configuration page allows users to create or specify IP ACL rules. To access this page, click **QoS > Access Control Lists > IP Access Control Lists > Configuration**.

IP ACL Configuration

Table	Current Number / Maximum Number
ACL	n / 100

Figure 3-182. QoS > Access Control Lists > IP Access Control Lists > Configuration

The following table describes the items in the previous menu.

Table 3-179. QoS > Access Control Lists > IP Access Control Lists > Configuration

Parameter	Description
IP ACL	Click the drop-down menu to select an existing entry or create an IP ACL entry. A new IP Access Control List may be created or the configuration of an existing IP ACL can be updated.
IP ACL ID	Enter a value for the IP ACL ID must be a whole number in the range of 1 to 99 for IP Standard Access Lists and 100 to 199 for IP Extended Access Lists.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Table	Displays the current number/maximum number of IP ACLs.
Rename	Click Rename to rename an existing IP ACL. This button is shown when you want to rename an existing IPv6 ACL.
Delete	Click Delete to remove the currently selected IP ACL from the switch configuration. This button is shown when you want to delete an existing IPv6 ACL.

Summary

The Summary page displays a summary of existing IP ACL IDs and the rules assigned for each. To access this page, click **QoS > Access Control Lists > IP Access Control Lists > Summary**.

IP ACL Summary

IP ACL ID/Name	Rules	Direction	Interface	VLAN
Refresh				

Figure 3-183. QoS > Access Control Lists > IP Access Control Lists > Summary

The following table describes the items in the previous menu.

Table 3-180. QoS > Access Control Lists > IP Access Control Lists > Summary

Parameter	Description
IP ACL ID/Name	Displays the IP ACL identifier.
Rules	Displays the number of rules currently configured for the IP ACL.
Direction	Displays the direction of packet traffic affected by the IP ACL. Direction can only be one of the following: <ul style="list-style-type: none"> • Inbound • Outbound
Interface	Displays the interfaces to which the IP ACL has been applied.
VLAN	Displays the VLANs to which the IP ACL has been applied.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Rule Configuration

The Rule Configuration page allows users to configure rules for the IP Access Control Lists created using the IP Access Control List Configuration screen. To access this page, click **QoS > Access Control Lists > IP Access Control Lists > Rule Configuration**.

IP ACL Rule Configuration

No ACLs Are Configured

Figure 3-184. QoS > Access Control Lists > IP Access Control Lists > Rule Configuration

The following table describes the items in the previous menu.

Table 3-181. QoS > Access Control Lists > IP Access Control Lists > Rule Configuration

Parameter	Description
IP ACL	Click the drop-down menu to select the IP ACL for which to create or update a rule.
Rule	Click the drop-down menu to select an existing rule from the pull-down menu or select 'Create New Rule.' ACL as well as an option to add a new Rule. New rules cannot be created if the maximum number of rules has been reached. For each rule, a packet must match all the specified criteria in order to be true against that rule and for the specified rule action (Permit/Deny) to take place.
Rule ID	Enter a whole number in the range of 1 to 1023 that will be used to identify the rule. An IP ACL may have up to 1023 rules.
Action	Click the drop-down menu to specify the policy a packet. The choices are permit or deny.
Logging	Displays the logging rule. When set to 'True', logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was 'hit' during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval.
Assign Queue ID	Displays the queue ID value. Specifies the hardware egress queue identifier used to handle all packets matching this IP ACL rule. Valid range of Queue Ids is 0 to 7. This field is visible for a 'Permit' Action.
Mirror Interface	Displays the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. This field cannot be set if a Redirect Interface is already configured for the ACL rule. This field is visible for a 'Permit' Action.
Redirect Interface	Displays the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field cannot be set if a Mirror Interface is already configured for the ACL rule. This field is visible for a 'Permit' Action.
Match Every	Displays the match policy (true or false). True signifies that all packets will match the selected IP ACL and Rule and will be either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria will not be offered. To configure specific match criteria for the rule, remove the rule and re-create it, or re-configure 'Match Every' to 'False' for the other match criteria to be visible.
Protocol Keyword	Displays the IP protocol match condition status for the selected IP ACL rule. The possible values are ICMP, IGMP, IP, TCP, and UDP. Either the 'Protocol Keyword' field or the 'Protocol Number' field can be used to specify an IP protocol value as a match criterion.

Table 3-181. QoS > Access Control Lists > IP Access Control Lists > Rule Configuration (Continued)

Parameter	Description
Protocol Number	Displays the IP protocol match condition for the selected IP ACL rule and identify the protocol by number. The protocol number is a standard value assigned by IANA and is interpreted as an integer from 1 to 255. Either the 'Protocol Number' field or the 'Protocol Keyword' field can be used to specify an IP protocol value as a match criterion.
Source IP Address	Enter an IP address using dotted- decimal notation to be compared to a packet's source IP Address as a match criteria for the selected IP ACL rule.
Source IP wildcard mask	Enter the IP wildcard mask in dotted-decimal notation to be used with the Source IP Address value.
Source L4 Port Keyword	Enter a packet's source layer 4 port as a match condition for the selected extended IP ACL rule. This is an optional configuration. The possible values are DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range. Either the 'Source L4 Port Keyword' field or the 'Source L4 Port Range' fields can be used to specify a source layer 4 port range as a match criterion.
Source L4 Port Number	Enter a packet's source layer 4 port as a match condition for the selected extended IP ACL rule. This is an optional configuration.
Source L4 Port Range (start port)	Enter the first port of the port range for a packet's source layer 4 port match condition for the selected extended IP ACL rule. Range of valid values is 0 to 65535. The value of the start port must be less than or equal to the end port. The start port, end port, and all ports in between will be part of the contiguous source port range. This is an optional configuration.
Source L4 Port Range (end port)	Enter the last port of the port range for a packet's source layer 4 port match condition for the selected extended IP ACL rule. Range of valid values is 0 to 65535. The value of the end port must be greater than or equal to the start port. The start port, end port, and all ports in between will be part of the contiguous source port range. This is an optional configuration.
Destination IP Address	Enter an IP address using dotted-decimal notation to be compared to a packet's destination IP Address as a match criteria for the selected extended IP ACL rule.
Destination IP wildcard mask	Enter the IP wildcard mask in dotted-decimal notation to be used with the Destination IP Address value.
Destination L4 Port Keyword	Enter the destination layer 4 port match conditions for the selected extended IP ACL rule. The possible values are DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range. Either this field or the 'Destination L4 Port Range' fields can be used to specify a destination layer 4 port range as a match criterion. This is an optional configuration.
Destination L4 Port Number	Enter a packet's destination layer 4 port number match condition for the selected extended IP ACL rule. This is an optional configuration.

Table 3-181. QoS > Access Control Lists > IP Access Control Lists > Rule Configuration (Continued)

Parameter	Description
Destination L4 Port Range (start port)	Enter a packet's destination layer 4 port match condition for the selected extended IP ACL rule. This field identifies the first port of the port range and has a value from 0 to 65535. The value of the start port must be less than or equal to the end port. The start port, end port, and all ports in between will be part of the contiguous source port range. This is an optional configuration.
Destination L4 Port Range (end port)	Enter a packet's destination layer 4 port match condition for the selected extended IP ACL rule. This field identifies the last port of the port range and has a value from 0 to 65535. The value of the end port must be greater than or equal to the start port. The start port, end port, and all ports in between will be part of the contiguous source port range. This is an optional configuration.
Service Type	<p>Click the drop-down menu to select a Service Type match condition for the extended IP ACL rule from the pull-down menu. The possible values are IP DSCP, IP precedence, and IP TOS, which are alternative ways of specifying a match criterion for the same Service Type field in the IP header, however each uses a different user notation. After a selection is made the appropriate value can be specified.</p> <ul style="list-style-type: none"> ● IP DSCP Configuration Specify the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high- order six bits of the Service Type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 63. The IP DSCP is selected by possibly selection one of the DSCP keyword from a drop-down box. If a value is to be selected by specifying its numeric value, then select the 'Other' option in the drop-down box and a text box will appear where the numeric value of the DSCP can be entered. ● IP Precedence Configuration The IP Precedence field in a packet is defined as the high- order three bits of the Service Type octet in the IP header. This is an optional configuration. Enter an integer from 0 to 7. ● IP TOS Configuration The IP TOS field in a packet is defined as all eight bits of the Service Type octet in the IP header. The TOS Bits value is a two- digit hexadecimal number from 00 to ff. The TOS Mask value is a two- digit hexadecimal number from 00 to ff, representing an inverted (i.e. wildcard) mask. The zero- valued bits in the TOS Mask denote the bit positions in the TOS Bits value that are used for comparison against the IP TOS field of a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a TOS Bits value of a0 and a TOS Mask of 00. This is an optional configuration.
Configure	Click Configure to setup the corresponding match criteria for the selected rule.
Delete	Click Delete to remove the currently selected Rule from the selected ACL. These changes will not be retained across a power cycle unless a save configuration is performed.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save. This button is shown when you are configuring individual match conditions.
Cancel	Click Cancel to discard the changes made on the page.

