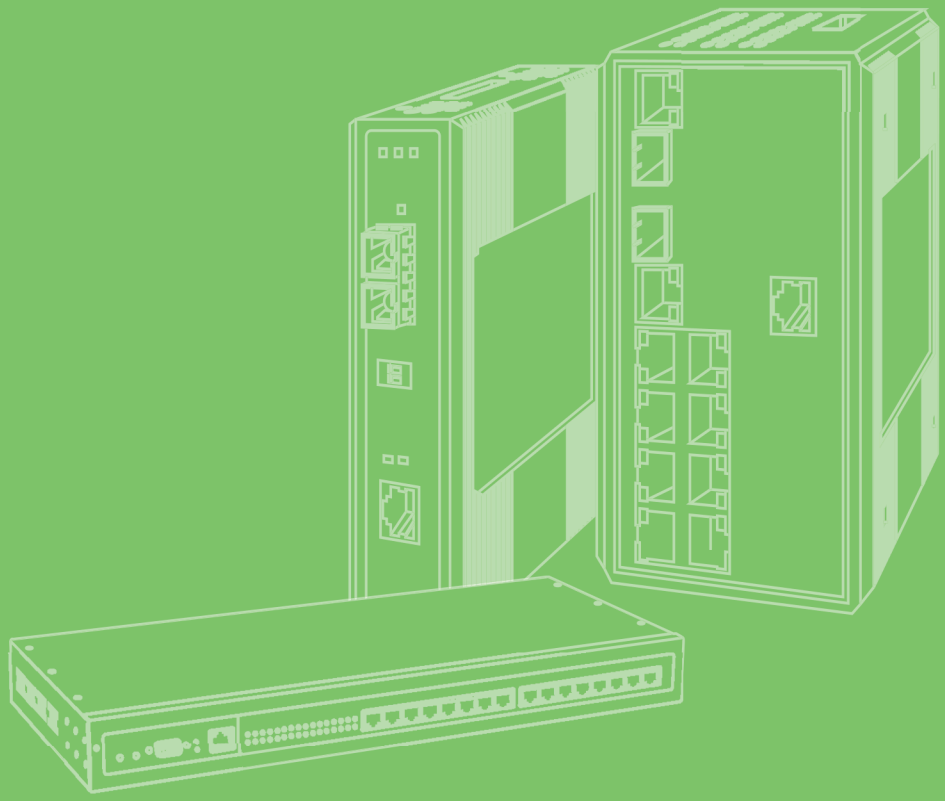
User Manual



Advantech NOS 5.2 SW User Manual for Layer 3 switches

Models covered by this User Manual:

EKI-87xx Series Managed Ethernet 10G L3 Switch

EKI-95xx-Rxxxxxx Series Managed Ethernet L3 Switch

*Please refer to Chapter 1 for specific supported models.

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2026 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. Information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties, which may result from its use.

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (5 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for five 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 ofwarranty 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:

1. 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.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. 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.
4. 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.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Edition 1

Printed in Taiwan September 2026

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

Note: 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.

Technical Support and Assistance

1. Visit the Advantech web site at www.advantech.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Warnings indicate conditions, which if not observed, can cause personal injury!*



Caution! *Cautions are included to help you avoid damaging hardware or losing data. e.g.*



There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note! *Notes provide optional additional information.*



Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: support@advantech.com

Safety Instructions

1. Read these safety instructions carefully.
2. Keep this User Manual for later reference.
3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
5. Keep this equipment away from humidity.
6. Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
7. The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
9. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
12. Never pour any liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If one of the following situations arises, get the equipment checked by service personnel:
15. The power cord or plug is damaged.
16. Liquid has penetrated into the equipment.
17. The equipment has been exposed to moisture.
18. The equipment does not work well, or you cannot get it to work according to the user's manual.
19. The equipment has been dropped and damaged.
20. The equipment has obvious signs of breakage.
21. DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO -40°C (-40°F) ~ 85°C (185°F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.
22. CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER, DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.
23. The sound pressure level at the operator's position according to IEC 704-1:1982 is no more than 70 dB (A).

DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Wichtige Sicherheishinweise

1. Bitte lesen sie Sich diese Hinweise sorgfältig durch.
2. Heben Sie diese Anleitung für den späteren Gebrauch auf.
3. Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie Keine Flüssig-oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
4. Die NetzanschluBsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
5. Das Gerät ist vor Feuchtigkeit zu schützen.
6. Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen.
7. Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor überhitzung schützt. Sorgen Sie dafür, daB diese Öffnungen nicht abgedeckt werden.
8. Beachten Sie beim. AnschluB an das Stromnetz die AnschluBwerte.
9. Verlegen Sie die NetzanschluBleitung so, daB niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
10. Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
11. Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
12. Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
13. Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
14. Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
15. Netzkabel oder Netzstecker sind beschädigt.
16. Flüssigkeit ist in das Gerät eingedrungen.
17. Das Gerät war Feuchtigkeit ausgesetzt.
18. Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
19. Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
20. Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.
21. VOSICHT: Explisionsgefahr bei unsachgemaben Austausch der Batterie.Ersatz nur durch densellben order einem vom Hersteller empfohlene-mahnlichen Typ. Entsorgung gebrauchter Batterien navh Angaben des Herstellers.
22. ACHTUNG: Es besteht die Explosionsgefahr, falls die Batterie auf nicht fachmännische Weise gewechselt wird. Verfangen Sie die Batterie nur gleicher oder entsprechender Type, wie vom Hersteller empfohlen. Entsorgen Sie Batterien nach Anweisung des Herstellers.
23. Der arbeitsplatzbezogene Schalldruckpegel nach DIN 45 635 Teil 1000 beträgt 70dB(A) oder weiger.

Haftungsausschluss: Die Bedienungsanleitungen wurden entsprechend der IEC-704-1 erstellt. Advantech lehnt jegliche Verantwortung für die Richtigkeit der in diesem Zusammenhang getätigten Aussagen ab.

Safety Precaution - Static Electricity

Static electricity can cause bodily harm or damage electronic devices. To avoid damage, keep static-sensitive devices in the static-protective packaging until the installation period. The following guidelines are also recommended:

- Wear a grounded wrist or ankle strap and use gloves to prevent direct contact to the device before servicing the device. Avoid nylon gloves or work clothes, which tend to build up a charge.
- Always disconnect the power from the device before servicing it.
- Before plugging a cable into any port, discharge the voltage stored on the cable by touching the electrical contacts to the ground surface.

Contents

Chapter 1 Introduction 1

Chapter 2 Configuration Utility 3

2.1 First Time Setup 4
2.1.1 Overview 4
2.1.2 Introduction 4
2.1.3 Administrative Interface Access 4
2.1.4 Using the Graphical (Web) Interface 5
2.1.5 Configuring the Switch for Network Access 5
2.1.6 Configuring the Ethernet Ports 6
2.2 Command Line Interface Configuration 7
2.2.1 Introduction to Command-Line Interface (CLI) 7
2.2.2 Accessing the CLI 7
2.3 Web Browser Configuration 8
2.3.1 Preparing for Web Configuration 8
2.3.2 System Login 8

Chapter 3 Managing Switch 9

3.1 Log In 10
3.2 Recommended Practices 10
3.3 Monitoring 10
3.3.1 Device Information 10
3.3.2 Logging Message 12
3.3.3 Port Monitoring 13
3.3.4 Link Aggregation 16
3.3.5 LLDP Statistics 16
3.3.6 IGMP Statistics 17
3.3.7 MLD Statistics 18
3.4 System 19
3.4.1 IP Settings 19
3.4.2 IPv6 Settings 20
3.4.3 System Time 21
3.4.4 Network Port 23
3.5 L2 Switching 23
3.5.1 Port Configuration 23
3.5.2 Port Mirror 25
3.5.3 Link Aggregation 26
3.5.4 802.1Q VLAN 30
3.5.5 802.3az EEE 36
3.5.6 Multicast 36
3.5.7 Jumbo Frame 46
3.5.8 Spanning Tree 47
3.5.9 X-Ring Pro 53
3.5.10 Loopback Detection 55
3.6 L3 Routing 57
3.6.1 NAT 57
3.6.2 Static Route 59
3.7 MAC Address Table 60
3.7.1 Static MAC 60
3.7.2 MAC Aging Time 61

3.7.3 Dynamic Forwarding Table 62
3.8 Security 63
3.8.1 Storm Control 63
3.8.2 Port Security 65
3.8.3 Protected Ports 66
3.8.4 DoS Prevention 66
3.8.5 Applications 70
3.8.6 802.1x 73
3.8.7 IP Security 75
3.8.8 Security login 76
3.8.9 Access Control List 79
3.8.10 IP Source Guard 82
3.8.11 ARP Spoofing 83
3.9 QoS 84
3.9.1 General 84
3.9.2 Qos Basic Mode 94
3.9.3 Rate Limit 96
3.10 Management 99
3.10.1 LLDP 99
3.10.2 SNMP 105
3.10.3 Power of Ethernet 108
3.10.4 TCP Modbus 112
3.10.5 DHCP Server 113
3.10.6 SMTP Client 120
3.10.7 NTP Server 123
3.10.8 Goose 124
3.10.9 DNS Server 126
3.11 Diagnostics 127
3.11.1 Cable Diagnostic 127
3.11.2 Ping Test 128
3.11.3 IPv6 Ping Test 129
3.11.4 System Log 131
3.11.5 DDM 133
3.11.6 LED Indication 135
3.11.7 Self Monitoring 136
3.12 Tools 138
3.12.1 Backup Manager 138
3.12.2 Upgrade Manager 139
3.12.3 Dual Image 140
3.12.4 Save Configuration 141
3.12.5 User Account 141
3.12.6 USB 145
3.12.7 N-Key 146
3.12.8 Reset System 147
3.12.9 Reboot Device 147
3.12.10 System Use Notice 147

List of Figures

Figure 3.1 Login Screen 10
Figure 3.2 Monitoring > Device Information 11
Figure 3.3 Monitoring > Logging Message 12
Figure 3.4 Monitoring > Logging Information 12
Figure 3.5 Monitoring > Logging Message 13
Figure 3.6 Monitoring > Port Monitoring > Port Statistics 13
Figure 3.7 Monitoring > Port Monitoring > IF MIB Counters 14
Figure 3.8 Monitoring > Port Monitoring > Ether-Like MIB Counters 14
Figure 3.9 Monitoring > Port Monitoring > Rmon MIB Counters 15
Figure 3.10 Monitoring > Port Monitoring > Port Utilization 15
Figure 3.11 Monitoring > Port Monitoring > TX 16
Figure 3.12 Monitoring > Port Monitoring > RX 16
Figure 3.13 Monitoring > Link Aggregation 16
Figure 3.14 Monitoring > LACP Information 16
Figure 3.15 Monitoring > LLDP Statistics 17
Figure 3.16 Monitoring > LLDP Port Statistics 17
Figure 3.17 Monitoring > IGMP Statistics 18
Figure 3.18 Monitoring > MLD Statistics 19
Figure 3.19 System > IP Settings 19
Figure 3.20 System > IP Address Information 20
Figure 3.21 System > IPv6 Settings 20
Figure 3.22 System > IPv6 Information 21
Figure 3.23 System > System Time 21
Figure 3.24 System > System Time Information 22
Figure 3.25 System > Network Port 23
Figure 3.26 System > Network Port Information 23
Figure 3.27 L2 Switching > Port Configuration 24
Figure 3.28 L2 Switching > Port Name Settings 24
Figure 3.29 L2 Switching > Port Status 25
Figure 3.30 L2 Switching > Port Configuration > Edit description of GE1 25
Figure 3.31 L2 Switching > Port Mirror 26
Figure 3.32 L2 Switching > Mirror Status 26
Figure 3.33 L2 Switching > Link Aggregation > Load Balance 27
Figure 3.34 L2 Switching > Link Aggregation > Load Balance Information 27
Figure 3.35 L2 Switching > Link Aggregation > LAG Management 27
Figure 3.36 L2 Switching > Link Aggregation > LAG Management Information 28
Figure 3.37 L2 Switching > Link Aggregation > LAG Port Settings 28
Figure 3.38 L2 Switching > Link Aggregation > LAG Port Status 29
Figure 3.39 L2 Switching > Link Aggregation > LACP Priority Settings 29
Figure 3.40 L2 Switching > Link Aggregation > LACP Priority Information 29
Figure 3.41 L2 Switching > Link Aggregation > LACP Port Settings 30
Figure 3.42 L2 Switching > Link Aggregation > LACP Port Information 30
Figure 3.43 L2 Switching > 802.1Q VLAN > VLAN Management 31
Figure 3.44 L2 Switching > 802.1Q VLAN > VLAN Table 31
Figure 3.45 L2 Switching > 802.1Q VLAN > VLAN Management > Edit VLAN Name of VLAN ID 1 31
Figure 3.46 L2 Switching > 802.1Q VLAN > PVID Settings 32
Figure 3.47 L2 Switching > 802.1Q VLAN > Port VLAN Status 33
Figure 3.48 L2 Switching > 802.1Q VLAN > Port to VLAN 34
Figure 3.49 L2 Switching > 802.1Q VLAN > Port-VLAN Mapping 35
Figure 3.50 L2 Switching > 802.1Q VLAN > VLAN Interface Management 35
Figure 3.51 L2 Switching > 802.1Q VLAN > VLAN Interface Status 36
Figure 3.52 L2 Switching > 802.3az EEE 36
Figure 3.53 L2 Switching > EEE Port Status 36
Figure 3.54 L2 Switching > Multicast > Unknown Multicast > Multicast Filtering 37
Figure 3.55 L2 Switching > Multicast > Unknown Multicast > Properties Information 37

Figure 3.56 L2 Switching > Multicast > Unknown Multicast > Flood Settings 37
Figure 3.57 L2 Switching > Multicast > Unknown Multicast > Flood Action Information 38
Figure 3.58 L2 Switching > Multicast > Unknown Multicast > Router-Port Settings 38
Figure 3.59 L2 Switching > Multicast > Unknown Multicast > Router-Port Information 38
Figure 3.60 L2 Switching > Multicast > IGMP Snooping > IGMP Settings 39
Figure 3.61 L2 Switching > Multicast > IGMP Snooping > IGMP Snooping Information 39
Figure 3.62 L2 Switching > Multicast > IGMP Snooping > IGMP Snooping Table 39
Figure 3.63 L2 Switching > Multicast > IGMP Snooping > IGMP Settings > Edit IGMP Snooping . 40
Figure 3.64 L2 Switching > Multicast > IGMP Snooping > IGMP Querier 40
Figure 3.65 L2 Switching > Multicast > IGMP Snooping > IGMP Querier Status 41
Figure 3.66 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups 41
Figure 3.67 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups Status 41
Figure 3.68 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups > Static Group Port Setting 42
Figure 3.69 L2 Switching > Multicast > IGMP Snooping > Multicast Groups 42
Figure 3.70 L2 Switching > Multicast > IGMP Snooping > Router Ports 42
Figure 3.71 L2 Switching > Multicast > MLD Snooping > MLD Settings 42
Figure 3.72 L2 Switching > Multicast > MLD Snooping > MLD Snooping Information 43
Figure 3.73 L2 Switching > Multicast > MLD Snooping > MLD Snooping Table 43
Figure 3.74 L2 Switching > Multicast > MLD Snooping > MLD Settings > Edit MLD Snooping 44
Figure 3.75 L2 Switching > Multicast > MLD Snooping > MLD Querier 44
Figure 3.76 L2 Switching > Multicast > MLD Snooping > MLD Querier Status 45
Figure 3.77 L2 Switching > Multicast > MLD Snooping > MLD Static Groups 45
Figure 3.78 L2 Switching > Multicast > MLD Snooping > MLD Static Groups Status 45
Figure 3.79 L2 Switching > Multicast > MLD Snooping > MLD Static Groups > Static Group Port Setting 46
Figure 3.80 L2 Switching > Multicast > MLD Snooping > Multicast Groups 46
Figure 3.81 L2 Switching > Multicast > MLD Snooping > Router Ports 46
Figure 3.82 L2 Switching > Jumbo Frame 46
Figure 3.83 L2 Switching > Jumbo Frame Config 47
Figure 3.84 L2 Switching > Spanning Tree > Global Settings 47
Figure 3.85 L2 Switching > Spanning Tree > Timing Settings 48
Figure 3.86 L2 Switching > Spanning Tree > STP Information 48
Figure 3.87 L2 Switching > Spanning Tree > Port Settings 48
Figure 3.88 L2 Switching > Spanning Tree > STP Port Status 49
Figure 3.89 L2 Switching > Spanning Tree > Bridge Settings 50
Figure 3.90 L2 Switching > Spanning Tree > Bridge Status 50
Figure 3.91 L2 Switching > Spanning Tree > Advanced Port Settings 50
Figure 3.92 L2 Switching > Spanning Tree > STP Port Status 51
Figure 3.93 L2 Switching > Spanning Tree > MST Config Identification 52
Figure 3.94 L2 Switching > Spanning Tree > MST Configuration Identification Information 52
Figure 3.95 L2 Switching > Spanning Tree > MST Instance Settings 52
Figure 3.96 L2 Switching > Spanning Tree > MSTI ID Information 53
Figure 3.97 L2 Switching > Spanning Tree > STP Statistics 53
Figure 3.98 L2 Switching > X-Ring Pro > X-Ring Pro Settings 54
Figure 3.99 L2 Switching > X-Ring Pro > Information 54
Figure 3.100 L2 Switching > X-Ring Pro > X-Ring Pro Groups 54
Figure 3.101 L2 Switching > X-Ring Pro > Ring Information 55
Figure 3.102 L2 Switching > Loopback Detection > Global Settings 55
Figure 3.103 L2 Switching > Loopback Detection > Loopback Detection Global Information 56
Figure 3.104 L2 Switching > Loopback Detection > Port Settings 56
Figure 3.105 L2 Switching > Loopback Detection > Loopback Detection Port Information 57
Figure 3.106 L3 Routing > NAT > SNAT 58
Figure 3.107 L3 Routing > NAT > Entry Information 58
Figure 3.108 L3 Routing > NAT > DNAT 59
Figure 3.109 L3 Routing > NAT > Entry Information 59
Figure 3.110 L3 Routing > Static Route 60
Figure 3.111 L3 Routing > Static Route Config Information 60
Figure 3.112 L3 Routing > Default Route Information 60
Figure 3.113 MAC Address Table > Static MAC 61