IPv6 Access Control Lists

Configuration

The Configuration page allows users to configure settings for existing IPv6 ACLs or create new ones. To access this page, click **QoS > Access Control Lists > IPv6 Access Control Lists > Configuration**.

IPv6 ACL Configuration

Table	Current Number / Maximum Number
ACL	0 / 100

Figure 3-185. QoS > Access Control Lists > IPv6 Access Control Lists > Configuration

The following table describes the items in the previous menu.

Table 3-182. QoS > Access Control Lists > IPv6 Access Control Lists > Configuration

Parameter	Description
IPv6 ACL	Click the drop-down menu to select a new IPv6 ACL entry or the configure an existing IPv6 ACL can be updated by selecting right option from the pull-down menu.
IPv6 ACL Name	Enter the IPv6 ACL Name string which includes alphanumeric characters only. The name must start with an alphabetic character. This field displays the name of the currently selected IPv6 ACL if the ACL has already been created. The name can have 1 to 31 alphanumeric characters.
Table	Displays the current number/maximum number of ACLs.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save. This button is shown when you create a new IPv6 ACL.
Rename	Click Rename to rename the currently selected IPv6 ACL and shows up only when an existing IPv6 ACL is selected.
Delete	Click Delete to remove the currently selected IPv6 ACL and shows up only when an existing IPv6 ACL is selected.

Summary

The Summary page displays a summary of existing IPv6 ACL IDs and the rules assigned for each. To access this page, click **QoS > Access Control Lists > IPv6 Access Control Lists > Summary**.

IPv6 ACL Summary

IPv6 ACL Name	Rules	Direction	Interface	VLAN
Refresh				

Figure 3-186. QoS > Access Control Lists > IPv6 Access Control Lists > Summary

The following table describes the items in the previous menu.

Table 3-183. QoS > Access Control Lists > IPv6 Access Control Lists > Summary

Parameter	Description
IPv6 ACL Name	Displays the IPv6 ACL identifier.
Rules	Displays the number of rules currently configured for the IPv6 ACL.
Direction	Displays the direction of packet traffic affected by the IPv6 ACL. Direction can only be one of the following: <ul style="list-style-type: none"> • Inbound • Outbound
Interface	Displays the interfaces to which the IPv6 ACL has been applied.
VLAN	Displays the VLANs to which the IPv6 ACL has been applied.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

Rule Configuration

The Rule Configuration page allows users to configure the rules for the IPv6 Access Control Lists. To access this page, click **QoS > Access Control Lists > IPv6 Access Control Lists > Rule Configuration**.

IPv6 ACL Rule Configuration

No ACLs Are Configured

Figure 3-187. QoS > Access Control Lists > IPv6 Access Control Lists > Rule Configuration

The following table describes the items in the previous menu.

Table 3-184. QoS > Access Control Lists > IPv6 Access Control Lists > Rule Configuration

Parameter	Description
IPv6 ACL Name	Click the drop-down menu to select the IPv6 ACL for which to create or update a rule.
Rule	Click the drop-down menu to select an existing rule from the pull-down menu or select 'Create New Rule.' New rules cannot be created if the maximum number of rules has been reached. For each rule, a packet must match all the specified criteria in order to be true against that rule and for the specified rule action (Permit/Deny) to take place.
Rule ID	Enter a whole number in the range of 1 to 1023 that will be used to identify the rule.
Action	Click the drop-down menu to select the policy (permit or deny).
Logging	Click the drop-down menu to enable or disable the logging function. If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was 'hit' during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval.
Assign Queue ID	Enter a value to specify the hardware egress queue identifier used to handle all packets matching this IPv6 ACL rule. Valid range of Queue IDs is 0 to 7. This field is visible for a 'Permit' Action.
Mirror Interface	Displays the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. This field cannot be set if a Redirect Interface is already configured for the ACL rule. This field is visible for a 'Permit' Action.
Redirect Interface	Displays the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field cannot be set if a Mirror Interface is already configured for the ACL rule. This field is visible for a 'Permit' Action.
Match Every	Click the drop-down menu to select the matching rule. True signifies that all packets will match the selected IPv6 ACL and Rule and will be either permitted or denied. In this case, since all packets match the rule, the option of configuring other match criteria will not be offered. To configure specific match criteria for the rule, remove the rule and re-create it, or re-configure 'Match Every' to 'False' for the other match criteria to be visible.
Protocol	Enter a value to configure IPv6 protocol. <ul style="list-style-type: none"> Specify an integer ranging from 0 to 255 after selecting protocol keyword "other". This number represents the IP protocol. Select name of a protocol from the existing list of Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).

Table 3-184. QoS > Access Control Lists > IPv6 Access Control Lists > Rule Configuration (Continued)

Parameter	Description
Source Prefix/Prefix-Length	Enter a value to specify the IPv6 Prefix--combined with IPv6 Prefix length of the network or host from which the packet is being sent. Prefix length can be in the range 0 to 128.
Source L4 Port	Enter a value to specify a packet's source layer 4 port as a match condition for the selected IPv6 ACL rule. Source port information is optional. Source port information can be specified in two ways: <ul style="list-style-type: none"> • Select keyword "other" from the drop down menu and specify the number of the port in the range from 0 to 65535. • Select one of the keyword from the list: DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range.
Source L4 Port Range (start port)	Enter a value to specify the first port of the port range for a packet's source layer 4 port match condition for the selected IPv6 ACL rule. Range of valid values is 0 to 65535. The value of the start port must be less than or equal to the end port. The start port, end port, and all ports in between will be part of the contiguous source port range. This is an optional configuration.
Source L4 Port Range (end port)	Enter a value to specify the last port of the port range for a packet's source layer 4 port match condition for the selected IPv6 ACL rule. Range of valid values is 0 to 65535. The value of the end port must be greater than or equal to the start port. The start port, end port, and all ports in between will be part of the contiguous source port range. This is an optional configuration.
Destination Prefix/PrefixLength	Enter up to 128-bit prefix combined with prefix length to be compared to a packet's destination IP Address as a match criteria for the selected IPv6 ACL rule. Prefix length can be in the range 0 to 128.
Destination L4 Port Keyword	Enter a value to specify the destination layer 4 port match conditions for the selected IPv6 ACL rule. The possible values are DOMAIN, ECHO, FTP, FTPDATA, HTTP, SMTP, SNMP, TELNET, TFTP, and WWW. Each of these values translates into its equivalent port number, which is used as both the start and end of the port range. Either this field or the 'Destination L4 Port Range' fields can be used to specify a destination layer 4 port range as a match criterion. This is an optional configuration.
Destination L4 Port Number	Enter a packet's destination layer 4 port number match condition for the selected IPv6 ACL rule. This is an optional configuration.
Destination L4 Port Range (start port)	Enter a packet's destination layer 4 port match condition for the selected IPv6 ACL rule. This field identifies the first port of the port range and has a value from 0 to 65535. The value of the start port must be less than or equal to the end port. The start port, end port, and all ports in between will be part of the contiguous source port range. This is an optional configuration.
Destination L4 Port Range (end port)	Enter a packet's destination layer 4 port match condition for the selected IPv6 ACL rule. This field identifies the last port of the port range and has a value from 0 to 65535. The value of the end port must be greater than or equal to the start port. The start port, end port, and all ports in between will be part of the contiguous source port range. This is an optional configuration.

Table 3-184. QoS > Access Control Lists > IPv6 Access Control Lists > Rule Configuration (Continued)

Parameter	Description
Flow Label	Enter a label is 20-bit number that is unique to an IPv6 packet, used by end stations to signify quality-of-service handling in routers. Flow label can specified within the range 0 to 1048575.
IPv6 DSCP Service	Enter the IP DiffServ Code Point (DSCP) field. The DSCP is defined as the high-order six bits of the Service Type octet in the IPv6 header. This is an optional configuration. Enter an integer from 0 to 63. The IPv6 DSCP is selected by possibly selection one of the DSCP keyword from a drop-down box. If a value is to be selected by specifying its numeric value, then select the 'Other' option in the drop-down box and a text box will appear where the numeric value of the DSCP can be entered.
Configure	Click Configure to setup the corresponding match criteria for the selected rule.
Delete	Click Delete to remove the currently selected Rule from the selected ACL. These changes will not be retained across a power cycle unless a save configuration is performed.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save. This button is shown when you are configuring individual match conditions.
Cancel	Click Cancel to discard the changes made on the page.

MAC Access Control Lists

Configuration

The Configuration page allows users to configure settings for existing MAC ACLs or create new ones. To access this page, click **QoS > Access Control Lists > MAC Access Control Lists > Configuration**.

MAC ACL Configuration

MAC ACL
Create New Extended MAC ACL ▾

MAC ACL Name

(Max 31 characters)

Table	Current Number / Maximum Number
ACL	n / 100

Figure 3-188. QoS > Access Control Lists > MAC Access Control Lists > Configuration

The following table describes the items in the previous menu.

Table 3-185. QoS > Access Control Lists > MAC Access Control Lists > Configuration

Parameter	Description
MAC ACL	Click the drop-down menu to create or configure an existing MAC ACL.
MAC ACL Name	Enter the MAC ACL name (start with a alphanumeric and up to 31 characters, include alphabetic, numeric, dash, underscore or dot)
Table	Displays the current number/maximum number of MAC ACLS.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Rename	Click Rename to rename the selected MAC ACL.
Delete	Click Delete to remove the selected MAC ACL.

Summary

The Summary page displays a summary of existing MAC ACL IDs and the rules assigned for each. To access this page, click **QoS > Access Control Lists > MAC Access Control Lists > Summary**.

MAC ACL Summary

MAC ACL Name	Rules	Direction	Interface	VLAN
Refresh				

Figure 3-189. QoS > Access Control Lists > MAC Access Control Lists > Summary The following table describes the items in the previous menu.

Table 3-186. QoS > Access Control Lists > MAC Access Control Lists > Summary

Parameter	Description
MAC ACL Name	Displays the MAC ACL name.
Rules	Displays the number of rules configured for the MAC ACL.
Direction	Displays the direction of packet traffic affected by the MAC ACL. The options are: <ul style="list-style-type: none"> • Inbound • Outbound
Interface	Displays the interfaces that the MAC ACL has been applied.
VLAN	Displays the VLANs that the MAC ACL has been applied.
Refresh	Click Refresh to update the screen.

Rule Configuration

The Rule Configuration page allows users to configure the rules for the MAC Access Control Lists. To access this page, click **QoS > Access Control Lists > MAC Access Control Lists > Rule Configuration**.

MAC ACL Rule Configuration

No MAC ACLs Configured

Figure 3-190. QoS > Access Control Lists > MAC Access Control Lists > Rule Configuration The following table describes the items in the previous menu.

Table 3-187. QoS > Access Control Lists > MAC Access Control Lists > Rule Configuration

Parameter	Description
MAC ACL Name	Click the drop-down menu to update the rule.
Rule	Click the drop-down menu to create or configure an existing rule.
Rule ID	Enter the rule ID (between 1 to 1023).
Action	Click Configure and click drop-down menu to select Permit or Deny if a packet matches the rule's criteria.
Match Every	Click Configure and click drop-down menu to select an indication to match every layer 2 MAC packet. The options are: <ul style="list-style-type: none"> • True - Signifies that every packet is considered to match the selected ACL Rule. • False - Signifies that it is not mandatory for every packet to match the selected ACL Rule.
Logging	Displays login status. When set to 'True', logging is enabled for this ACL rule (subject to resource availability in the device). If the Access List Trap Flag is also enabled, this will cause periodic traps to be generated indicating the number of times this rule was 'hit' during the current report interval. A fixed 5 minute report interval is used for the entire system. A trap is not issued if the ACL rule hit count is zero for the current interval.
Assign Queue ID	Displays the queue identifier. Specifies the hardware egress queue identifier used to handle all packets matching this ACL rule. Valid range of Queue Ids is 0 to 7. This field is visible for a 'Permit' Action.
Mirror Interface	Enter the specific egress interface where the matching traffic stream is copied in addition to being forwarded normally by the device. This field cannot be set if a Redirect Interface is already configured for the ACL rule. This field is visible for a 'Permit' Action.
Redirect Interface	Enter the specific egress interface where the matching traffic stream is forced, bypassing any forwarding decision normally performed by the device. This field cannot be set if a Mirror Interface is already configured for the ACL rule. This field is visible for a 'Permit' Action.

Table 3-187. QoS > Access Control Lists > MAC Access Control Lists > Rule Configuration (Continued)

Parameter	Description
CoS	Click Configure and enter the 802.1p user priority (between 0 to 7) to compare against an Ethernet frame.
Secondary CoS	Click Configure and enter the secondary 802.1p user priority (between 0 to 7) to compare against an Ethernet frame.
Destination MAC	Click Configure and enter the MAC address (XX:XX:XX:XX:XX:XX) to compare against an Ethernet frame.
Destination MAC Mask	Click Configure and enter the MAC mask address (XX:XX:XX:XX:XX:XX) to compare against an Ethernet frame.
Ethertype Key	Click Configure and click the drop-down menu to select the ethertype value. The options are: <ul style="list-style-type: none"> ● Appletalk ● ARP ● IBM SNA ● IPv4 ● IPv6 ● IPX ● MPLS multicast ● MPLS unicast ● NetBIOS ● Novell ● PPPoE ● Reverse ARP ● User Value
Ethertype User Value	Click Configure and enter the Ether-type value (between 0x0600 to 0xFFFF) when Ether-type Key is User Value.
Source MAC	Click Configure and enter the MAC address (XX:XX:XX:XX:XX:XX).
Source MAC Mask	Click Configure and enter the MAC mask address (XX:XX:XX:XX:XX:XX).
VLAN Range	
From	Click Configure and enter the VLAN ID (between 0 to 4095) to compare against an Ethernet frame.
To	Click Configure and enter the VLAN ID (between 0 to 4095) to compare against an Ethernet frame.
VLAN	Click Configure and enter the VLAN ID (between 0 to 4095) to compare against an Ethernet frame.
Secondary VLAN Range	

Table 3-187. QoS > Access Control Lists > MAC Access Control Lists > Rule Configuration (Continued)

Parameter	Description
From	Click Configure and enter the secondary VLAN ID (between 0 to 4095) to compare against an Ethernet frame.
To	Click Configure and enter the secondary VLAN ID (between 0 to 4095) to compare against an Ethernet frame.
Secondary VLAN	Click Configure and enter the secondary VLAN ID (between 0 to 4095) to compare against an Ethernet frame.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Remove to remove the selected rule. To save the values across a power cycle perform a system save.

Interface Configuration

The Interface Configuration page allows users to configure settings for each ACL interface. To access this page, click **QoS > Access Control Lists > Interface Configuration**.

ACL Interface Configuration

The screenshot shows the ACL Interface Configuration page. At the top, there is a form with the following fields:

- Interface:** A dropdown menu currently showing 'ge0/1'.
- Direction:** A dropdown menu currently showing 'In/Out'.
- ACL Type:** A dropdown menu.
- Sequence Number:** A text input field containing '1'. To its right, a note reads: 'Range 1 to 4294967295. Enter 0 for auto generate.'

 Below the form is a section titled 'List of Assigned ACLs' which contains a table with the following columns: Interface, Direction, Sequence Number, ACL Type, and ACL ID. Below the table is a 'Submit' button.

Figure 3-191. QoS > Access Control Lists > Interface Configuration

The following table describes the items in the previous menu.

Table 3-188. QoS > Access Control Lists > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the interface for ACL mapping.
Direction	Click the drop-down menu to select the packet filtering direction for ACL. The options are: <ul style="list-style-type: none"> • Inbound • Outbound
ACL Type	Click the drop-down menu to select the type of ACL. The options are: <ul style="list-style-type: none"> • IP ACL • MAC ACL • IPv6 ACL

Table 3-188. QoS > Access Control Lists > Interface Configuration (Continued)

Parameter	Description
IP ACL	Click the drop-down menu to select a IP ACL. And it's only available when ACL Type is IP ACL.
MAC ACL	Click the drop-down menu to select a MAC ACL. And it's only available when ACL Type is MAC ACL.
IPv6 ACL	Click the drop-down menu to select a IPv6 ACL. And it's only available when ACL Type is IPv6 ACL.
Sequence Number	Enter a sequence number (between 0 to 4294967295, 0 means auto generate) to indicate the order of this access list.
List of AssignedACLs	
Interface	Displays the selected interface.
Direction	Displays the selected packet filtering direction for ACL.
Sequence Number	Displays the sequence number of the specified ACL.
ACL Type	Displays the type of ACL assigned to selected interface and direction.
ACL ID	Displays the ACL number or ACL name assigned to selected interface and direction.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Remove	Click Remove to remove the selected ACL interface direction mapping.