Figure 3.114 MAC Address Table > Static MAC Status 61
Figure 3.115 MAC Address Table > MAC Aging Time 61
Figure 3.116 MAC Address Table > Dynamic Address Status 62
Figure 3.117 MAC Address Table > Dynamic Forwarding Table 62
Figure 3.118 MAC Address Table > MAC Address Information 63
Figure 3.119 Security > Storm Control > Global Settings 63
Figure 3.120 Security > Storm Control > Storm Control Global Information 63
Figure 3.121 Security > Storm Control > Port Settings 64
Figure 3.122 Security > Storm Control > Storm Control Port Information 65
Figure 3.123 Security > Port Security 65
Figure 3.124 Security > Port Security Information 66
Figure 3.125 Security > Protected Ports 66
Figure 3.126 Security > Protected Ports Status 66
Figure 3.127 Security > DoS Prevention > DoS Global Settings 67
Figure 3.128 Security > DoS Prevention > DoS Global Information 69
Figure 3.129 Security > DoS Prevention > DoS Port Settings 69
Figure 3.130 Security > DoS Prevention > DoS Port Status 70
Figure 3.131 Security > Applications > TELNET 70
Figure 3.132 Security > Applications > Telnet Information 71
Figure 3.133 Security > Applications > SSH 71
Figure 3.134 Security > Applications > SSH Information 71
Figure 3.135 Security > Applications > HTTP 72
Figure 3.136 Security > Applications > HTTP Information 72
Figure 3.137 Security > Applications > HTTPS 72
Figure 3.138 Security > Applications > HTTPS Information 73
Figure 3.139 Security > 802.1x > 802.1x Global Settings 73
Figure 3.140 Security > 802.1x > 802.1x Information 74
Figure 3.141 Security > 802.1x > 802.1x Port Configuration 74
Figure 3.142 Security > 802.1x > 802.1x Port Authorization 75
Figure 3.143 Security > IP Security > Global Settings 75
Figure 3.144 Security > IP Security > IP Security Status 75
Figure 3.145 Security > IP Security > Entry Settings 76
Figure 3.146 Security > IP Security > IP Security Entry Information 76
Figure 3.147 Security > Security login > Security Login Global Settings 76
Figure 3.148 Security > Security login > RADIUS Settings 77
Figure 3.149 Security > Security login > TACACS Settings 77
Figure 3.150 Security > Security login > Security Login Global Information 78
Figure 3.151 Security > Security login > Security Login Access Control Settings 78
Figure 3.152 Security > Security login > Security Login type Settings 79
Figure 3.153 Security > Security login > Security Login Access Control Information 79
Figure 3.154 Security > Access Control List > MAC ACL > Entry Settings 80
Figure 3.155 Security > Access Control List > MAC ACL > Entry List 81
Figure 3.156 Security > Access Control List > IP ACL > Entry Settings 81
Figure 3.157 Security > Access Control List > IP ACL > Entry List 82
Figure 3.158 Security > IP Source Guard > Global Settings 82
Figure 3.159 Security > IP Source Guard > Global Information 82
Figure 3.160 Security > IP Source Guard > Entry Settings 83
Figure 3.161 Security > IP Source Guard > Entry Information 83
Figure 3.162 Security > ARP Spoofing 83
Figure 3.163 Security > Entry Information 84
Figure 3.164 QoS > General > QoS Properties 84
Figure 3.165 QoS > General > QoS Global Information 84
Figure 3.166 QoS > General > QoS Settings 85
Figure 3.167 QoS > General > QoS Status 86
Figure 3.168 QoS > General > QoS Scheduling 87
Figure 3.169 QoS > General > Queue Information 87
Figure 3.170 QoS > General > CoS Mapping 88
Figure 3.171 QoS > General > CoS Mapping Information 89
Figure 3.172 QoS > General > Queue Mapping Information 89
Figure 3.173 QoS > General > DSCP Mapping 90

Figure 3.174 QoS > General > DSCP Mapping Information (DSCP 0–31) 91
Figure 3.174 QoS > General > DSCP Mapping Information (DSCP 32–63) 92
Figure 3.175 QoS > General > Queue Mapping Information 93
Figure 3.176 QoS > General > IP Precedence Mapping 93
Figure 3.177 QoS > General > IP Precedence Mapping Information 94
Figure 3.178 QoS > General > Queue Mapping Information 94
Figure 3.179 QoS > Qos Basic Mode > Global Settings 95
Figure 3.180 QoS > Qos Basic Mode > Basic Mode Global Information 95
Figure 3.181 QoS > Qos Basic Mode > Port Settings 95
Figure 3.182 QoS > Qos Basic Mode > Basic Mode Port Information 96
Figure 3.183 QoS > Rate Limit > Ingress Bandwidth Control 96
Figure 3.184 QoS > Rate Limit > Ingress Bandwidth Control Status 97
Figure 3.185 QoS > Rate Limit > Egress Bandwidth Control 97
Figure 3.186 QoS > Rate Limit > Egress Bandwidth Control Status 98
Figure 3.187 QoS > Rate Limit > Egress Queue 98
Figure 3.188 QoS > Rate Limit > Egress Per Queue Status 99
Figure 3.189 Management > LLDP > LLDP System Settings 99
Figure 3.190 Management > LLDP > LLDP Global Config 100
Figure 3.191 Management > LLDP > LLDP Port Settings 100
Figure 3.192 Management > LLDP > Optional TLVs Selection 101
Figure 3.193 Management > LLDP > LLDP Port Status 102
Figure 3.194 Management > LLDP > VLAN Name TLV VLAN Selection 102
Figure 3.195 Management > LLDP > LLDP Port VLAN TLV Status 103
Figure 3.196 Management > LLDP > LLDP Local Device Info 103
Figure 3.197 Management > LLDP > Port Status 104
Figure 3.198 Management > LLDP > LLDP Remote Device Info 104
Figure 3.199 Management > LLDP > LLDP Overloading 105
Figure 3.200 Management > SNMP > SNMP Settings 105
Figure 3.201 Management > SNMP > SNMP Information 106
Figure 3.202 Management > SNMP > SNMP Community 106
Figure 3.203 Management > SNMP > Community Status 106
Figure 3.204 Management > SNMP > SNMPv3 EngineID 107
Figure 3.205 Management > SNMP > SNMPv3 Settings 107
Figure 3.206 Management > SNMP > User Status 107
Figure 3.207 Management > SNMP > SNMP Trap 108
Figure 3.208 Management > SNMP > Trap Host Status 108
Figure 3.209 Management > Power of Ethernet > PoE System Settings 109
Figure 3.210 Management > Power of Ethernet > PoE System Information 109
Figure 3.211 Management > Power of Ethernet > PoE Port Settings 110
Figure 3.212 Management > Power of Ethernet > PoE Port Config Information 110
Figure 3.213 Management > Power of Ethernet > PoE Port Status 110
Figure 3.214 Management > Power of Ethernet > PoE Failure Check 111
Figure 3.215 Management > Power of Ethernet > POE Failure Check Device Setting 111
Figure 3.216 Management > Power of Ethernet > POE Failure Check Entry Table 112
Figure 3.217 Management > Power of Ethernet > PoE Failure Check Status 112
Figure 3.218 Management > TCP Modbus 113
Figure 3.219 Management > TCP Modbus Status 113
Figure 3.220 Management > DHCP Server > Status Settings 113
Figure 3.221 Management > DHCP Server > Status Information 114
Figure 3.222 Management > DHCP Server > Global Settings 114
Figure 3.223 Management > DHCP Server > Global Information 115
Figure 3.224 Management > DHCP Server > Port Settings 115
Figure 3.225 Management > DHCP Server > Port Information 116
Figure 3.226 Management > DHCP Server > VLAN Settings 116
Figure 3.227 Management > DHCP Server > Entry Information 117
Figure 3.228 Management > DHCP Server > Option 82 Settings 118
Figure 3.229 Management > DHCP Server > Entry Information 119
Figure 3.230 Management > DHCP Server > Client MAC Settings 119
Figure 3.231 Management > DHCP Server > Client MAC Information 120
Figure 3.232 Management > DHCP Server > Lease Entry 120

Figure 3.233 Management > SMTP Client > Global Settings 120
Figure 3.234 Management > SMTP Client > SMTP Information 120
Figure 3.235 Management > SMTP Client > Profile Settings 121
Figure 3.236 Management > SMTP Client > Profile Target Mail Settings 121
Figure 3.237 Management > SMTP Client > Profile Information 122
Figure 3.238 Management > SMTP Client > Sending Message 122
Figure 3.239 Management > NTP Server 123
Figure 3.240 Management > NTP Server Status 124
Figure 3.241 Management > Goose > Goose Settings 124
Figure 3.242 Management > Goose > Goose Age Configuration 125
Figure 3.243 Management > Goose > Goose Information 125
Figure 3.244 Management > Goose > Goose Qos Settings 125
Figure 3.245 Management > Goose > Goose Qos Information 126
Figure 3.246 Management > Goose > Goose MAC Table 126
Figure 3.247 Management > Goose > Goose Monitoring Table 126
Figure 3.248 Management > DNS Server > DNS Server Settings 126
Figure 3.249 Management > DNS Server > DNS Server Information 127
Figure 3.250 Management > DNS Server > DNS Server Host Table 127
Figure 3.251 Management > DNS Server > DNS Server Host Table 127
Figure 3.252 Diagnostics > Cable Diagnostic 128
Figure 3.253 Diagnostics > Test Results 128
Figure 3.254 Diagnostics > Ping Test 128
Figure 3.255 Diagnostics > IPv6 Ping Test 130
Figure 3.256 Diagnostics > System Log > Logging Service 131
Figure 3.257 Diagnostics > System Log > Logging Information 131
Figure 3.258 Diagnostics > System Log > Local Logging 131
Figure 3.259 Diagnostics > System Log > Local Logging Setting Status 132
Figure 3.260 Diagnostics > System Log > System Log Server 132
Figure 3.261 Diagnostics > System Log > Remote Logging Setting Status 133
Figure 3.262 Diagnostics > DDM 133
Figure 3.263 Diagnostics > Diagnostic Alarm Information 133
Figure 3.264 Diagnostics > DMI INFO 134
Figure 3.265 Diagnostics > Vendor Info 134
Figure 3.266 Diagnostics > LED Indication 135
Figure 3.267 Diagnostics > LED Information 135
Figure 3.268 Diagnostics > Event Information 135
Figure 3.269 Diagnostics > Event Detail 136
Figure 3.270 Diagnostics > Self Monitoring > Global Settings 136
Figure 3.271 Diagnostics > Self Monitoring > Global Information 136
Figure 3.272 Diagnostics > Self Monitoring > CPU Degrade Settings 136
Figure 3.273 Diagnostics > Self Monitoring > CPU Degrade Information 137
Figure 3.274 Diagnostics > Self Monitoring > System Settings 137
Figure 3.275 Diagnostics > Self Monitoring > System Information 137
Figure 3.276 Diagnostics > Self Monitoring > Port Settings 137
Figure 3.277 Diagnostics > Self Monitoring > Port Information 138
Figure 3.278 Tools > Backup Manager 139
Figure 3.279 Tools > Upgrade Manager 140
Figure 3.280 Tools > Dual Image 140
Figure 3.281 Tools > Images Information 0 141
Figure 3.282 Tools > Images Information 1 141
Figure 3.283 Tools > User Account > User Account 142
Figure 3.284 Tools > User Account > Local Users 142
Figure 3.285 Tools > User Account > Password Change 142
Figure 3.286 Tools > User Account > Local Users 143
Figure 3.287 Tools > User Account > Password Rule 143
Figure 3.288 Tools > User Account > Password Rule Status 144
Figure 3.289 Tools > User Account > Wrong Password 144
Figure 3.290 Tools > User Account > Wrong Password Information 144
Figure 3.291 Tools > User Account > User Name Expired 145
Figure 3.292 Tools > User Account > User Name Expired Information 145

Figure 3.293 Tools > USB 145
Figure 3.294 Tools > USB Information 146
Figure 3.295 Tools > N-Key 146
Figure 3.296 Tools > N-Key Information 146
Figure 3.297 Tools > System Use Notice 147
Figure 3.298 Tools > System Use Notice 148

Chapter 1

Introduction

Thank you for choosing Advantech's Managed Ethernet Switches.

Before starting to use the managed switch, we recommend reading the User Manual. It will help you quickly understand how to configure and manage your managed switch through its intuitive web-based management interface.

Supported Models

This User Manual covers the following models:

- EKI-8712G-4XFI
- EKI-8712G-4XFPI
- EKI-8720G-4XFI
- EKI-8720G-4XFPI
- EKI-8720G-8F4XFI
- EKI-8728G-4XFI
- EKI-9520E/G-RXXXXXX-A Series
- EKI-9516E/G-RXXXXXX-B Series
- EKI-9512E/G-RXXXXXX-B Series
- EKI-9508E/G-RXXXXXX-A Series

* For the EKI-95 series, X may be any alphanumeric character or blank.

Manual Overview

Methods and an introduction to configuring Advantech's managed switches will be presented in the next two chapters. Please refer to the descriptions below for the main functions of each chapter.

Chapter 2: Configuration Utility – Guides you through the basic configuration required when setting up the switch for the first time.

Chapter 3: Managing Switch – Provides detailed instructions for configuring and using the switch's management features.

We hope this User Manual helps you get the most out of your Advantech Managed Ethernet Switch and provides you with a smooth user experience.

Thank you again for choosing Advantech. If you have any questions or need further assistance, please feel free to contact us.

Chapter 2

Configuration Utility

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.

Note! *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 Chrome, Firefox, or Internet Explorer.

Note! *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, only HTTP is enabled. Either or both may be enabled or disabled to secure the switch. HTTPS is configured under **Applications > HTTPS**.

To access the graphical interface, enter a URL like http://192.168.1.1 in your browser's address bar. Replace "192.168.1.1" with your switch's IP address if you've changed it from the factory default. Once HTTPS has been enabled under **Applications > HTTPS**, you can replace "http" with "https" to use secure HTTP; until then only port 80 accepts connections.

The web server in the switch uses a signed security certificate. When HTTPS is enabled and 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.

Note! *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.

To configure the switch for network access, select **System > IP Settings** to reach the IP configuration 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.

Note! *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 the address of a router that connects two different networks. On this L3 switch the default gateway is **not** part of the IP Settings menu — it is configured under **L3 Routing > Static Route**, in the Default Route Information section. No default route is configured at the factory.

- 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 with out 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 autonegotiation 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
- 10000f–10000 Mbps, Full Duplex (SFP only)

On managed switches with gigabit combination ports, those ports with 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. Otherwise, the switch will use the fixed Ethernet port and the corresponding settings for it.

Note! *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. The 10G SFP+ port only supports backward compatibility down to 1 Gbps.*

2.2 Command Line Interface Configuration

2.2.1 Introduction to Command-Line Interface (CLI)

The command-line interface (CLI) is constructed with an eye toward automation of CLI-based configuration. The interaction is modeled on that used in many Internet protocols such as Telnet, FTP, and SMTP. After each command is entered and processed, the switch will issue a reply that consists of a numeric status code and a human-readable explanation of the status.

The general format of commands is:

section parameter [value]

where:

- section is used to group parameters.
- parameter will specify the parameter within the section. For example, the network section will have parameters for DHCP, IP address, subnet mask, and default gateway.
- value is the new value of the parameter. If value is omitted, the current value is displayed.

Please note that new values will not take effect until explicitly committed.

Sections and parameter names are case sensitive (e.g., “Network” is not the same as “network”).

Note! *Any commands in the CLI Commands section of this chapter, with the exception of the global commands, must be prefaced with the name of the section they are in. For example, to change the IP address of the switch, you would type:*

network address <newIP>

2.2.2 Accessing the CLI

To access the CLI interface, establish Ethernet or serial connectivity to the switch.

To connect by Ethernet, open a command prompt window and type:

telnet <switchip> (where <switchip> is the IP address of the switch)

At the login prompt, type “admin” for the username and “admin” for the password. The switch will respond with “Welcome to L3 Management Switch” and present the `Switch#` prompt.

2.3 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].

2.3.1 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: none configured at the factory (see **L3 Routing > Static Route**)
- User name: admin
- Password: admin

2.3.2 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.

Chapter 3

Managing Switch

3.1 Log In

To access the login window, connect the device to the network. Once the switch is installed and connected, power on the switch see the following procedures to log into your switch.

When the switch is first installed, the default network configuration is set to DHCP enabled. You will need to make sure your network environment supports the switch setup before connecting it to the network.

1. Launch your web browser on a computer.
2. In the browser's address bar type in the switch's default IP address (192.168.1.1). The login screen displays.
3. 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.
4. Click **Login** to enter the management interface.

The following figure displays the Login Screen.

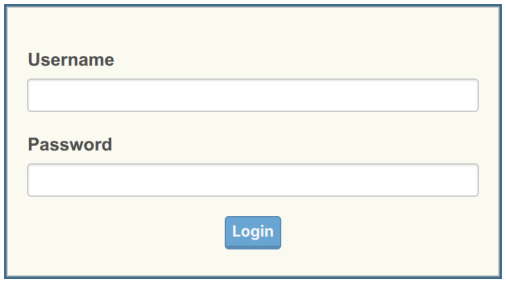


Figure 3.1 Login Screen

3.2 Recommended Practices

One of the easiest things to do to help increase the security posture of the network infrastructure is to implement a policy and standard for secure management. This practice is an easy way to maintain a healthy and secure network.

After you have performed the basic configurations on your switches, the following is a recommendation which is considered best practice policy.

3.3 Monitoring

3.3.1 Device Information

The Device Information menu lists information, such as: System Name, System Location, MAC Address, Firmware version, and more, pertaining to the system. The information is for review only. To modify the device information, see the respective item within the user interface.

To access this page, click **Monitoring > Device Information**.

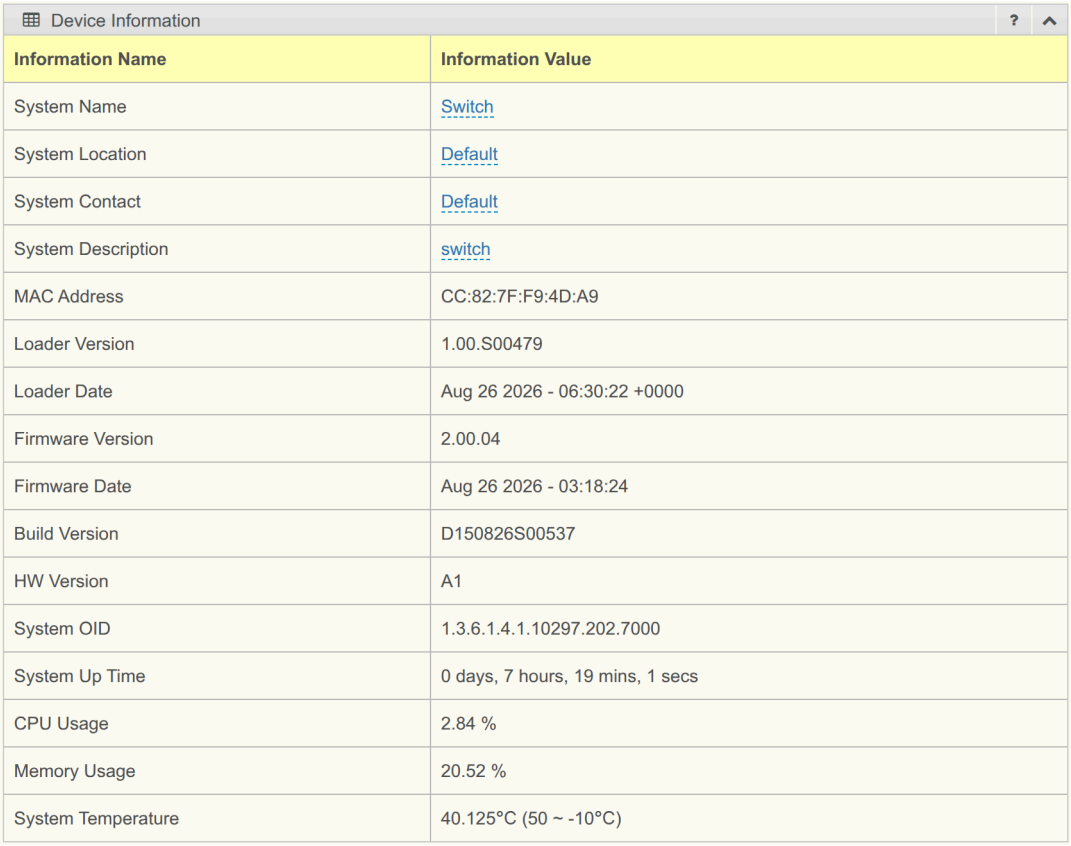


Figure 3.2 Monitoring > Device Information

The following table describes the items in the previous figure.

Item	Description
System Name	Click **Switch** to enter the system name: up to 128 alphanumeric characters (default is Switch).
System Location	Click **Default** to enter the location: up to 256 alphanumeric characters (default is Default).
System Contact	Click **Default** to enter the contact person: up to 128 alphanumeric characters (default is Default).
System Description	Displays the description of the switch.
MAC Address	Displays the MAC address of the switch.
Loader Version	Displays the current loader version of the switch.
Loader Date	Displays the current loader build date of the switch.
Firmware Version	Displays the current firmware version of the switch.
Firmware Date	Displays the current firmware build date of the switch.
Build Version	Displays the current firmware build version of the switch.
HW Version	Displays the hardware version of the switch.
System OID	Displays the base object ID of the switch.
System Up Time	Displays the time since the last switch reboot.
CPU Usage	Displays the current CPU utilization of the switch.
Memory Usage	Displays the current memory utilization of the switch.
System Temperature	Displays the current temperature of the switch.

3.3.2 Logging Message

The Logging Message Filter page allows you to enable the display of logging message filter.

To access this page, click **Monitoring > Logging Message**.

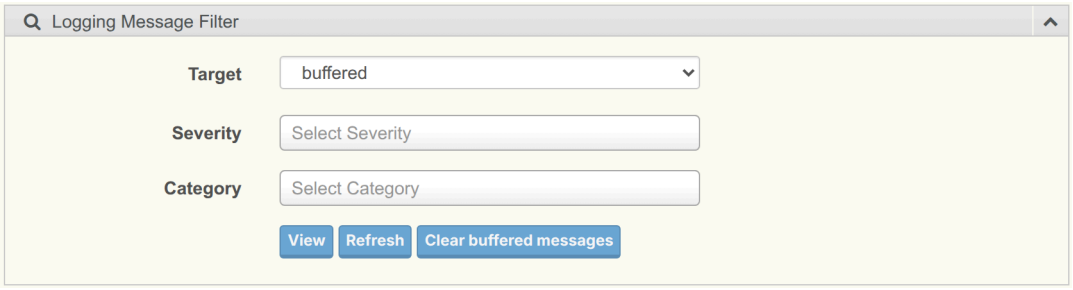


Figure 3.3 Monitoring > Logging Message

The following table describes the items in the previous figure.

Item	Description
Target	Click the drop-down menu to select a target to store the log messages. ■ Buffered: Store log messages in RAM. All log messages are cleared after system reboot. ■ File: Store log messages in a file.
Severity	The setting allows you to designate a severity level for the Logging Message Filter function. Click the drop-down menu to select the severity level target setting. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity. ■ alert: Indicates action must be taken immediately. ■ crit: 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.
Category	Click the drop-down menu to select the category level target setting.
View	Click **View** to display all Logging Information and Logging Message information.
Refresh	Click **Refresh** to update the screen.
Clear buffered messages	Click **Clear buffered messages** to clear the logging buffer history list.

The following figure displays the **Logging Information** settings.

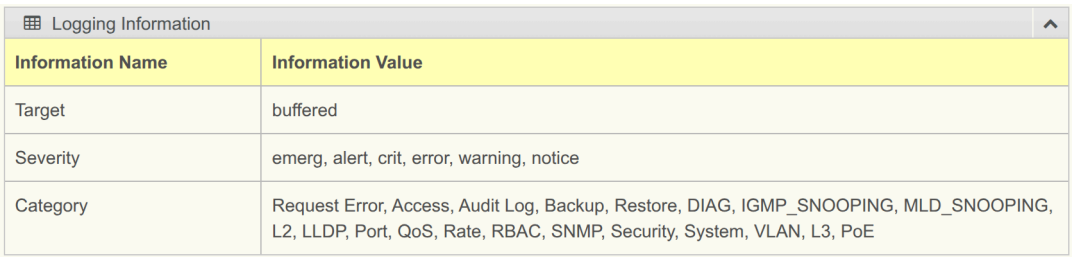


Figure 3.4 Monitoring > Logging Information

The following figure displays the **Logging Message** settings.

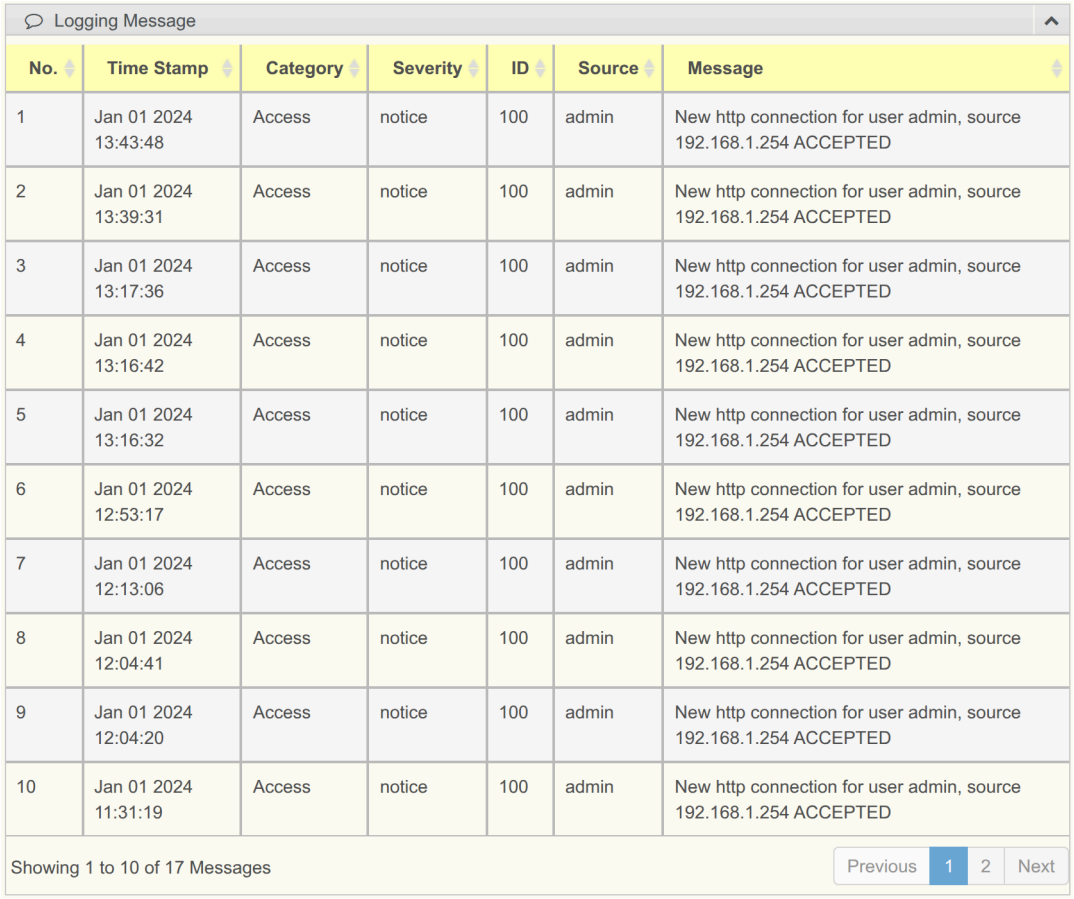


Figure 3.5 Monitoring > Logging Message

3.3.3 Port Monitoring

Port Network Monitor is a bandwidth and network monitoring tool for the purpose of capturing network traffic and measuring of network throughput. The monitoring functionality includes listing of port statistics as well as port utilization.

3.3.3.1 Port Statistics

To access this page, click **Monitoring > Port Monitoring > Port Statistics**.



Figure 3.6 Monitoring > Port Monitoring > Port Statistics

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select a port and its captured statistical setting values.
Clear	Click **Clear** to clear the counter selections.

The following figure displays the **IF MIB Counters** settings.

GE1 IF MIB Counters

IF MIB Counter Name	MIB Counter Value
ifInOctets	0
ifHCInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	0
ifHCOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	0
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

Figure 3.7 Monitoring > Port Monitoring > IF MIB Counters

The following figure displays the **Ether-Like MIB Counters** settings.

GE1 Ether-Like MIB Counters

Ether-Like MIB Counter Name	MIB Counter Value
dot3StatsAlignmentErrors	0
dot3StatsFCSErrors	0
dot3StatsSingleCollisionFrames	0
dot3StatsMultipleCollisionFrames	0
dot3StatsDeferredTransmissions	0
dot3StatsLateCollisions	0
dot3StatsExcessiveCollisions	0
dot3StatsFrameTooLongs	0
dot3StatsSymbolErrors	0
dot3ControlInUnknownOpcodes	0
dot3InPauseFrames	0
dot3OutPauseFrames	0

Figure 3.8 Monitoring > Port Monitoring > Ether-Like MIB Counters

The following figure displays the **RMON MIB Counters** settings.

GE1 Rmon MIB Counters

Rmon MIB Counter Name	MIB Counter Value
etherStatsDropEvents	0
etherStatsOctets	0
etherStatsPkts	0
etherStatsBroadcastPkts	0
etherStatsMulticastPkts	0
etherStatsCRCAlignErrors	0
etherStatsUnderSizePkts	0
etherStatsOverSizePkts	0
etherStatsFragments	0
etherStatsJabbers	0
etherStatsCollisions	0
etherStatsPkts64Octets	0
etherStatsPkts65to127Octets	0
etherStatsPkts128to255Octets	0
etherStatsPkts256to511Octets	0
etherStatsPkts512to1023Octets	0
etherStatsPkts1024to1518Octets	0

Figure 3.9 Monitoring > Port Monitoring > Rmon MIB Counters

3.3.3.2 Port Utilization

To access this page, click **Monitoring > Port Monitoring > Port Utilization**.

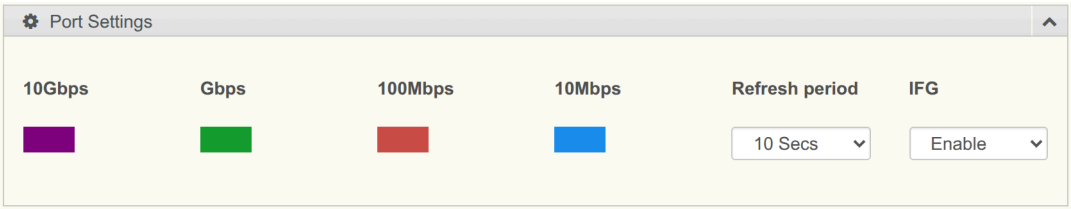


Figure 3.10 Monitoring > Port Monitoring > Port Utilization

The following table describes the items in the previous figure.

Item	Description
Refresh period	Click the drop-down menu to select and designate a period (second intervals) to refresh the information (TX and RX) listings.
IFG	Click the drop-down menu to enable or disable the Interframe Gap (IFG) statistic.

The following figure displays the **TX** settings.