VLAN Configuration

The VLAN Configuration page allows users to configure settings for each VLAN ID. To access this page, click **QoS > Access Control Lists > VLAN Configuration**.

VLAN Based ACL Configuration

VLAN ID	<input type="text" value="1"/>			
Direction	<input type="text" value="Inbound"/>			
ACL Type	<input type="text"/>			
Sequence Number	<input type="text"/> (1 to 4294967295)			
<input type="button" value="Submit"/>				
List of Assigned ACLs				
VLAN ID	Direction	ACL Type	ACL Identifier	Sequence Number

Figure 3-192. QoS > Access Control Lists > VLAN Configuration

The following table describes the items in the previous menu.

Table 3-189. QoS > Access Control Lists > VLAN Configuration

Parameter	Description
VLAN ID	Click the drop-down menu to select a VLAN ID for ACL mapping.
Direction	Click the drop-down menu to select the packet filtering direction for ACL. The options are: <ul style="list-style-type: none"> • Inbound • Outbound
ACL Type	Click the drop-down menu to select the type of ACL. The options are: <ul style="list-style-type: none"> • IP ACL • MAC ACL • IPv6 ACL
IP ACL	Click the drop-down menu to select a IP ACL. And it's only available when ACL Type is IP ACL.
MAC ACL	Click the drop-down menu to select a MAC ACL. And it's only available when ACL Type is MAC ACL.
IPv6 ACL	Click the drop-down menu to select a IPv6 ACL. And it's only available when ACL Type is IPv6 ACL.
Sequence Number	Enter a sequence number (between 1 to 4294967295, 0 means auto generate) to indicate the order of this access list.
List of AssignedACLs	
VLAN ID(s)	Displays the list of VLAN ID.
Direction	Displays the selected packet filtering direction for ACL.
ACL Type	Displays the type of ACL assigned to the selected VLAN and direction.
ACL Identifier	Displays the ACL number or ACL name assigned to the selected VLAN and direction.
Sequence Number	Displays the sequence number of the specified VLAN and direction.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Remove	Click Remove to remove the selected VLAN direction mapping.

Interface/VLAN Summary

The Interface/VLAN Summary displays a list of existing Interfaces and VLANs and the settings assigned for each. To access this page, click **QoS > Access Control Lists > Interface/VLAN Summary**.

Interface or VLAN based ACL(s) Summary

Summary Display Selector interface ▼

Interface	Direction	Sequence Number	ACL Type	ACL ID
<input type="button" value="Refresh"/>				

Figure 3-193. QoS > Access Control Lists > Interface/VLAN Summary

The following table describes the items in the previous menu.

Table 3-190. QoS > Access Control Lists > Interface/VLAN Summary

Parameter	Description
Summary Display Selector	Click the drop-down menu to select an interface or VLAN.
Interface	Displays the list of interface IP ACL applied.
VLAN ID	Displays the list of VLAN IP ACL applied.
Direction	Displays the direction of packet traffic affected by the IP ACL.
Sequence Number	Displays the sequence number of the specified VLAN and direction.
ACL Type	Displays the type of ACL assigned to the selected VLAN and direction.
ACL ID	Displays the ACL number or ACL name assigned to the selected VLAN and direction.
Refresh	Click Refresh to update the screen.

3.7.2 Differentiated Services

Diffserv Configuration

The Diffserv Configuration allows users to enable or disable differentiate traffic based on its class. To access this page, click **QoS > Differentiated Services > Diffserv Configuration**.

Diffserv Configuration

DiffServ Admin Mode	Enable ▾	Submit
MIB Table	Current Number / Maximum Number	
Class Table	- / 32	
Class Rule Table	0 / 416	
Policy Table	1 / 64	
Policy Instance Table	0 / 1792	
Policy Attribute Table	0 / 5576	
Service Table	0 / 24	

Figure 3-194. QoS > Differentiated Services > Diffserv Configuration

The following table describes the items in the previous menu.

Table 3-191. QoS > Differentiated Services > Diffserv Configuration

Parameter	Description
DiffServ Admin Mode	Click the drop-down menu to enable or disable DiffServ services.
Class Table	Displays the number of configured DiffServ classes out of the total allowed on the switch.
Class Rule Table	Displays the number of configured class rules out of the total allowed on the switch.
Policy Table	Displays the number of configured policies out of the total allowed on the switch.
Policy Instance Table	Displays the number of configured policy instances out of the total allowed on the switch.
Policy Attributes Table	Displays the number of configured policy attributes out of the total allowed on the switch.
Service Table	Displays the number of configured services out of the total allowed on the switch.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

Class Configuration

The Class Configuration page allows users to configure criteria for each class. To access this page, click **QoS > Differentiated Services > Class Configuration**.

DiffServ Class Configuration

Figure 3-195. QoS > Differentiated Services > Class Configuration

The following table describes the items in the previous menu.

Table 3-192. QoS > Differentiated Services > Class Configuration

Parameter	Description
Class Selector	Click the drop-down menu to create or configure an existing class.
Class Name	Enter a class name (between 1 to 31 alphanumeric characters, case-sensitive, default is not available)
Class Type	Displays the selected class type.
Class Layer 3 Protocol	Click the drop-down menu to select or display the protocol to indicate how to interpret any layer 3. The options are: <ul style="list-style-type: none"> • IPv4 • IPv6
Class Match Selector	Click the drop-down menu to select a match criteria to a selected class. <ul style="list-style-type: none"> • If the specified class does not reference any other class, the 'Reference Class' match criterion is included in the drop down match criteria list. A class reference can be established by selecting 'Reference Class' and invoking the 'Add Match Criteria' button. • If the specified class references another class, the 'Reference Class' match criterion is not included in the drop down match criteria list. This prevents the user from trying to add yet another class reference, since a specified class can reference at most one other class of the same type. Moreover, a 'Remove Reference Class' button appears on the screen that can be invoked to remove the current class reference.
Match Criteria	Displays the configured match criteria for the specified class.
Values	Displays the values of the configured match criteria.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Cancel	Click Cancel to discard the changes made on the page.

Table 3-192. QoS > Differentiated Services > Class Configuration (Continued)

Parameter	Description
Delete	Click Delete to delete the selected class.
Rename	Click Rename to rename the selected class.
Add Match Criteria	Click Add Match Criteria to specify match criteria. NOTE: Delete the match criteria by deleting the class.
Remove Reference Class	Click Remove Reference Class to delete class reference. And it is only available when a specified class references to another class.

Class Summary

The Class Summary page displays a list of each class name and type, as well as reference class. To access this page, click **QoS > Differentiated Services > Class Summary**.

DiffServ Class Summary

Class Name	Class Type	Reference Class
:	AI(1FV+)	

Figure 3-196. QoS > Differentiated Services > Class Summary

The following table describes the items in the previous menu.

Table 3-193. QoS > Differentiated Services > Class Summary

Parameter	Description
Class Name	Displays the name of DiffServ classes.
Class Type	Displays the type of the class with the layer 3 protocol of the class.
Reference Class	Displays the reference class name of the class.
Refresh	Click Refresh to update the screen.

Policy Configuration

The Policy Configuration page allows users to add policies to existing interfaces. To access this page, click **QoS > Differentiated Services > Policy Configuration**.

DiffServ Policy Configuration

Policy Selector	1		
Policy Name	1	(1 to 31 alphanumeric characters)	<input type="button" value="Rename"/> <input type="button" value="Delete"/>
Policy Type	In		
Available Class List	1		<input type="button" value="Add Selected Class"/>
Member Class List	No Member Classes		

Figure 3-197. QoS > Differentiated Services > Policy Configuration

The following table describes the items in the previous menu.

Table 3-194. QoS > Differentiated Services > Policy Configuration

Parameter	Description
Policy Selector	Click the drop-down menu to create or configure an existing policy.
Policy Name	Enter the policy name (between 1 to 31 alphanumeric).
Policy Type	Click the drop-down menu to select traffic direction.
Available Class List	Click the drop-down menu to select an existing class for the policy.
Member Class List	Click the drop-down menu to select an existing class for the policy.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.
Delete	Click Delete to delete the selected policy.
Rename	Click Rename to rename the selected policy.
Add Selected Class	Click Add Selected Class to create a policy class instance by attaching the policy to the specified class.
Remove Selected Class	Click Remove Selected Class to remove a policy class instance by detaching the policy from the specified class.

Policy Summary

The Policy Summary page displays a list of each class name and type, as well as reference class. To access this page, click **QoS > Differentiated Services > Policy Summary**.

DiffServ Policy Summary

Policy Name	Policy Type	Member Classes
1	Ir	

Figure 3-198. QoS > Differentiated Services > Policy Summary

The following table describes the items in the previous menu.

Table 3-195. QoS > Differentiated Services > Policy Summary

Parameter	Description
Policy Name	Displays the name of DiffServ policy.
Policy Type	Displays the type of DiffServ policy.
Member Classes	Displays the name of each class instance within DiffServ policy.
Refresh	Click Refresh to update the screen.

Policy Class Definition

The Policy Class Definition page allows users to a policy. To access this page, click **QoS > Differentiated Services > Policy Class Definition**.

DiffServ Policy Class Definition

The screenshot shows a web form titled "DiffServ Policy Class Definition". It contains three main sections: "Policy Selector" with a dropdown menu, "Policy Type" with a text input field containing "in", and "Member Class List" with a text input field containing "No Member Classes".

Figure 3-199. QoS > Differentiated Services > Policy Class Definition

The following table describes the items in the previous menu.

Table 3-196. QoS > Differentiated Services > Policy Class Definition

Parameter	Description
Policy Selector	Click the drop-down menu to select the DiffServ policy name.
Policy Type	Displays the type of the policy.
Member Class List	Displays the DiffServ classes of the policy.
Policy Attribute Selector	Displays all attributes supported for this type of policy, from which one can be selected.
Configure Selected Attribute	Click Configure Selected Attribute to configuration criterion can be specified per invocation of this button. Based on the selected configuration criterion, an individual configuration screen is provided.

Policy Attribute Summary

The Policy Attribute Summary page displays the list of selected policies and attributes assigned for each. To access this page, click **QoS > Differentiated Services > Policy Attribute Summary**.

DiffServ Policy Attribute Summary

The screenshot shows a table with five columns: "Policy Name", "Policy Type", "Class Name", "Attribute", and "Attribute Details". Below the table is a "Refresh" button.

Figure 3-200. QoS > Differentiated Services > Policy Attribute Summary

The following table describes the items in the previous menu.

Table 3-197. QoS > Differentiated Services > Policy Attribute Summary

Parameter	Description
Policy Name	Displays the name of the DiffServ policy.
Policy Type	Displays the type of the DiffServ policy.
Class Name	Displays the name of the DiffServ class attached by the policy.
Attribute	Displays the attributes attached to the policy class instances.

Table 3-197. QoS > Differentiated Services > Policy Attribute Summary (Continued)

Parameter	Description
Attribute Details	Displays the configured values of the attached attributes.
Refresh	Click Refresh to update the screen.

Service Configuration

The Service Configuration page allows users to select an interface and assign an In/Out policy for each. To access this page, click **QoS > Differentiated Services > Service Configuration**.

DiffServ Service Configuration

The screenshot shows a web form titled "DiffServ Service Configuration". It contains three dropdown menus stacked vertically. The first is labeled "Interface" and has "ge0/1" selected. The second is labeled "Policy In" and has "None" selected. The third is labeled "Policy Out" and has "None" selected. Below these menus is a "Submit" button.

Figure 3-201. QoS > Differentiated Services > Service Configuration

The following table describes the items in the previous menu.

Table 3-198. QoS > Differentiated Services > Service Configuration

Parameter	Description
Interface	Click the drop-down menu to select an interface.
Direction	Click the drop-down menu to select the traffic direction of the interface. It is only available when Interface is All.
Policy In	Click the drop-down menu to select a policy name and the policy type is In.
Policy Out	Click the drop-down menu to select a policy name and the policy type is Out.
Table Interface	Displays the interface that uniquely specifies an interface. It is only available when Interface is All.
Table Direction	Displays the traffic direction for this service interface. It is only available when Interface is All.
Table Operational Status	Displays the operational status of this service interface. It is only available when Interface is All.
Table Policy Name	Displays the name of the attached policy. It is only available when Interface is All.
Submit	Click Submit to update the screen. To save the values across a power cycle perform a system save.

Service Summary

The Service Summary page displays a list of the interfaces and summary for each. To access this page, click **QoS > Differentiated Services > Service Summary**.

DiffServ Service Summary

Interface	Direction	Operational Status	Policy Name
Refresh			

Figure 3-202. QoS > Differentiated Services > Service Summary

The following table describes the items in the previous menu.

Table 3-199. QoS > Differentiated Services > Service Summary

Parameter	Description
Interface	Displays the interface that uniquely specifies an interface.
Direction	Displays the traffic direction for this service interface.
Operational Status	Displays the operational status of this service interface.
Policy Name	Displays the name of the attached policy.
Refresh	Click Refresh to update the screen.

Service Statistics

The Service Statistics page displays service-level statistical information in tabular form for all interfaces in the system to which a DiffServ policy has been attached. To access this page, click **QoS > Differentiated Services > Service Statistics**.

DiffServ Service Statistics

Counter Mode Selector	Octets
-----------------------	--------

Interface	Direction	Operational Status	Offered Octets	Discarded Octets	Sent Octets
Refresh					

Figure 3-203. QoS > Differentiated Services > Service Statistics

The following table describes the items in the previous menu.

Table 3-200. QoS > Differentiated Services > Service Statistics

Parameter	Description
Counter Mode Selector	Click the drop-down menu to select the format of the displayed counter values. The default is Octets.
Interface	Displays the interface that uniquely specifies an interface.
Direction	Displays the traffic direction for this service interface.
Operational Status	Displays the operational status of this service interface.

Table 3-200. QoS > Differentiated Services > Service Statistics (Continued)

Parameter	Description
Offered Packets/Octets	Displays the count of the total number of packets/octets offered to all class instances.
Discarded Packets/Octets	Displays the count of the total number of packets/octets discarded for all class instances.
Sent Packets/Octets	Displays the count of the total number of packets/octets forwarded for all class instances.
Refresh	Click Refresh to update the screen.

Service Detailed Statistics

The Service Detailed Statistics page displays class-oriented statistical information for the policy specified by the interface and direction. To access this page, click **QoS > Differentiated Services > Service Detailed Statistics**.

DiffServ Service Detailed Statistics

Counter Mode Selector Octets ▾

Interface None ▾

Direction In ▾

Policy Name

Operational Status

Member Classes None ▾

Offered Octets

Discarded Octets

Figure 3-204. QoS > Differentiated Services > Service Detailed Statistics The following table describes the items in the previous menu.

Table 3-201. QoS > Differentiated Services > Service Detailed Statistics

Parameter	Description
Counter Mode Selector	Click the drop-down menu to select the format of the displayed counter values. The default is Octets.
Interface	Click the drop-down menu to select the interface. List of all valid slot number and port number combinations in the system that have a DiffServ policy currently attached in In direction.
Direction	Click the drop-down menu to select a direction for statistics.
Policy Name	Displays the policy name attached to the interface and direction.
Operational Status	Displays the policy operational status attached to the interface and direction.

Table 3-201. QoS > Differentiated Services > Service Detailed Statistics (Continued)

Parameter	Description
Member Classes	Click the drop-down menu to select a DiffServ class defined as members of the select policy name. List of all DiffServ classes currently defined as members of the selected Policy Name. Choose one member class name at a time to display its statistics. If no class is associated with the chosen policy then nothing will be populated in the list.
Offered Octets	Displays the count of the packets/octets offered to the class instance before the defined DiffServ treatment is applied.
Discarded Octets	Displays the count of the packets/octets discarded for the class instance for any reason due to DiffServ treatment of the traffic class.
Refresh	Click Refresh to update the screen.

3.7.3 Class of Service

Class of Service

802.1p Priority Mapping

The 802.1p Priority Mapping allows users to assign 802.1p priority and traffic class for each interface. To access this page, click **QoS > Class of Service > Class of Service > 802.1p Priority Mapping**.

802.1p Priority Mapping

Interface

802.1p Priority	Traffic Class
0	<input type="text" value="2"/>
1	<input type="text" value="0"/>
2	<input type="text" value="7"/>
3	<input type="text" value="3"/>
4	<input type="text" value="4"/>
5	<input type="text" value="5"/>
6	<input type="text" value="6"/>
7	<input type="text" value="7"/>

Figure 3-205. QoS > Class of Service > Class of Service > 802.1p Priority Mapping

The following table describes the items in the previous menu.