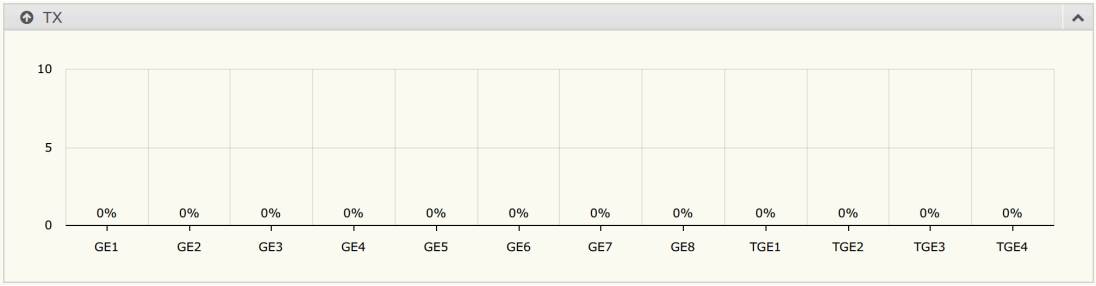


Figure 3.11 Monitoring > Port Monitoring > TX

The following figure displays the **RX** settings.

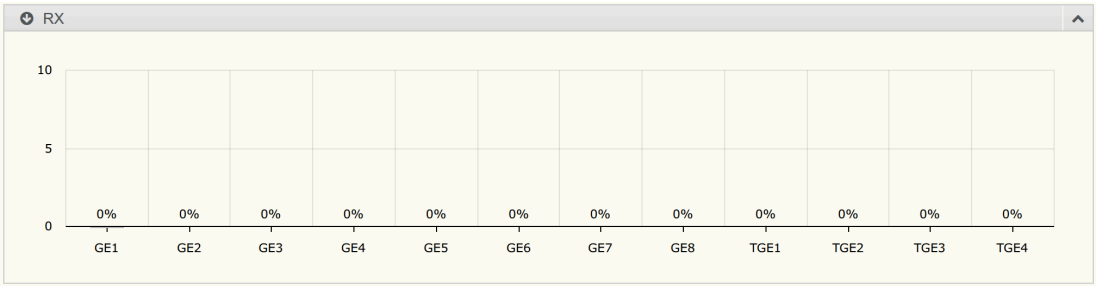


Figure 3.12 Monitoring > Port Monitoring > RX

3.3.4 Link Aggregation

The Link Aggregation function provides LAG information for each trunk. It displays membership status, link state and membership type for each port.

To access this page, click **Monitoring > Link Aggregation**.

Link Aggregation Group Status

LAG	Name	Type	Link State	Active Member	Standby Member
Trunk1		---	Not Present	-	-
Trunk2		---	Not Present	-	-
Trunk3		---	Not Present	-	-
Trunk4		---	Not Present	-	-
Trunk5		---	Not Present	-	-
Trunk6		---	Not Present	-	-
Trunk7		---	Not Present	-	-
Trunk8		---	Not Present	-	-

Figure 3.13 Monitoring > Link Aggregation

The following figure displays the **LACP Information** settings.

LACP Information

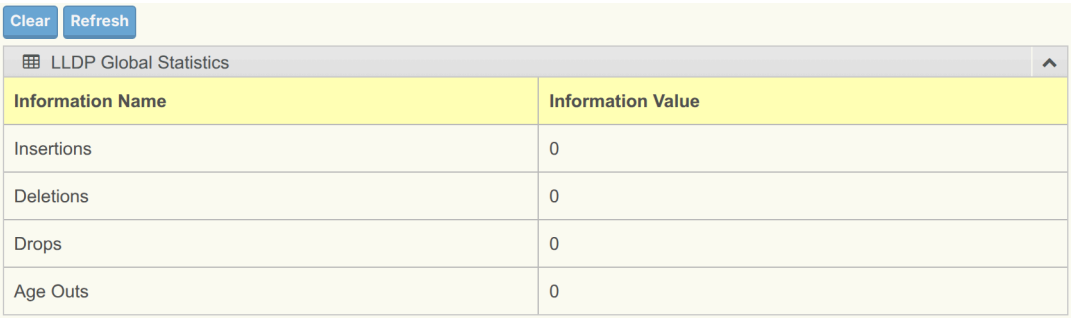
LAG	Port	PartnerSysId	PnKey	AtKey	Sel	Mux	Receiv	PrdTx	AtState	PnState

Figure 3.14 Monitoring > LACP Information

3.3.5 LLDP Statistics

The LLDP Statistics page displays the LLDP statistics.

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



Information Name	Information Value
Insertions	0
Deletions	0
Drops	0
Age Outs	0

Figure 3.15 Monitoring > LLDP Statistics

The following table describes the items in the previous figure.

Item	Description
Clear	Click **Clear** to reset LLDP 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.

The following figure displays the **LLDP Port Statistics** settings.

LLDP Port Statistics

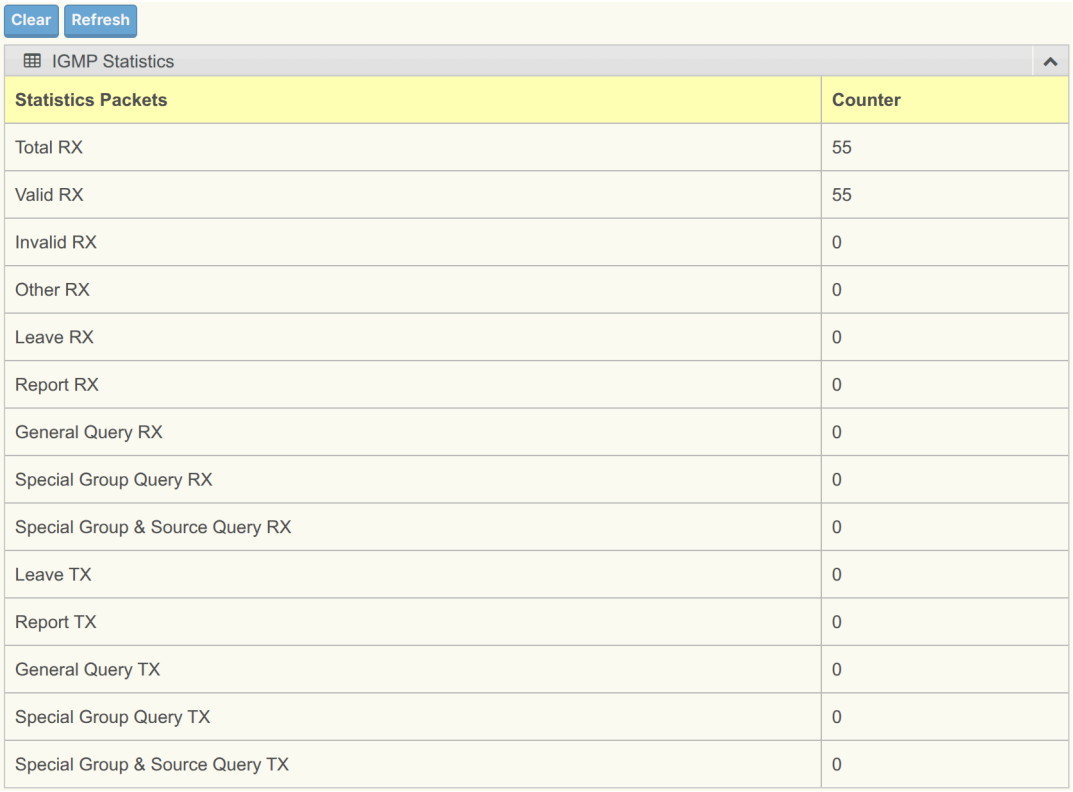
Port	TX Frames	RX Frames			RX TLVs		RX Ageouts
	Total	Total	Discarded	Errors	Discarded	Unrecognized	Total
GE1	0	0	0	0	0	0	0
GE2	0	0	0	0	0	0	0
GE3	0	0	0	0	0	0	0
GE4	0	0	0	0	0	0	0
GE5	0	0	0	0	0	0	0
GE6	0	0	0	0	0	0	0
GE7	0	0	0	0	0	0	0
GE8	0	0	0	0	0	0	0
TGE1	0	0	0	0	0	0	0
TGE2	0	0	0	0	0	0	0
TGE3	0	0	0	0	0	0	0
TGE4	0	0	0	0	0	0	0

Figure 3.16 Monitoring > LLDP Port Statistics

3.3.6 IGMP Statistics

The IGMP Statistics function displays statistical package information for IP multi casting.

To access this page, click **Monitoring > IGMP Statistics**.



Statistics Packets	Counter
Total RX	55
Valid RX	55
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

Figure 3.17 Monitoring > IGMP Statistics

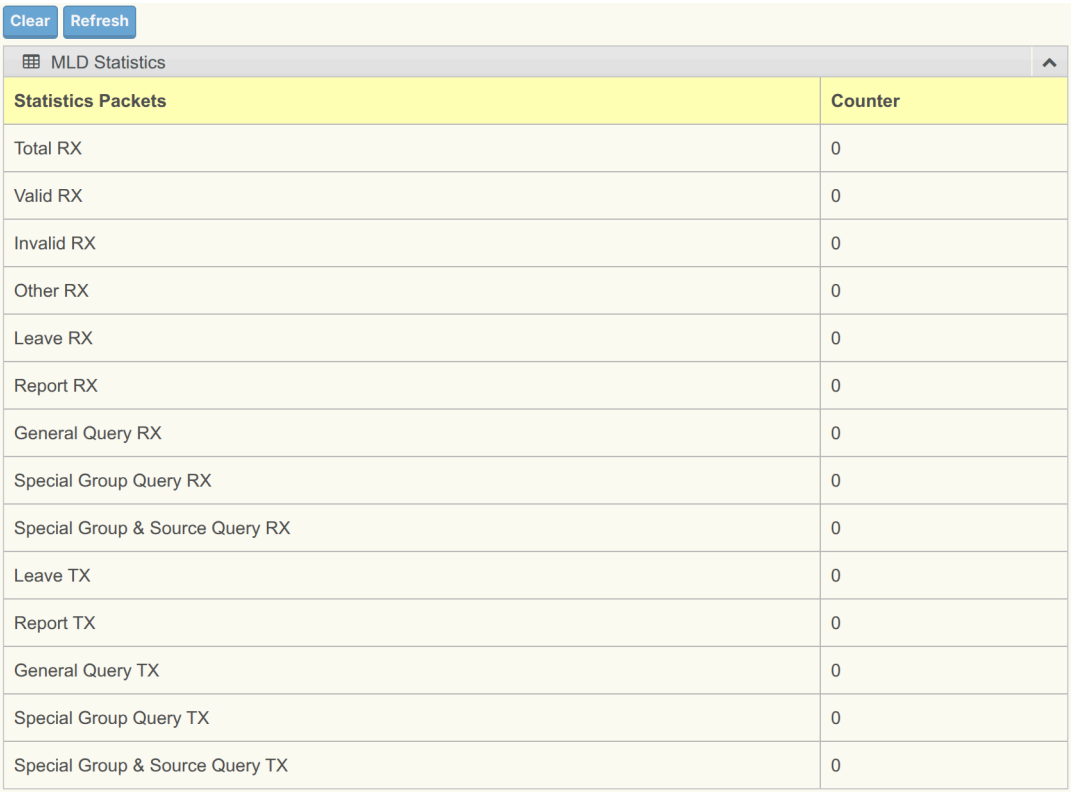
The following table describes the items in the previous figure.

Item	Description
Clear	Click **Clear** to refresh IGMP 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.

3.3.7 MLD Statistics

The MLD Statistics function displays statistical package information for MLD message.

To access this page, click **Monitoring > MLD Statistics**.



Statistics Packets	Counter
Total RX	0
Valid RX	0
Invalid RX	0
Other RX	0
Leave RX	0
Report RX	0
General Query RX	0
Special Group Query RX	0
Special Group & Source Query RX	0
Leave TX	0
Report TX	0
General Query TX	0
Special Group Query TX	0
Special Group & Source Query TX	0

Figure 3.18 Monitoring > MLD Statistics

The following table describes the items in the previous figure.

Item	Description
Clear	Click **Clear** to refresh MLD 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.

3.4 System

3.4.1 IP Settings

The IP Settings menu allows you to select a static or DHCP network configuration. The Static displays the configurable settings for the static option.

To access this page, click **System > IP Settings**.

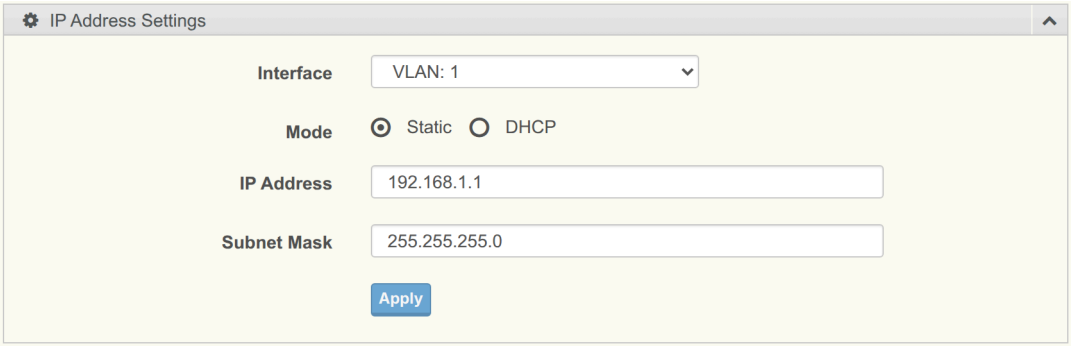


Figure 3.19 System > IP Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the VLAN interface whose address is configured.
Mode	Click the radio button to select the IP Address Setting mode: Static or DHCP.
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.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **IP Address Information** settings.

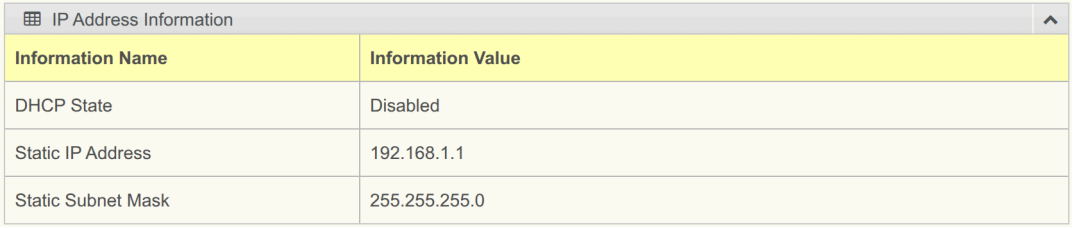


Figure 3.20 System > IP Address Information

3.4.2 IPv6 Settings

To access this page, click **System > IPv6 Settings**.

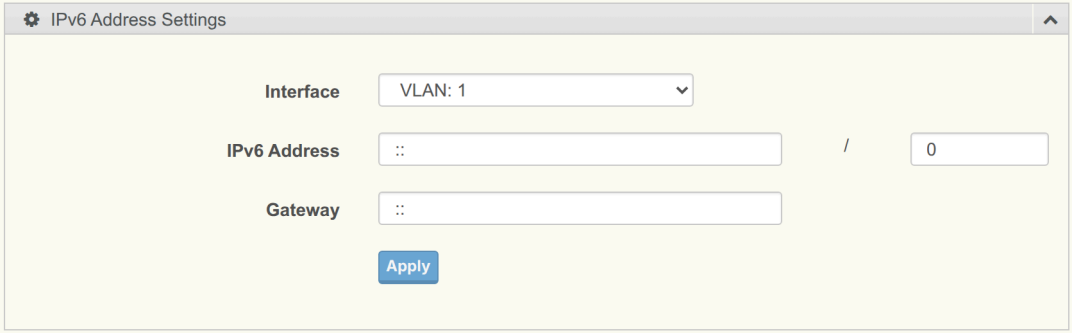


Figure 3.21 System > IPv6 Settings

The following table describes the items in the previous figure.

Item	Description
Interface	Click the drop-down menu to select the VLAN interface whose address is configured.
IPv6 Address	Enter the IPv6 address for the system.
Gateway	Enter the gateway address for the system.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **IPv6 Information** settings.

IPv6 Information

Information Name	Information Value
IPv6 Link Local Address	fe80::ce82:7fff:fef9:4da9 / 64
IPv6 Static Address	:: / 0
IPv6 Static Router	::

Figure 3.22 System > IPv6 Information

3.4.3 System Time

To access this page, click **System > System Time**.