Table 3-202. QoS > Class of Service > Class of Service > 802.1p Priority Mapping

Parameter	Description
Interface	Click the drop-down menu to select the physical interface for which you want to display or configure data. Select 'All' to set the parameters for all ports to the same values.
802.1p Priority	Displays the 802.1p priority to be mapped.
Traffic Class	Click the drop-down menu to select the internal traffic class to map the corresponding 802.1p priority.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Trust Mode Configuration

The Trust Mode Configuration allows users to assign a trust mode for each interface. To access this page, click **QoS > Class of Service > Trust Mode Configuration**.

CoS Trust Mode Configuration

Interface ge0/1 ▾

Interface Trust Mode trust: nst1p ▾

Current 802.1p Priority Mapping

802.1p Priority	Traffic Class
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Figure 3-206. QoS > Class of Service > Trust Mode Configuration

The following table describes the items in the previous menu.

Table 3-203. QoS > Class of Service > Trust Mode Configuration

Parameter	Description
Interface	Click the drop-down menu to select a CoS configurable interface. The option "Global" represents the most recent global configuration settings. These may be overridden on a per- interface basis.
Interface Trust Mode	Click the drop-down menu to select the policy to trust a particular packet marking at ingress. Interface Trust Mode can only be one of the following: <ul style="list-style-type: none"> • untrusted • trust dot1p • trust ip-dscp <p>NOTE: Default value is trust dot1p.</p>
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Restore Defaults	Click Restore Defaults to restores default settings.
Untrusted Traffic Class	Displays the untrusted traffic class. When 'untrusted' is selected, this displays traffic class (i.e. queue) to which all traffic is directed when in 'untrusted' mode. Valid Range is 0 to 6. For an Untrusted interface, packets are handled in accordance with the user configurable VLAN Priority value of the ingress port.
Non-IP Traffic Class	Displays the non-IP traffic class. When 'trust ip-dscp' is selected, this displays traffic class (i.e. queue) to which all non-IP traffic is directed when in 'trust ip-precedence' or 'trust ip-dscp' mode. Valid Range is 0 to 6.
Current 802.1p Priority Mapping	Displays the current 802.1p priority mapping configuration.

IP DSCP Mapping Configuration

The IP DSCP Mapping Configuration allows users to assign IP DSCP value and traffic class for each interface. To access this page, click **QoS > Class of Service > IP DSCP Mapping Configuration**.

CoS IP DSCP Mapping Configuration

Interface Global ▾

IP DSCP Value	Traffic Class
0	2 ▾
1	2 ▾
2	2 ▾
3	2 ▾
4	2 ▾
5	2 ▾
6	2 ▾
7	2 ▾
8	U ▾
9	0 ▾
10	0 ▾
11	U ▾
12	0 ▾
13	0 ▾
14	U ▾
15	0 ▾
16	1 ▾
17	1 ▾
18	1 ▾
19	1 ▾

Figure 3-207. QoS > Class of Service > IP DSCP Mapping Configuration

The following table describes the items in the previous menu.

Table 3-204. QoS > Class of Service > IP DSCP Mapping Configuration

Parameter	Description
Slot/Port	Click the drop-down menu to select the CoS configurable interfaces. The option "Global" represents the most recent global configuration settings. These may be overridden on a per-interface basis.
Traffic Class	Displays the internal traffic class to map the corresponding IP DSCP value. Valid Range is 0 to 7.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.
Restore Defaults	Click Restore Defaults to restores default settings.

Interface Configuration

The Interface Configuration allows users to assign interface shaping rate for each interface. To access this page, click **QoS > Class of Service > Interface Configuration**.

CoS Interface Configuration

Submit Restore Defaults

Figure 3-208. QoS > Class of Service > Interface Configuration

The following table describes the items in the previous menu.

Table 3-205. QoS > Class of Service > Interface Configuration

Parameter	Description
Interface	Click the drop-down menu to select the CoS configurable interfaces. The option "Global" represents the most recent global configuration settings. These may be overridden on a per-interface basis.
Interface Shaping Rate	Enter a value to set the maximum bandwidth allowed, typically used to shape the outbound transmission rate. This value is controlled independently of any per-queue maximum bandwidth configuration. It is effectively a second-level shaping mechanism. Default value is 0. Valid Range is 0 to 100 in increments of 1. The value 0 means maximum is unlimited.
Restore Defaults	Click Restore Defaults to restores default settings.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Queue Configuration

The Interface Queue Configuration allows users to configure queue settings for each inter-face. To access this page, click **QoS > Class of Service > Interface Queue Configuration**.

CoS Interface Queue Configuration

Submit Restore Defaults for All Queues

Figure 3-209. QoS > Class of Service > Interface Queue Configuration

The following table describes the items in the previous menu.

Table 3-206. QoS > Class of Service > Interface Queue Configuration

Parameter	Description
Interface	Click the drop-down menu to select the CoS configurable interfaces. The option "Global" represents the most recent global configuration settings. These may be overridden on a per-interface basis.
Minimum Bandwidth Allocated	Enter a value to the sum of individual Minimum Bandwidth values for all queues in the interface. The sum cannot exceed the defined maximum of 100. This value is considered while configuring the Minimum Bandwidth for a queue in the selected interface.
Queue ID	Specifies all the available queues per interface (platform based).
Minimum Bandwidth	Specifies the minimum guaranteed bandwidth allotted to this queue. Setting this value higher than its corresponding Maximum Bandwidth automatically increases the maximum to the same value. Default value is 0. Valid Range is 0 to 100 in increments of 1. The value 0 means no guaranteed minimum. Sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum 100.
Maximum Bandwidth	Enter a value to specify the maximum bandwidth allowed for this queue, typically used to shape the outbound transmission rate. This value can be set to 0 without regard to its corresponding Minimum Bandwidth, but cannot otherwise be set less than the Minimum Bandwidth. The value 0 means maximum is unlimited. Default value is 0. Valid Range is 0 to 100 in increments of 1.
Scheduler Type	Click the drop-down menu to set the type of scheduling used for this queue. Scheduler Type can only be one of the following: <ul style="list-style-type: none"> • strict • weighted <p>NOTE: Default value is weighted.</p>
Queue Management Type	Click the drop-down menu to set the queue depth management technique used for queues on this interface. This is only used if device supports independent settings per-queue. Queue Management Type can only be one of the following: <ul style="list-style-type: none"> • taildrop <p>NOTE: Default value is taildrop.</p>
Restore Defaults for All Queues	Click Restore Defaults for All Queues to restore default settings for all queues on the selected interface.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

Interface Queue Status

The Interface Queue Status displays a list the interfaces and the queue summary for each interface. To access this page, click **QoS > Class of Service > Interface Queue Status**.

CoS Interface Queue Status

Interface ge0/1 ▼

Queue ID	Minimum Bandwidth	Scheduler Type	Queue Management Type
0	0	strict	taildrop
-	0	strict	taildrop
2	0	strict	taildrop
3	0	strict	taildrop
4	0	strict	taildrop
5	0	strict	taildrop
6	0	strict	taildrop
7	0	strict	taildrop

Figure 3-210. QoS > Class of Service > Interface Queue Status

The following table describes the items in the previous menu.

Table 3-207. QoS > Class of Service > Interface Queue Status

Parameter	Description
Interface	Click the drop-down menu to select the CoS configurable interfaces. The option "Global" represents the most recent global configuration settings. These may be overridden on a per-interface basis.
Queue ID	Displays the available queues per interface (platform based).
Minimum Bandwidth	Displays the minimum guaranteed bandwidth allotted to this queue. The value 0 means no guaranteed minimum. Sum of individual Minimum Bandwidth values for all queues in the selected interface cannot exceed defined maximum of 100.
Maximum Bandwidth	Displays the maximum bandwidth allowed for this queue, typically used to shape the outbound transmission rate. The value 0 means maximum is unlimited.
Scheduler Type	Displays the type of scheduling used for this queue. Scheduler Type can only be one of the following: <ul style="list-style-type: none"> ● strict ● weighted
Queue Management Type	Displays the queue depth management technique used for queues on this interface. This is only used if device supports independent settings per-queue. Queue Management type available: taildrop.

Protocol CoS Queue Forwarding

The Protocol CoS Queue Forwarding page allows users to force protocol BPDUs forwarding on specific CoS Queue. To access this page, click **QoS > Class of Service > Protocol CoS Queue Forwarding**.

Protocol CoS Queue Forwarding

GOOSE

Admin Mode	Disable ▾
Traffic Class	0 ▾

Submit

Figure 3-211. QoS > Class of Service > Protocol CoS Queue Forwarding

The following table describes the items in the previous menu.

Table 3-208. QoS > Class of Service > Protocol CoS Queue Forwarding

Parameter	Description
Admin Mode	Click the drop-down menu to select the force forwarding administration state. You must select enable if you want force forwarding protocol BPDUs to specific Traffic Class. The factory default is Disable.
Traffic Class	Enter a value to set the force forwarding protocol BPDUs. Valid Range: 0 to 7.
Submit	Click Submit to update the configuration to the switch. Configuration changes take effect immediately. These changes will not be retained across a power cycle unless a save is performed.

3.8. Maintenance

3.8.1 System Resources

The System Resources page displays memory usage and total CPU Utilization. To access this page, click **Maintenance > System Resources**.

System Resources

Memory Usage

Free Memory (kbytes)	96096
In-Use Memory (kbytes)	156616

CPU Usage

Total CPU Utilization	21.3%
-----------------------	-------

Refresh

Figure 3-212. Maintenance > System Resources

The following table describes the items in the previous menu.

Table 3-209. Maintenance > System Resources

Parameter	Description
Free Memory	Displays the available Free Memory on system in kilobytes.
In-Use Memory	Displays the allocated Memory for the system in kilobytes.
Total CPU Utilization	Displays the total CPU Utilization in terms of Percentage.
Refresh	Click Refresh to update the data on the screen with the present state of the data in the switch.

3.8.2 Config Save

The Config Save page allows users to save all the changes that were made to the configuration panels. To access this page, click **Maintenance > Config Save**.

Save All Applied Changes

Saving all applied changes will cause all changes to configuration panels that were applied, but not saved, to be saved, thus retaining their new values across a system reboot.

Save

Figure 3-213. Maintenance > Config Save

The following table describes the items in the previous menu.

Table 3-210. Maintenance > Config Save

Parameter	Description
Save	Click Save to have configuration changes you have made to be saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

3.8.3 Factory Defaults

The Factory Defaults page allows users to reset all configuration parameters to the default values. To access this page, click **Maintenance > Factory Defaults**.

Reset Configuration To Defaults

Exercising this function will cause all configuration parameters to be reset to their default values.

Reset

Figure 3-214. Maintenance > Factory Defaults

The following table describes the items in the previous menu.

Table 3-211. Maintenance > Factory Defaults

Parameter	Description
Reset	Click Reset to have all configuration parameters reset to their factory default values. All changes that have been made will be lost, even if you have issued a save. You will be shown a confirmation screen after you select the button.

3.8.4 Download

The Download page allows users to download a file to the switch. To access this page, click **Maintenance > Download**.

Download File To Switch

Figure 3-215. Maintenance > Download

The following table describes the items in the previous menu.

Table 3-212. Maintenance > Download

Parameter	Description
File Type	Click the drop-down menu to select the type of file you want to download: <ul style="list-style-type: none"> Startup Configuration - Text based startup configuration file. Script - Text based configuration script file. Firmware - Specify image file when you want to upgrade the operational flash. NOTE: To download SSH key files, SSH must be administratively disabled and there can be no active SSH sessions.
Transfer Mode	Click the drop-down menu to select the protocol to use to transfer the file. <ul style="list-style-type: none"> TFTP - Trivial File Transfer Protocol SFTP - Secure File Transfer Program SCP - Secure Copy USB - Universal Serial Bus
Server Address Type	Enter the IPv4 address to indicate the format of the TFTP/SFTP/SCP Server Address field.

Table 3-212. Maintenance > Download (Continued)

Parameter	Description
Server Address	Enter the IP address of the server in accordance with the format indicated by the Server Address Type. The factory default is the IPv4 address 0.0.0.0. The switch remembers the last server address used.
Transfer File Path	Enter the path on the server where the selected file is located. You may enter up to 160 characters. The factory default is blank. The switch remembers the last file path used.
Transfer File Name	Enter the name of the file you want to download from the TFTP/SFTP/SCP/USB server. You may enter up to 31 characters. The factory default is blank. The switch remembers the last file name used.
User Name	Enter the username for remote login to SFTP/SCP server where the file resides. This field is visible only when SFTP or SCP transfer modes are selected.
Password	Enter the password for remote login to SFTP/SCP server where the file resides. This field is visible only when SFTP or SCP transfer modes are selected.
Start File Transfer	Click Start File Transfer to initiate the download, check this box before pressing the Submit button.
File Transfer Status	Click File Transfer Status to the last row of the table is used to display information about the progress of the file transfer.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

3.8.5 Upload

The Upload page allows users to upload a file from the switch. To access this page, click **Maintenance > Upload**.

Upload File From Switch

File Type	Startup Configuration ▾
Transfer Mode	TFTP ▾
Server Address Type	IPv4 ▾
Server Address	0.0.0.0
Transfer File Path	<input type="text"/>
Transfer File Name	<input type="text"/>
Start File Transfer	<input type="checkbox"/>
File Transfer Status	

Submit

Figure 3-216. Maintenance > Upload

The following table describes the items in the previous menu.

Table 3-213. Maintenance > Upload

Parameter	Description
File Type	Click the drop-down menu to select the type of file you want to upload: <ul style="list-style-type: none"> ● Startup Configuration - Specify Text based configuration when you want to retrieve the startup script file. ● Syslog - Specify syslog to retrieve the system log records. ● Trap Log - Specify trap log to retrieve the system trap records. ● Script - Specify Text based configuration when you want to retrieve the script file. ● Mib File - Specify mib file (.zip) to retrieve the mib data of system.
Transfer Mode	Click the drop-down menu to select the protocol to use to transfer the file. <ul style="list-style-type: none"> ● TFTP - Trivial File Transfer Protocol ● SFTP - Secure File Transfer Program ● SCP - Secure Copy ● USB - Universal Serial Bus
Server Address Type	Click the drop-down menu to select either IPv4 or IPv6 or DNS to indicate the format of the Server Address field. The factory default is IPv4.
Server Address	Enter the IP address of the server in accordance with the format indicated by the Server Address Type. The factory default is the IPv4 address 0.0.0.0. The switch remembers the last server address used.
Transfer File Path	Enter the path on the server where the selected file has to be located. You may enter up to 32 characters. The factory default is blank. The switch remembers the last file path used.
Transfer File Name	Enter the name of the file you want to upload from the switch to the server. You may enter up to 31 characters. The factory default is blank. The switch remembers the last file name used.
User Name	Enter the username for remote login to SFTP/SCP server where the file resides. This field is visible only when SFTP or SCP transfer modes are selected.
Password	Enter the password for remote login to SFTP/SCP server where the file resides. This field is visible only when SFTP or SCP transfer modes are selected.
Start File Transfer	Click Start File Transfer to initiate the upload, check this box before pressing the Submit button.
File Transfer Status	Click File Transfer Status to display information about the progress of the file transfer.
Submit	Click Submit to update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

3.8.6 System Reset

The System Reset will cause all operations to stop, sessions to be aborted, reboot the switch, and require the user to log in again. Any unsaved changes will be lost. To access this page, click **Maintenance > System Reset**.

System Reset

Resetting the switch will cause all operations of this switch to stop. This session will be broken and you will have to log in again after the switch has rebooted. Any unsaved changes will be lost.

Figure 3-217. Maintenance > System Reset

The following table describes the items in the previous menu.

Table 3-214. Maintenance > System Reset

Parameter	Description
Reset	Click Reset to select this button to reboot the switch. Any configuration changes you have made since the last time you issued a save will be lost. You will be shown a confirmation screen after you select the button.

3.8.7 Network Diagnostics

Ping

The Ping page allows users to tell the switch to send a Ping request to a specified IP address, and to check whether the switch can communicate with a particular IP station. To access this page, click **Maintenance > Network Diagnostics > Ping**.

Ping

Host Name/IP Address	<input type="text"/>	(Max 255 characters/X.X.X.X)
Count	<input type="text" value="1"/>	(1 to 15)
Interval	<input type="text" value="0"/>	(1 to 60)
Size	<input type="text" value="0"/>	(0 to 65507)
Ping	<input type="text"/>	

Figure 3-218. Maintenance > Network Diagnostics > Ping

The following table describes the items in the previous menu.