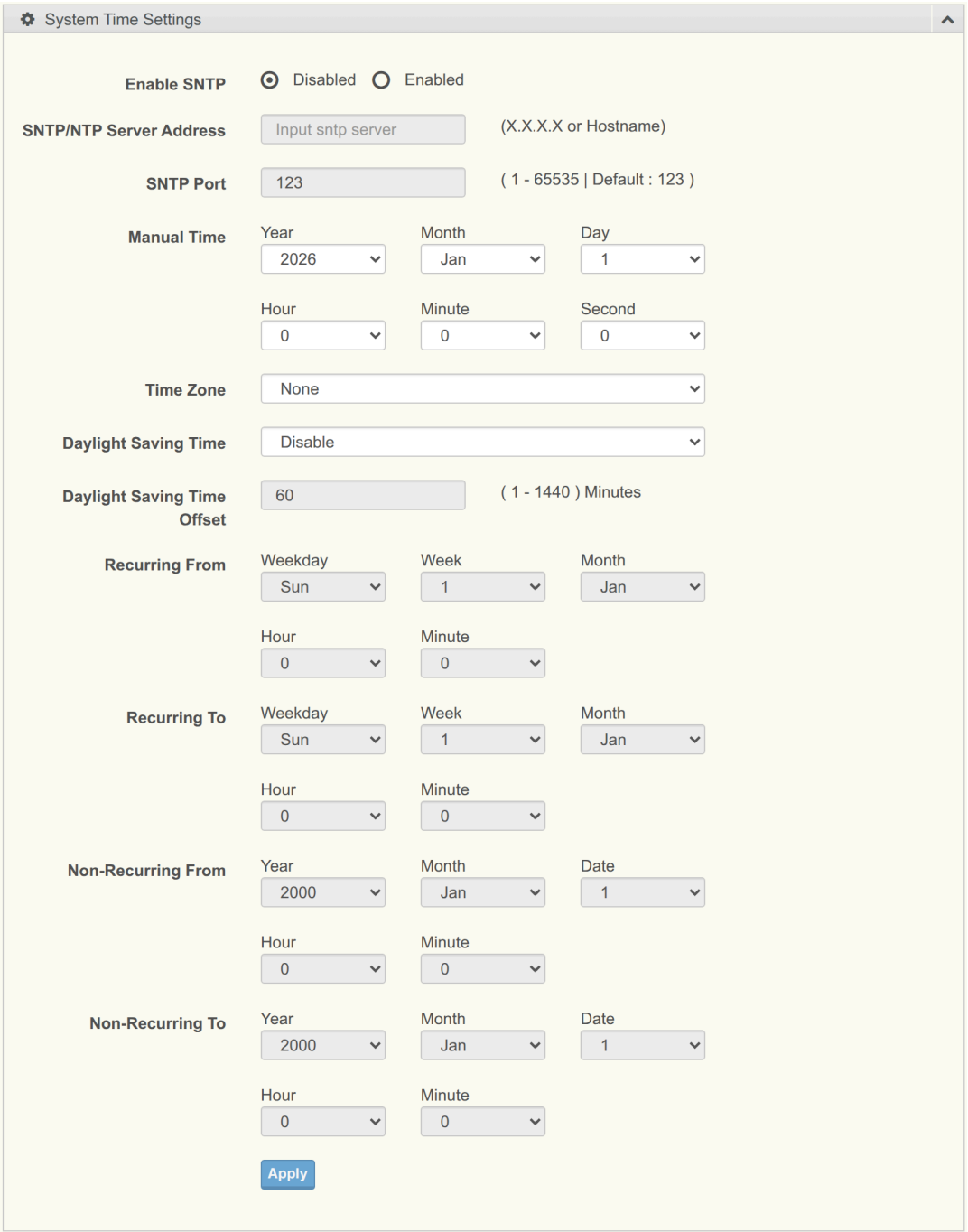


Figure 3.23 System > System Time

The following table describes the items in the previous figure.

Item	Description
Enable SNTP	Click the radio button to enable or disable the SNTP.
SNTP/NTP Server Address	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.
SNTP Port	Enter the port on the server to which SNTP requests are to be sent. Allowed range is 1 to 65535 (default: 123).
Manual Time	Click the drop-down menus to set local date and time of the system.
Time Zone	Click the drop-down menu to select a system time zone.
Daylight Saving Time	Click the drop-down menu to enable or disable the daylight saving time settings.
Daylight Saving Time Offset	Enter the offsetting variable in seconds to adjust for daylight saving time.
Recurring From	Click the drop-down menu to designate the start date and time for daylight saving time.
Recurring To	Click the drop-down menu to designate the end date and time for daylight saving time.
Non-Recurring From	Click the drop-down menu to designate a start date and time for a non-recurring daylight saving time event.
Non-Recurring To	Click the drop-down menu to designate the end date and time for a non-recurring daylight saving time event.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **System Time Information** settings.

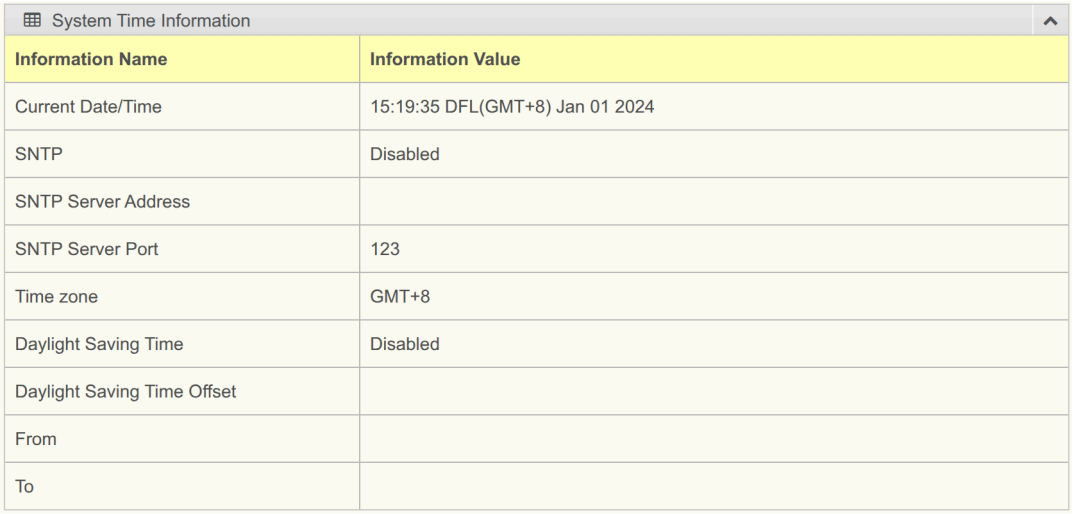


Figure 3.24 System > System Time Information

3.4.4 Network Port

To access this page, click **System > Network Port**.



Figure 3.25 System > Network Port

The following table describes the items in the previous figure.

Item	Description
HTTP	By default, the HTTPS port setting is set to port 80. To assign the web interface to a different port, enter the port number in the field.
HTTPS	By default, the HTTPS port setting is set to port 443. To assign the web interface to a different port, enter the port number in the field.
TELNET	By default, the TELNET port setting is set to port 23. To assign the web interface to a different port, enter the port number in the field.
SSH	By default, the SSH port setting is set to port 22. To assign the web interface to a different port, enter the port number in the field.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Network Port Information** settings.

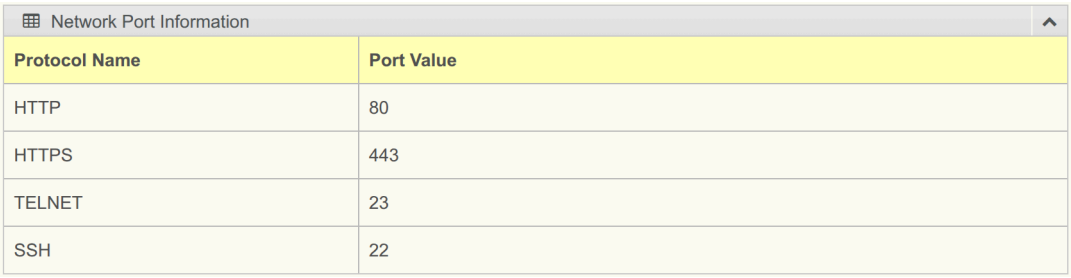


Figure 3.26 System > Network Port Information

3.5 L2 Switching

3.5.1 Port Configuration

Port Configuration describes how to use the user interface to configure LAN ports on the switch.

To access this page, click **L2 Switching > Port Configuration**.

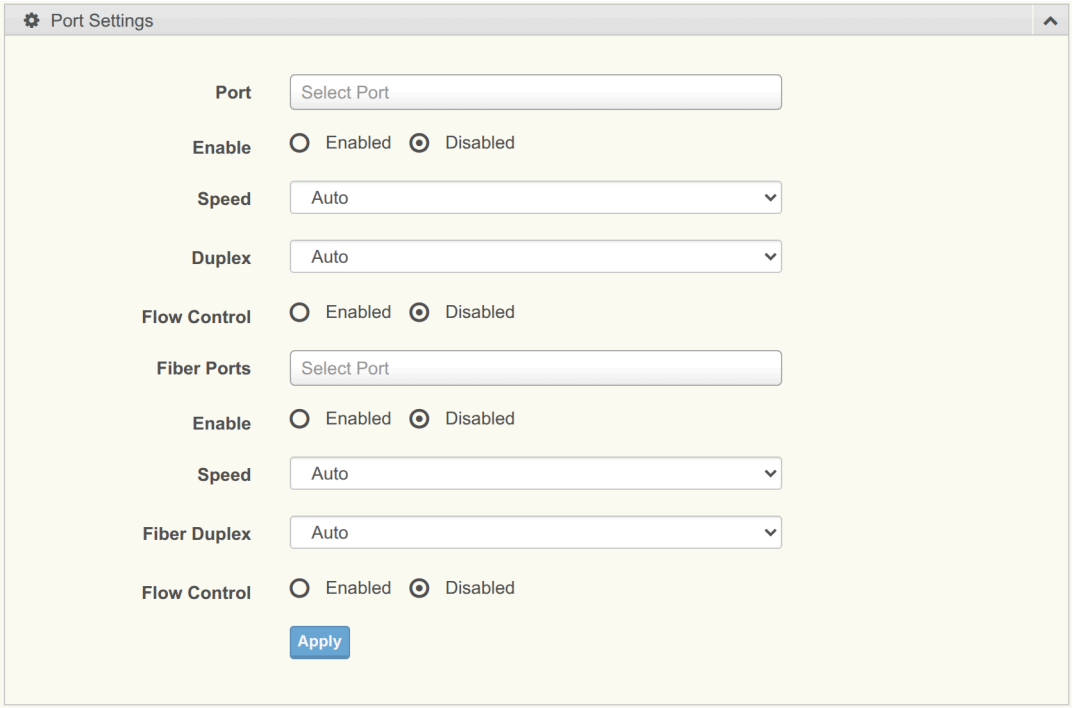


Figure 3.27 L2 Switching > Port Configuration

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port for the L2 Switch setting.
Enabled	Click the radio-button to enable or disable the Port Setting function.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto-100M, Auto-1000M, Auto-10/100M, 10M, 100M, or 1000M.
Duplex	Click the drop-down menu to select the duplex setting: Auto, Half or Full.
Flow Control	Click the radio button to enable or disable the flow control function.
Fiber Ports	Click the drop-down menu to select the port for the L2 Switch Fiber port setting.
Enabled	Click the radio-button to enable or disable the Fiber Port Setting function.
Speed	Click the drop-down menu to select the fiber port speed: Auto, Auto1000M, 100M, or 1000M.
Fiber Duplex	Click the drop-down menu to select the duplex setting: Half or Full.
Flow Control	Click the radio button to enable or disable the flow control function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Port Name Settings** settings.



Figure 3.28 L2 Switching > Port Name Settings

The following table describes the items in the previous figure.

Item	Description
Display Method	Click the drop-down menu to select how a port is identified in the Port Status table: by port number or by the description entered for it.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Port Status** settings. Click **Edit** beside a port to enter a description for that port.

Port Status

Port	Description	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
GE1	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE2	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE3	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE4	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE5	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE6	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
GE7	Edit	Enabled	UP	Auto-1000M	Full	Disabled	Disabled
GE8	Edit	Enabled	DOWN	Auto	Auto	Disabled	Disabled
TGE1	Edit	Enabled	DOWN	Auto	Full	Disabled	Disabled
TGE2	Edit	Enabled	DOWN	Auto	Full	Disabled	Disabled
TGE3	Edit	Enabled	DOWN	Auto	Full	Disabled	Disabled
TGE4	Edit	Enabled	DOWN	Auto	Full	Disabled	Disabled

Figure 3.29 L2 Switching > Port Status

The following figure displays the dialog that opens when **Edit** is clicked.



Figure 3.30 L2 Switching > Port Configuration > Edit description of GE1

3.5.2 Port Mirror

Port mirroring function allows the sending of a copy of network packets seen on one switch port to a network monitoring connection on another switch port. Port mirroring can be used to analyze and debug data or diagnose errors on a network or to mirror either inbound or outbound traffic (or both).

There are no preset values in the Port Mirror. The displayed values do not represent the actual setting values.

To access this page, click **L2 Switching > Port Mirror**.

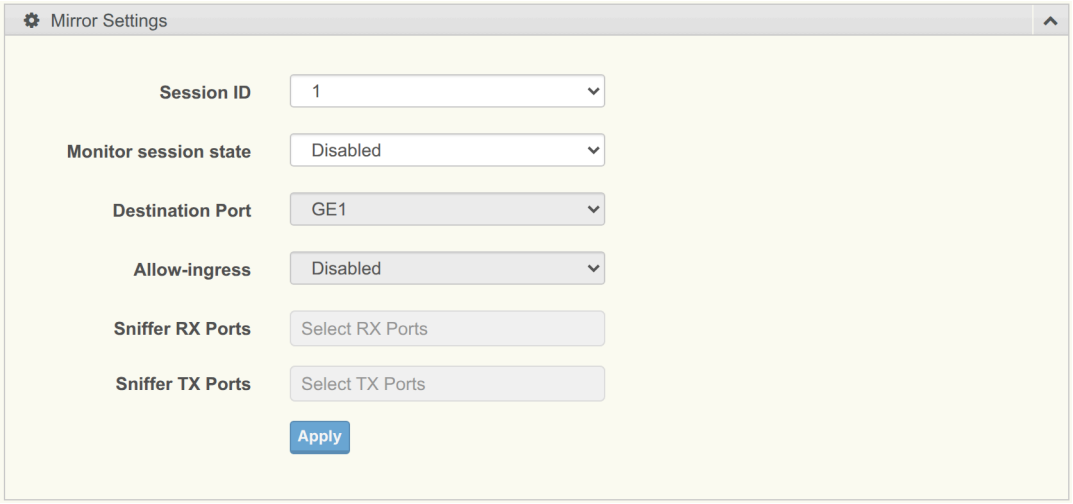


Figure 3.31 L2 Switching > Port Mirror

The following table describes the items in the previous figure.

Item	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.
Monitor session state	Click the drop-down menu to enable or disable the session mode for a selected session ID.
Destination Port	Click the drop-down menu to select the destination port and receive all the traffic from configured mirrored port(s).
Allow-ingress	Click the drop-down menu to enable or disable the Allow-ingress function.
Sniffer RX Ports	Enter the variable to define the RX port.
Sniffer TX Ports	Enter the variable to define the TX port.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Mirror Status** settings.

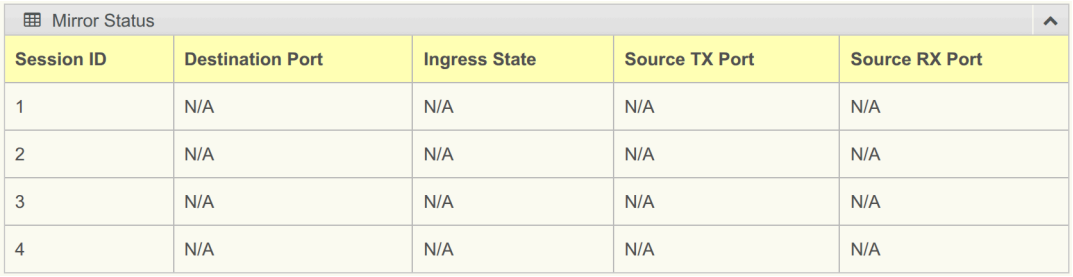


Figure 3.32 L2 Switching > Mirror Status

3.5.3 Link Aggregation

Link Aggregation is a method for combining multiple network connections in parallel in order to increase throughput beyond the capability of a single connection, and to provide redundancy in case one of the links should fail.

3.5.3.1 Load Balance

The Load Balancing page allows you to select between a MAC Address or IP/MAC Address algorithm for the even distribution of IP traffic across two or more links.

To access this page, click **L2 Switching > Link Aggregation > Load Balance**.

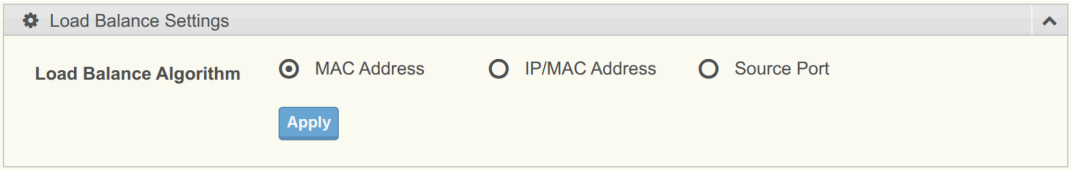


Figure 3.33 L2 Switching > Link Aggregation > Load Balance

The following table describes the items in the previous figure.

Item	Description
Load Balance Algorithm	Select the radio button to select the Load Balance Setting: MAC Address, IP/MAC Address or Source Port.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Load Balance Information** settings.



Figure 3.34 L2 Switching > Link Aggregation > Load Balance Information

3.5.3.2 LAG Management

Link aggregation is also known as trunking. It is a feature available on the Ethernet gateway and is used with Layer 2 Bridging. Link aggregation allows for the logical merging of multiple ports into a single link.

To access this page, click **L2 Switching > Link Aggregation > LAG Management**.

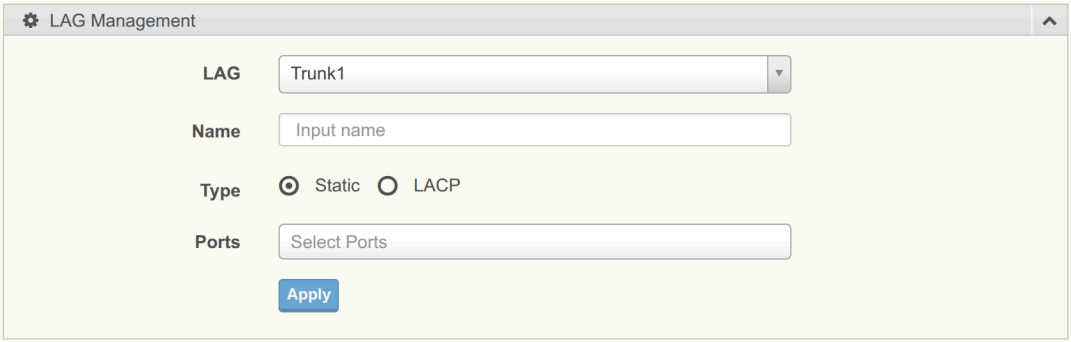


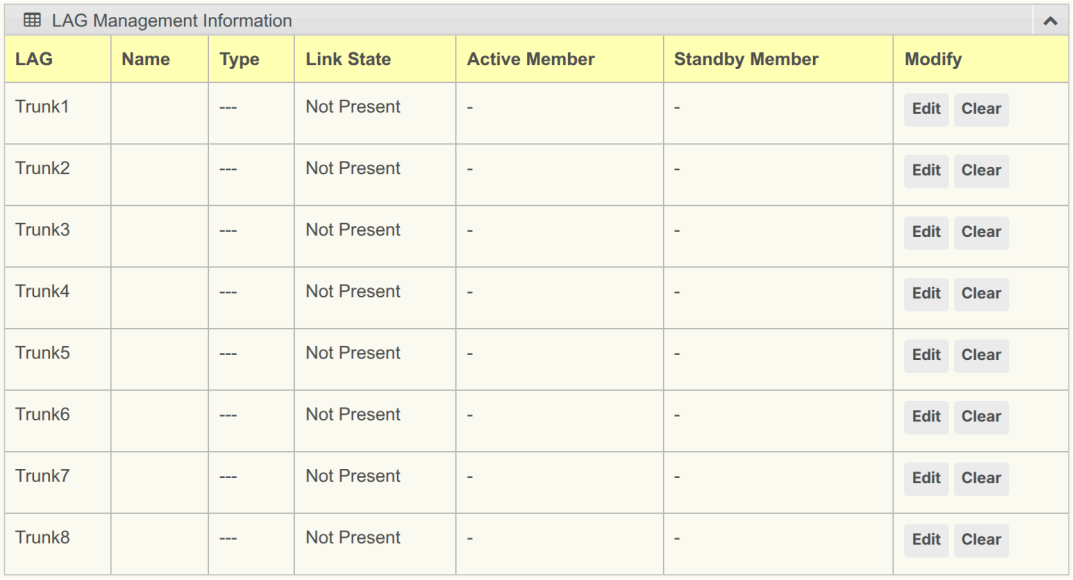
Figure 3.35 L2 Switching > Link Aggregation > LAG Management

The following table describes the items in the previous figure.

Item	Description
LAG	Click the drop-down menu to select the designated trunk group: Trunk1-Trunk8.
Name	Enter an entry to specify the LAG name.
Type	Click the radio button to specify the type mode: Static or LACP.
Ports	Click the drop-down menu to select designated ports. The available ports vary by model; the figure shows GE1-GE8 and TGE1-TGE4.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **LAG Management Information** settings.

Click **Edit** beside a trunk to modify it, or **Clear** to remove its member ports.



LAG	Name	Type	Link State	Active Member	Standby Member	Modify
Trunk1		---	Not Present	-	-	Edit Clear
Trunk2		---	Not Present	-	-	Edit Clear
Trunk3		---	Not Present	-	-	Edit Clear
Trunk4		---	Not Present	-	-	Edit Clear
Trunk5		---	Not Present	-	-	Edit Clear
Trunk6		---	Not Present	-	-	Edit Clear
Trunk7		---	Not Present	-	-	Edit Clear
Trunk8		---	Not Present	-	-	Edit Clear

Figure 3.36 L2 Switching > Link Aggregation > LAG Management Information

3.5.3.3 LAG Port Settings

The LAG Port Settings page allows you to enable or disable, set LAG status, speed and flow control functions.

In this example we will configure a LAG between the following switches:

To access this page, click **L2 Switching > Link Aggregation > LAG Port Settings**.

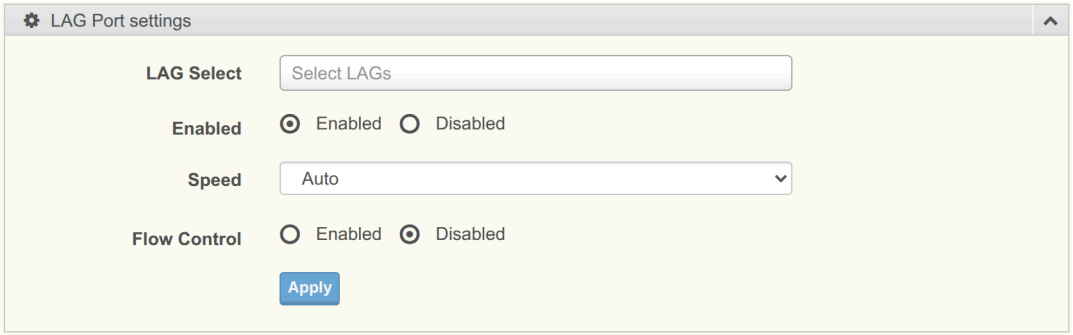


Figure 3.37 L2 Switching > Link Aggregation > LAG Port Settings

The following table describes the items in the previous figure.

Item	Description
LAG Select	Click the drop-down menu to select a predefined LAG trunk definition: Trunk1-Trunk8.
Enabled	Click the radio button to enable or disable the LAG Port.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto-100M, Auto-1000M, Auto-10/100M, 10M, 100M, or 1000M.
Flow Control	Click the radio button to enable or disable the Flow Control for the LAG Port.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **LAG Port Status** settings.

LAG Port Status

LAG	Description	Port Type	Enable State	Link Status	Speed	Duplex	FlowCtrl Config	FlowCtrl Status
Trunk1			Enabled		Auto	Auto	Disabled	Disabled
Trunk2			Enabled		Auto	Auto	Disabled	Disabled
Trunk3			Enabled		Auto	Auto	Disabled	Disabled
Trunk4			Enabled		Auto	Auto	Disabled	Disabled
Trunk5			Enabled		Auto	Auto	Disabled	Disabled
Trunk6			Enabled		Auto	Auto	Disabled	Disabled
Trunk7			Enabled		Auto	Auto	Disabled	Disabled
Trunk8			Enabled		Auto	Auto	Disabled	Disabled

Figure 3.38 L2 Switching > Link Aggregation > LAG Port Status

3.5.3.4 LACP Priority Settings

The LACP Priority Settings page allows you to configure the system priority for LACP.

To access this page, click **L2 Switching > Link Aggregation > LACP Priority Settings**.



Figure 3.39 L2 Switching > Link Aggregation > LACP Priority Settings

The following table describes the items in the previous figure.

Item	Description
System Priority	Enter the value (1-65535) to designate the LACP system priority.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **LACP Priority Information** settings.

LACP Priority Information

Information Name	Information Value
System Priority	32768

Figure 3.40 L2 Switching > Link Aggregation > LACP Priority Information

3.5.3.5 LACP Port Settings

Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. By configuring the LACP function, the switch can negotiate an automatic bundling of links by sending LACP packets to the peer device (also implementing LACP).

To access this page, click **L2 Switching > Link Aggregation > LACP Port Settings**.

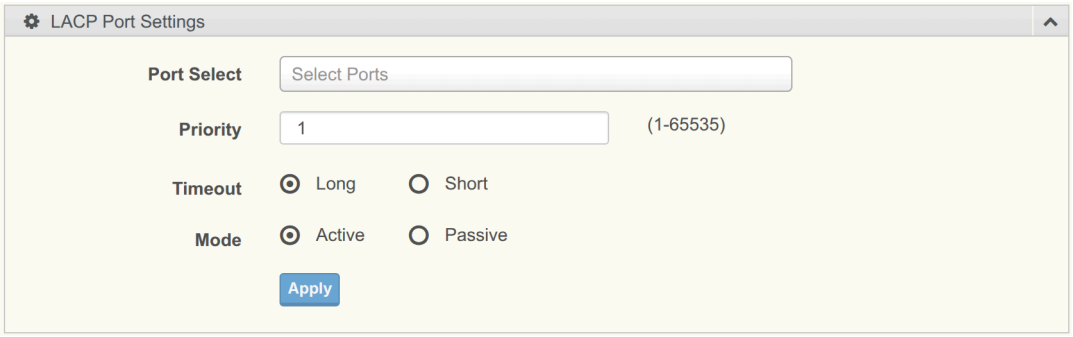


Figure 3.41 L2 Switching > Link Aggregation > LACP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select a port for the LACP Port Settings. The available ports vary by model; the figure shows GE1-GE8 and TGE1-TGE4. However, the available settings are dependent on the connected LACP device and may not be listed as displayed in the current figure.
Priority	Enter a variable (1 to 65535) to assign a priority to the defined port selection.
Timeout	Click the radio button to select a long or short timeout period.
Mode	Click the radio button to select the setting mode: Active or Passive. ■ Active: Enables LACP unconditionally. ■ Passive: Enables LACP only when an LACP device is detected (default state).
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **LACP Port Information** settings.

LACP Port Information

Port Name	Priority	Timeout	Mode
GE1	1	Long	Passive
GE2	1	Long	Passive
GE3	1	Long	Passive
GE4	1	Long	Passive
GE5	1	Long	Passive
GE6	1	Long	Passive
GE7	1	Long	Passive
GE8	1	Long	Passive
TGE1	1	Long	Passive
TGE2	1	Long	Passive
TGE3	1	Long	Passive
TGE4	1	Long	Passive

Figure 3.42 L2 Switching > Link Aggregation > LACP Port Information

3.5.4 802.1Q VLAN

The 802.1Q VLAN feature allows for a single VLAN to support multiple VLANs. With the 802.1Q feature you can preserve VLAN IDs and segregate different VLAN traffic.

The 802.1Q VLAN tag feature encapsulates the 802.1Q VLAN tagging within another 802.1Q VLAN tag. The outer tag is assigned following the AP group, while the inner VLAN ID is assigned dynamically by the AAA server.

3.5.4.1 VLAN Management

The management of VLANs is available through the VLAN Settings page. Through this page you can add or delete VLAN listings and add a prefix name to an added entry.

To access this page, click **L2 Switching > 802.1Q VLAN > VLAN Management**.

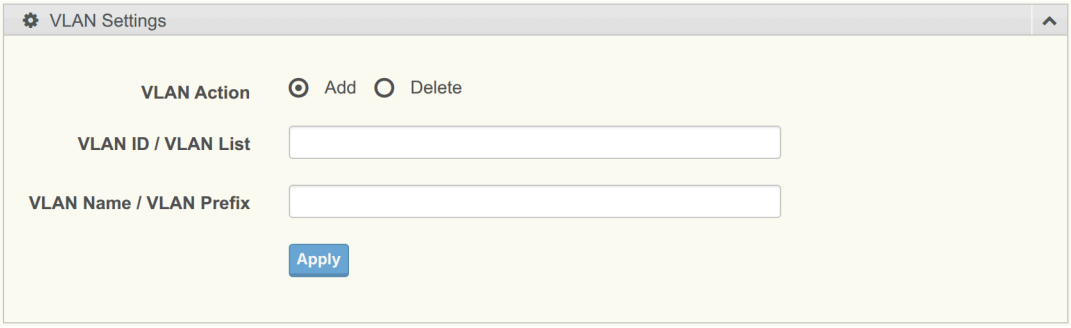


Figure 3.43 L2 Switching > 802.1Q VLAN > VLAN Management

The following table describes the items in the previous figure.

Item	Description
VLAN Action	Click the radio button to add or delete the VLAN entry shown in the previous field.
VLAN ID / VLAN List	Enter the name of the VLAN entry to setup.
VLAN Name / VLAN Prefix	Enter the prefix to be used by the VLAN list entry in the previous field.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **VLAN Table** settings.

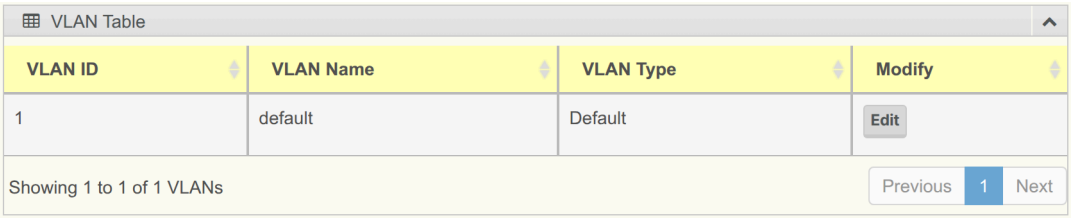


Figure 3.44 L2 Switching > 802.1Q VLAN > VLAN Table

The following figure displays the dialog that opens when **Edit** is clicked.

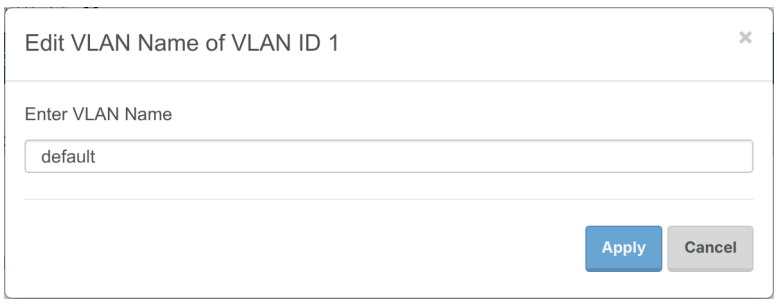


Figure 3.45 L2 Switching > 802.1Q VLAN > VLAN Management > Edit VLAN Name of VLAN ID 1

3.5.4.2 PVID Settings

The PVID Settings page allows you to designate a PVID for a selected port, define the accepted type and enable/disable the ingress filtering.

To access this page, click **L2 Switching > 802.1Q VLAN > PVID Settings**.