Table 3-215. Maintenance > Network Diagnostics > Ping

Parameter	Description
Host Name/IP Address	Enter the IP Address or Host Name of the station you want the switch to ping. The initial value is blank. The IP Address or Host Name you enter is not retained across a power cycle. Hostnames are composed of series of labels concatenated with dots. Each label must be between 1 and 63 characters long, and the entire host-name has a maximum of 255 characters.
Count	Enter the number of echo requests you want to send. The default value is 1. The value ranges from 1 to 15. The Count you enter is not retained across a power cycle.
Interval	Enter the Interval between ping packets in seconds. The default value is 3. The value ranges from 1 to 60. The Interval you enter is not retained across a power cycle.
Size	Enter the Size of ping packet. The default value is 0. The value ranges from 0 to 65507. The Size you enter is not retained across a power cycle.
Ping	Click This screen displays the reply format of ping. If a reply to the ping is not received, you will see <ul style="list-style-type: none"> • Tx = Count, Rx = 0 Min/Max/Avg RTT = 0/0/0 msec, otherwise you will see • Received response for Seq Num 0 Rtt xyz usec • Received response for Seq Num 1 Rtt abc usec • Received response for Seq Num 2 Rtt def usec • Tx = Count, Rx = Count Min/Max/Avg RTT = xyz/abc/def msec.
Submit	Update the switch with the values on the screen. If you want the switch to retain the new values across a power cycle you must perform a save.

TraceRoute

The TraceRoute page allows users to determine the layer 3 path to a specific IP address or hostname. To access this page, click **Maintenance > Network Diagnostics > TraceRoute**.

TraceRoute

Hostname / IP Address	<input type="text"/>	(Max: 255 characters/x.x.x.x)
Probes Per Hop	<input type="text" value="3"/>	(1 to 10)
MaxTTL	<input type="text" value="30"/>	(1 to 255)
InitTTL	<input type="text" value="1"/>	(0 to 255)
MaxFail	<input type="text" value="5"/>	(0 to 255)
Interval(secs)	<input type="text" value="3"/>	(1 to 60)
Port	<input type="text" value="33434"/>	(1 to 65535)
Size	<input type="text" value="0"/>	(0 to 65507)
TraceRoute	<input type="text"/>	
<input type="button" value="Submit"/>		

Figure 3-219. Maintenance > Network Diagnostics > TraceRoute

The following table describes the items in the previous menu.

Table 3-216. Maintenance > Network Diagnostics > TraceRoute

Parameter	Description
Hostname/IP Address	Enter the name of the target host or its IP address. Hostnames are a series of labels separated by with periods. Each label must be between 1 and 63 characters long. The entire hostname must be no more than 255 characters.
Probes Per Hop	Enter the range to specify the number of probes. Traceroute works by sending UDP packets with increasing Time-To-Live (TTL) values. You can specify here the number of probes sent with each TTL. The default value is 3. The range is from 1 to 10.
MaxTTL	Enter the maximum Time-To-Live (TTL). The traceroute terminates after sending probes that can be layer 3 forwarded this number of times. If the destination is further away, the traceroute will not reach it. The default value is 30. The value ranges from 1 to 255.
InitTTL	Enter the initial Time-To-Live (TTL). This value controls the maximum number of layer 3 hops that the first set of probes may travel. The default value is 1. The value ranges from 0 to 255.
MaxFail	Enter the number of consecutive failures that terminate the traceroute. If the switch fails to receive a response for this number of consecutive probes, the traceroute terminates. The default value is 5. The value ranges from 0 to 255.
Interval	Enter the time between probes in seconds. The default value is 3. The value ranges from 1 to 60.
Port	Enter the UDP destination port number to be used in probe packets. The port number should be a port that the target host is not listening on, so that when the probe reaches the destination, it responds with an ICMP Port Unreachable message. The default value is 33434. The value ranges from 1 to 65535.
Size	Enter the size of probe payload in bytes. The default value is 0. The value ranges from 0 to 65507.

Table 3-216. Maintenance > Network Diagnostics > TraceRoute (Continued)

Parameter	Description
TraceRoute	<p>Displays the results in this format:</p> <pre> 1 10.20.24.1 0 ms 0 ms 0 ms 2 266.20.17.9 10 ms 0 ms 10 ms 3 366.20.246.82 10 ms 20 ms 10 ms 4 129.20.4.4 20 ms 10 ms 40 ms 5 129.20.3.55 80 ms 80 ms 90 ms 6 129.20.5.246 80 ms 80 ms 80 ms 7 198.20.90.26 70 ms 70 ms 70 ms 8 216.20.255.105 90 ms 70 ms 80 ms 9 63.20.216.155 80 ms 80 ms 90 ms Hop Count = 9 Last TTL = 9 Test attempt = 27 Test Success = 27 </pre> <p>For each TTL value probed, the results show the IP address of the router that responded to the probes and the response time for each probe. If no response is received for probes with a particular TTL, the IP address is reported as 0.0.0.0. An error code may be printed with the response time for each probe. The error codes signify that either no response was received or an ICMP Destination Unreachable message was received with error codes as follows:</p> <ul style="list-style-type: none"> * no response was received to the probe 4. P - Protocol unreachable (RFC 792) 5. N - Network unreachable (RFC 792) 6. H - Host unreachable (RFC 792) 7. F - Fragmentation needed and DF set (RFC 792) 8. S - Source route failed (RFC 792) 9. A - Communication with Destination Network is Administratively Prohibited (RFC 1122) 10.C - Communication with Destination Host is Administratively Prohibited (RFC 1122) <p>Hop Count is the number of sets of probes sent, each set of probes having a particular TTL. Last TTL is the TTL sent in the final set of probes. Test Attempt is the number of probes sent. Test Success is the number of probes that received a response.</p>
Submit	Click Submit to start the traceroute.

Cable Test

The Cable Test page allows users to check cable status and function for each interface. To access this page, click **Maintenance > Network Diagnostics > Cable Test**.

Port Cable Test

The screenshot shows a web interface for testing a cable. At the top, there is a label 'Interface' followed by a dropdown menu currently showing 'ge0/1'. Below this, centered, is a button labeled 'Test Cable'.

Figure 3-220. Maintenance > Network Diagnostics > Cable Test

The following table describes the items in the previous menu.

Table 3-217. Maintenance > Network Diagnostics > Cable Test

Parameter	Description
Interface	Click the drop-down menu to select the interface. This field indicates the interface to which the cable to be tested is connected.
Cable Test Results	
Cable Status	<p>Displays the cable status as Normal, Open or Short.</p> <ul style="list-style-type: none"> • 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. <p>This field is displayed after the "Test Cable" button has been clicked and results are available.</p> <p>This field is not visible when the page is initially displayed.</p>
Cable Length	<p>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. The Cable Length is only displayed if the cable status is Normal. This field is displayed after the "Test Cable" button has been clicked and results are available.</p> <p>This field is not visible when the page is initially displayed.</p>
Failure Location Distance	<p>Displays 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. This field is displayed after the "Test Cable" button has been clicked and results are available. This field is not visible when the page is initially displayed.</p>
Test Cable	<p>Click Test Cable to perform a cable test on the selected interface. The cable test may take up to 2 seconds to complete. If the port has an active link then the link is not taken down and the cable status is always "Normal". 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 be "Open" or "Short" because some Ethernet adapters leave unused wire pairs unterminated or grounded.</p>

Troubleshooting

Chapter 4

Troubleshooting

Verify that is using the right power cord/adaptor (DC 24-48V), please don't use the power adapter with DC output higher than 48V, or it may damage this device.

Select the proper UTP/STP cable to construct the user network. Use unshielded twisted-pair (UTP) or shield twisted-pair (STP) cable for RJ-45 connections that depend on the connector type the switch equipped: 100R Category 3, 4 or 5 cable for 10Mbps connections, 100R Category 5 cable for 100Mbps connections, or 100R Category 5e/ above cable for 1000Mbps connections. Also be sure that the length of any twisted-pair connection does not exceed 100 meters (328 feet).

R = replacement letter for Ohm symbol.

Diagnosing LED Indicators: To assist in identifying problems, the switch can be easily monitored through panel indicators, which describe common problems the user may encounter and where the user can find possible solutions.

If the power indicator does not light on when the power cord is plugged in, you may have a problem with power cord. Then check for loose power connections, power losses or surges at power outlet. If you still cannot resolve the problem, contact the local dealer for assistance.

If the LED indicators are normal and the connected cables are correct but the packets still cannot be transmitted. Please check the user system's Ethernet devices' configuration or status.