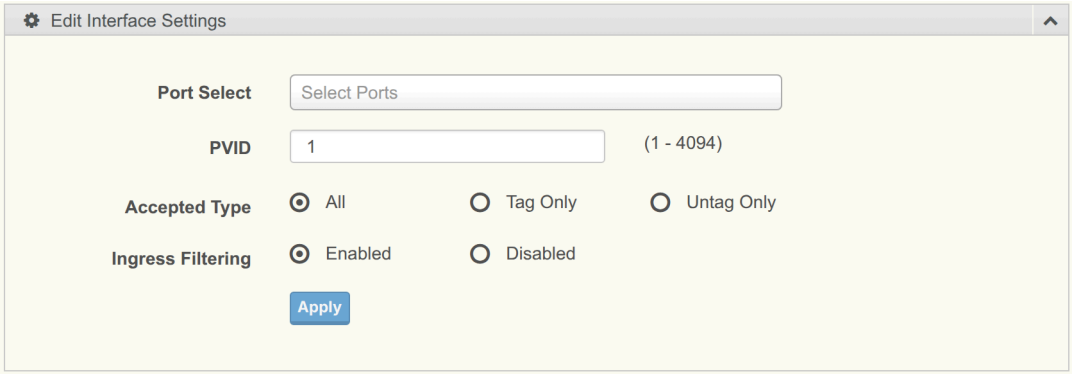


Figure 3.46 L2 Switching > 802.1Q VLAN > PVID Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select a port and edit its settings. The available ports vary by model; the figure shows GE1-GE8, TGE1-TGE4, and Trunk1-Trunk8.
PVID	Enter the VLAN ID you want assigned to untagged or priority tagged frames received on this port. The value ranges 1 to 4094. The default is 1.
Accepted Type	Click the radio button to specify which frames to forward. Tag Only discards any untagged or priority tagged frames. Untag Only discards any tagged frames. All accepts all untagged and tagged frames. Whichever you select, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN standard. The default is All.
Ingress Filtering	Click the radio button to specify how you want the port to handle tagged frames. If you enable Ingress Filtering, 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 Disabled, all tagged frames will be accepted. The default is Disabled.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Port VLAN Status** settings.

Port VLAN Status

Port	Interface VLAN Mode	PVID	Accept Frame Type	Ingress Filtering
GE1	Hybrid	1	ALL	Enabled
GE2	Hybrid	1	ALL	Enabled
GE3	Hybrid	1	ALL	Enabled
GE4	Hybrid	1	ALL	Enabled
GE5	Hybrid	1	ALL	Enabled
GE6	Hybrid	1	ALL	Enabled
GE7	Hybrid	1	ALL	Enabled
GE8	Hybrid	1	ALL	Enabled
TGE1	Hybrid	1	ALL	Enabled
TGE2	Hybrid	1	ALL	Enabled
TGE3	Hybrid	1	ALL	Enabled
TGE4	Hybrid	1	ALL	Enabled
Trunk1	Hybrid	1	ALL	Enabled
Trunk2	Hybrid	1	ALL	Enabled
Trunk3	Hybrid	1	ALL	Enabled
Trunk4	Hybrid	1	ALL	Enabled
Trunk5	Hybrid	1	ALL	Enabled
Trunk6	Hybrid	1	ALL	Enabled
Trunk7	Hybrid	1	ALL	Enabled
Trunk8	Hybrid	1	ALL	Enabled

Figure 3.47 L2 Switching > 802.1Q VLAN > Port VLAN Status

3.5.4.3 Port to VLAN

The Port to VLAN page allows you to add a port to a VLAN and select the related parameters.

To access this page, click **L2 Switching > 802.1Q VLAN > Port to VLAN**.



Figure 3.48 L2 Switching > 802.1Q VLAN > Port to VLAN

The following table describes the items in the previous figure.

Item	Description
Port	Displays the assigned port to the entry.
Interface VLAN Mode	Displays the Hybrid mode to the listed VLAN port.
Membership	Displays the assigned membership status of the port entry, options include: Forbidden, Excluded Tagged or Untagged.
Apply	Click **Apply** to save the values and update the screen.

3.5.4.4 Port-VLAN Mapping

The following figure displays the **Port-VLAN Mapping Table** settings.

To access this page, click **L2 Switching > 802.1Q VLAN > Port-VLAN Mapping**.

Port-VLAN Mapping Table

Port	Mode	Administrative VLANs	Operational VLANs
GE1	Hybrid	1UP	1UP
GE2	Hybrid	1UP	1UP
GE3	Hybrid	1UP	1UP
GE4	Hybrid	1UP	1UP
GE5	Hybrid	1UP	1UP
GE6	Hybrid	1UP	1UP
GE7	Hybrid	1UP	1UP
GE8	Hybrid	1UP	1UP
TGE1	Hybrid	1UP	1UP
TGE2	Hybrid	1UP	1UP
TGE3	Hybrid	1UP	1UP
TGE4	Hybrid	1UP	1UP
Trunk1	Hybrid	1UP	1UP
Trunk2	Hybrid	1UP	1UP
Trunk3	Hybrid	1UP	1UP
Trunk4	Hybrid	1UP	1UP
Trunk5	Hybrid	1UP	1UP
Trunk6	Hybrid	1UP	1UP
Trunk7	Hybrid	1UP	1UP
Trunk8	Hybrid	1UP	1UP

Figure 3.49 L2 Switching > 802.1Q VLAN > Port-VLAN Mapping

3.5.4.5 VLAN Interface Management

The VLAN Interface Management page allows you to create a Layer 3 interface on an existing VLAN, so that the VLAN can be given its own IP address and take part in routing. The lower table lists the VLAN interfaces that are already defined and allows you to remove them.

The following figure displays the **VLAN Interface Creation** settings.

To access this page, click **L2 Switching > 802.1Q VLAN > VLAN Interface Management**.



Figure 3.50 L2 Switching > 802.1Q VLAN > VLAN Interface Management

The following figure displays the **VLAN Interface Status** settings.



Figure 3.51 L2 Switching > 802.1Q VLAN > VLAN Interface Status

3.5.5 802.3az EEE

The 802.3az Energy Efficient Ethernet (EEE) innovative green feature reduces energy consumption through intelligent functionality:

- Traffic detection — Energy Efficient Ethernet (EEE) compliance
- Inactive link detection

Inactive link detection function automatically reduces power usage when inactive links or devices are detected.

To access this page, click **L2 Switching > 802.3az EEE**.

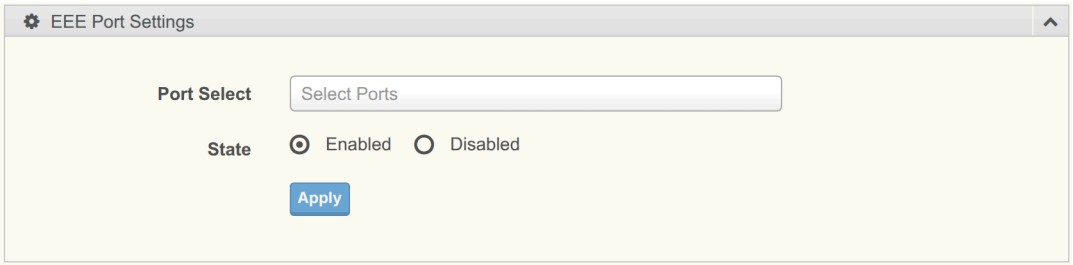


Figure 3.52 L2 Switching > 802.3az EEE

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port to setup the EEE function.
State	Click **Enabled** or **Disabled** to set the state mode of the port select setting.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **EEE Port Status** settings.

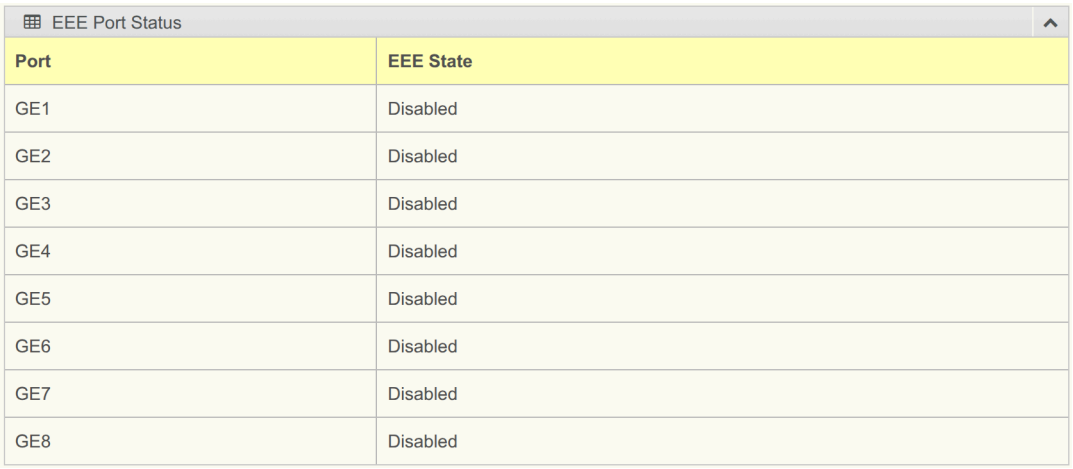


Figure 3.53 L2 Switching > EEE Port Status

3.5.6 Multicast

Multicast forwarding allows a single packet to be forwarded to multiple destinations. The service is based on L2 switch receiving a single packet addressed to a specific

Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

3.5.6.1 Unknown Multicast

The Unknown Multicast menu allows you to define how the switch treats multicast traffic for groups that are not present in the multicast forwarding table, and how dynamically learned router ports are aged out.

Multicast Filtering

The Multicast Filtering page allows for the definition of action settings when an unknown multicast request is received. The options include: Drop, Flood, or Router Port.

To access this page, click **L2 Switching > Multicast > Unknown Multicast > Multicast Filtering**.

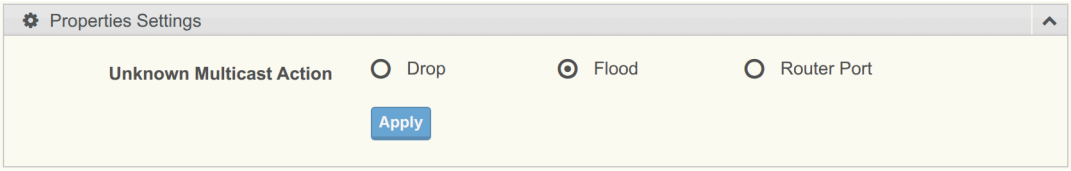


Figure 3.54 L2 Switching > Multicast > Unknown Multicast > Multicast Filtering

The following table describes the items in the previous figure.

Item	Description
Unknown Multicast Action	Select the configuration protocol: Drop, Flood, or Router Port, to apply for any unknown multicast event.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Properties Information** settings.

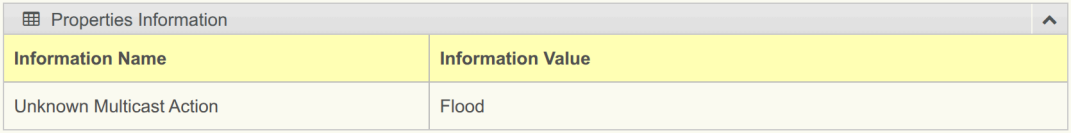


Figure 3.55 L2 Switching > Multicast > Unknown Multicast > Properties Information

Flood Settings

The Flood Settings page allows you to override the global unknown multicast action on a per-VLAN basis. A VLAN that is not listed follows the system setting defined on the Multicast Filtering page.

To access this page, click **L2 Switching > Multicast > Unknown Multicast > Flood Settings**.

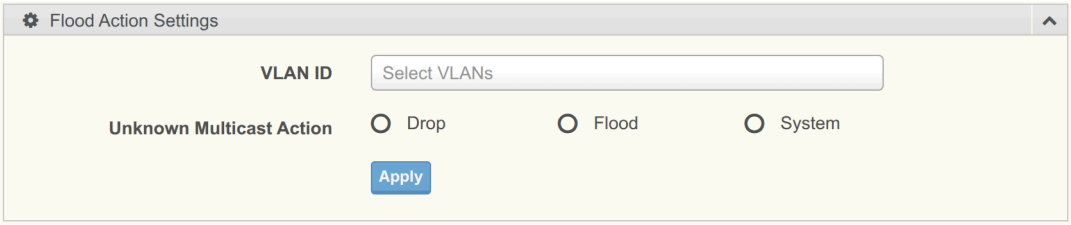


Figure 3.56 L2 Switching > Multicast > Unknown Multicast > Flood Settings

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Enter a value to specify the VLAN to which the action applies, ranging from 1 to 4094.

Item	Description
Unknown Multicast Action	Click the radio button to select the action applied to the designated VLAN: ■ Drop: Discard the unknown multicast traffic in this VLAN. ■ Flood: Forward the unknown multicast traffic to all ports in this VLAN. ■ System: Follow the global setting defined on the Unknown Multicast page.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Flood Action Information** settings.

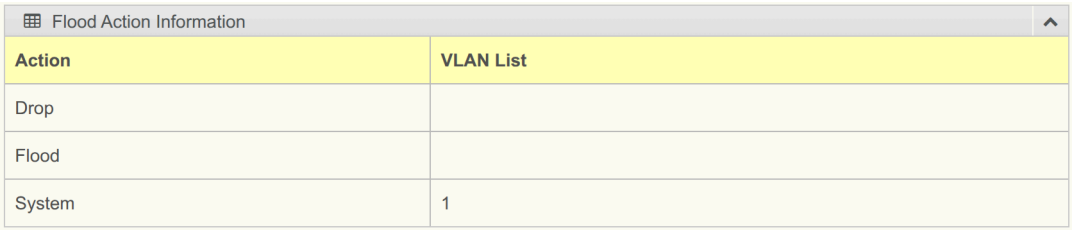


Figure 3.57 L2 Switching > Multicast > Unknown Multicast > Flood Action Information

Router-Port Settings

The Router-Port Settings page allows you to define how a dynamically learned multicast router port is aged out once the upstream router stops sending traffic.

To access this page, click **L2 Switching > Multicast > Unknown Multicast > Router-Port Settings**.

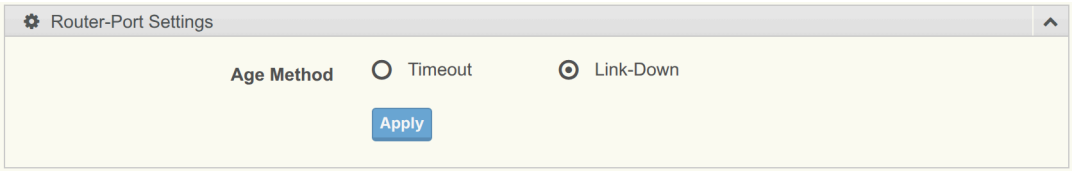


Figure 3.58 L2 Switching > Multicast > Unknown Multicast > Router-Port Settings

The following table describes the items in the previous figure.

Item	Description
Age Method	Click the radio button to select the condition that ages out a dynamic router port: ■ Timeout: Age the port out after the configured timeout expires. ■ Link-Down: Age the port out as soon as the link goes down.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Router-Port Information** settings.

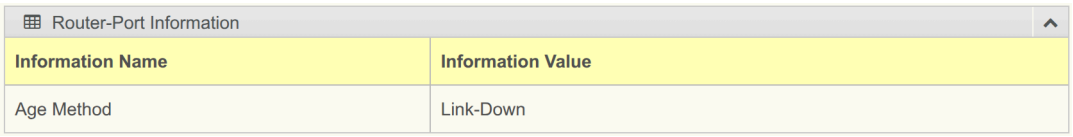


Figure 3.59 L2 Switching > Multicast > Unknown Multicast > Router-Port Information

3.5.6.2 IGMP Snooping

IGMP Snooping is defined as the process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP Snooping allows a network switch to listen in on the IGMP conversation between hosts and routers and maintain a map of which

links need which IP multicast streams. Multicasts can be filtered from the links which do not need them in turn controlling which ports receive specific multicast traffic.

IGMP Settings

To access this page, click **L2 Switching > Multicast > IGMP Snooping > IGMP Settings**.

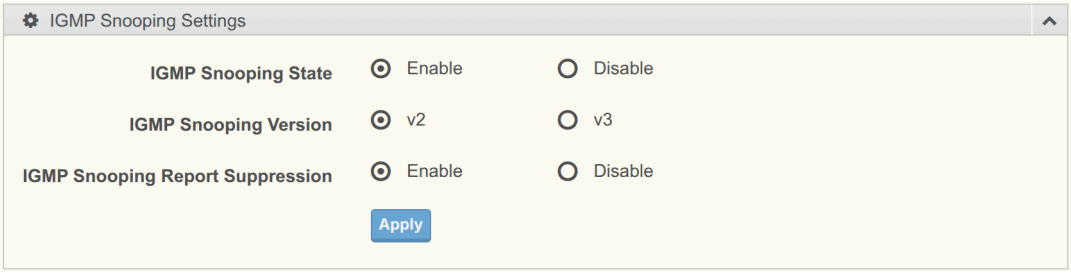


Figure 3.60 L2 Switching > Multicast > IGMP Snooping > IGMP Settings

The following table describes the items in the previous figure.

Item	Description
IGMP Snooping State	Select **Enable** or **Disable** to designate the IGMP Snooping State.
IGMP Snooping Version	Select designate the IGMP Snooping Version: V2 or V3.
IGMP Snooping Report Suppression	Select **Enable** or **Disable** to setup the report suppression for IGMP Snooping.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **IGMP Snooping Information** settings.

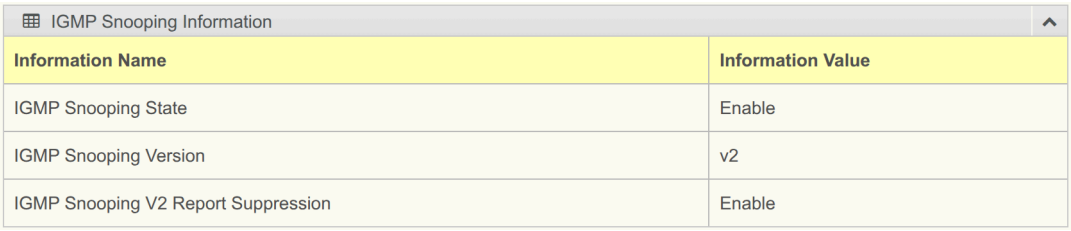


Figure 3.61 L2 Switching > Multicast > IGMP Snooping > IGMP Snooping Information

The following figure displays the **IGMP Snooping Table** settings.

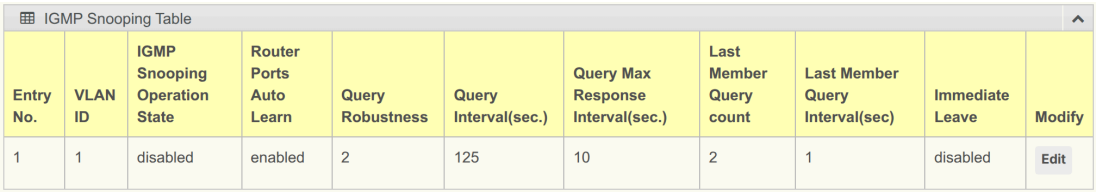


Figure 3.62 L2 Switching > Multicast > IGMP Snooping > IGMP Snooping Table

The following figure displays the dialog that opens when **Edit** is clicked.

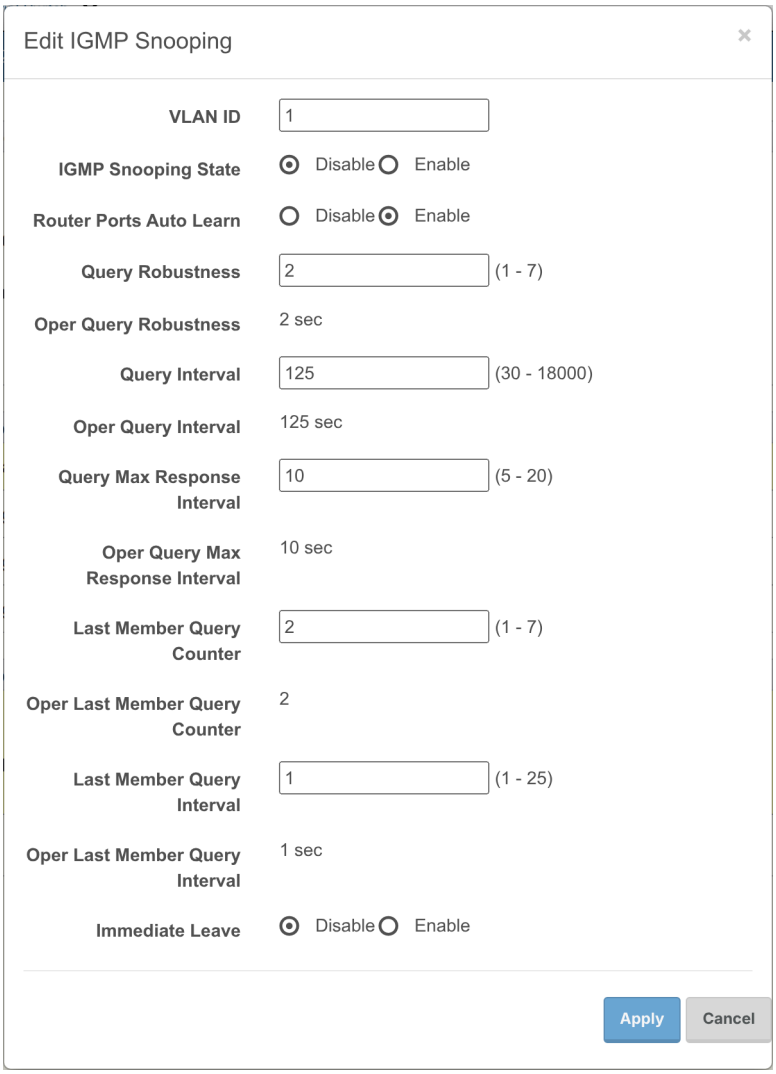


Figure 3.63 L2 Switching > Multicast > IGMP Snooping > IGMP Settings > Edit IGMP Snooping

IGMP Querier

IGMP Querier allows snooping to function by creating the tables for snooping. General queries must be unconditionally forwarded by all switches involved in IGMP snooping.

To access this page, click **L2 Switching > Multicast > IGMP Snooping > IGMP Querier**.

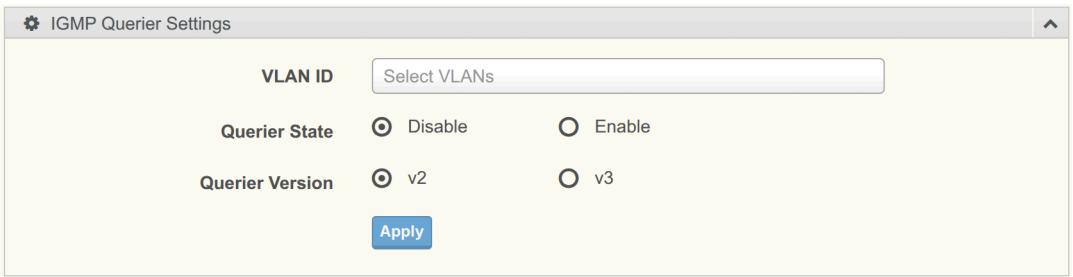


Figure 3.64 L2 Switching > Multicast > IGMP Snooping > IGMP Querier

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Select the VLAN ID to define the local IGMP querier.

Item	Description
Querier State	Select **Disable** or **Enable** to configure the VLAN ID (IGMP Querier).
Querier Version	Select the querier version (V2 or V3) designated to the selected VLAN ID.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **IGMP Querier Status** settings.



Figure 3.65 L2 Switching > Multicast > IGMP Snooping > IGMP Querier Status

IGMP Static Groups

To access this page, click **L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups**.

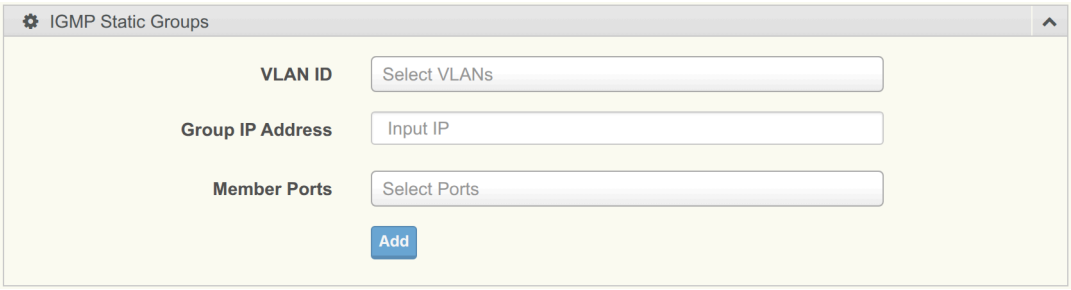


Figure 3.66 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Select the VLAN ID to define IGMP static group.
Group IP Address	Enter the IP address assigned to the VLAN ID.
Member Ports	Enter the port numbers to associate with the static group.
Add	Click **Add** to add an IGMP group.

The following figure displays the **IGMP Static Groups Status** settings.



Figure 3.67 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups Status

The following figure displays the dialog that opens when **Edit** is clicked.

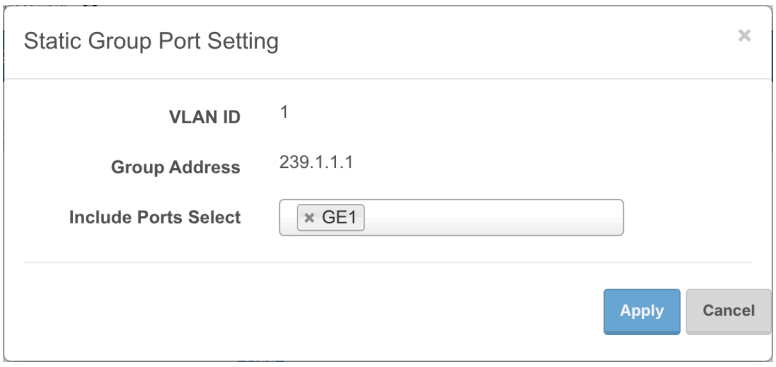


Figure 3.68 L2 Switching > Multicast > IGMP Snooping > IGMP Static Groups > Static Group Port Setting

Multicast Groups

The following figure displays the **Multicast Groups** settings.

To access this page, click **L2 Switching > Multicast > IGMP Snooping > Multicast Groups**.

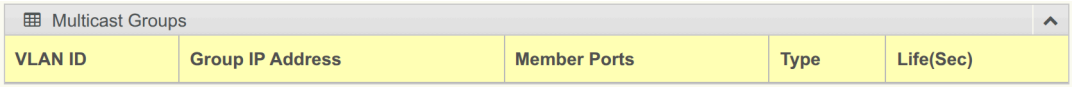


Figure 3.69 L2 Switching > Multicast > IGMP Snooping > Multicast Groups

Router Ports

The following figure displays the **Router Ports** settings.

To access this page, click **L2 Switching > Multicast > IGMP Snooping > Router Ports**.

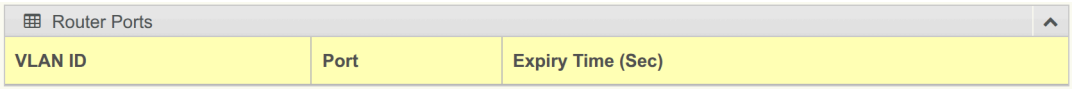


Figure 3.70 L2 Switching > Multicast > IGMP Snooping > Router Ports

3.5.6.3 MLD Snooping

The MLD Snooping page allows you to select the snooping status (enable or disable), the version (v1 or v2) and the enabling/disabling of the report suppression for the MLD querier, which sends out periodic general MLD queries and are forwarded through all ports in the VLAN.

MLD Settings

To access this page, click **L2 Switching > Multicast > MLD Snooping > MLD Settings**.



Figure 3.71 L2 Switching > Multicast > MLD Snooping > MLD Settings

The following table describes the items in the previous figure.

Item	Description
MLD Snooping State	Select **Enable** or **Disable** to setup the MLD Snooping State.

Item	Description
MLD Snooping Version	Select the querier version (V1 or V2) designated to the MLD Snooping Version.
MLD Snooping Report Suppression	Select **Enable** or **Disable** to designate the status of the report suppression.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **MLD Snooping Information** settings.



Figure 3.72 L2 Switching > Multicast > MLD Snooping > MLD Snooping Information

The following figure displays the **MLD Snooping Table** settings.

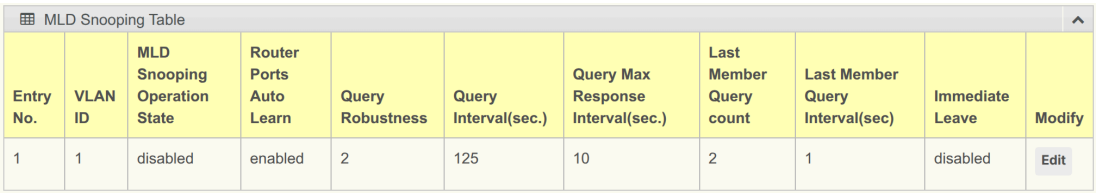


Figure 3.73 L2 Switching > Multicast > MLD Snooping > MLD Snooping Table

The following figure displays the dialog that opens when **Edit** is clicked.

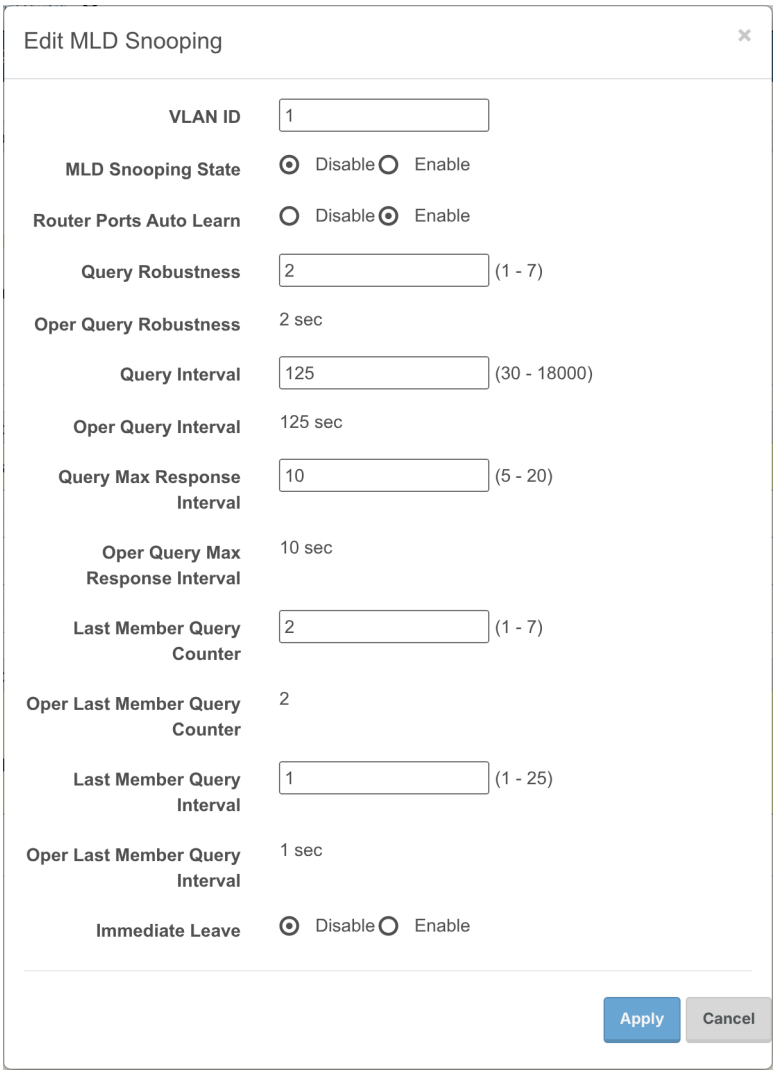


Figure 3.74 L2 Switching > Multicast > MLD Snooping > MLD Settings > Edit MLD Snooping

MLD Querier

The MLD Querier page allows you to select and enable/disable the MLD querier and define the version (MLDv1 or MLDv2) when enabled.

To access this page, click **L2 Switching > Multicast > MLD Snooping > MLD Querier**.

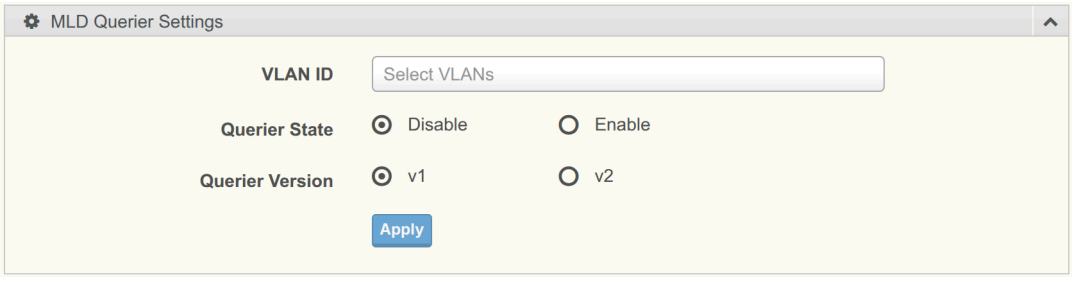


Figure 3.75 L2 Switching > Multicast > MLD Snooping > MLD Querier

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Enter the VLAN ID to configure.

Item	Description
Querier State	Select **Enable** or **Disable** status on the selected VLAN. ■ Enable: Enable IGMP Querier Election. ■ Disable: Disable IGMP Querier Election.
Querier Version	Select the querier version (IGMPV1 or IGMPV2) designated to the MLD Querier function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **MLD Querier Status** settings.



Figure 3.76 L2 Switching > Multicast > MLD Snooping > MLD Querier Status

MLD Static Groups

The MLD Static Group page allows you to configure specified ports as static member ports.

To access this page, click **L2 Switching > Multicast > MLD Snooping > MLD Static Groups**.

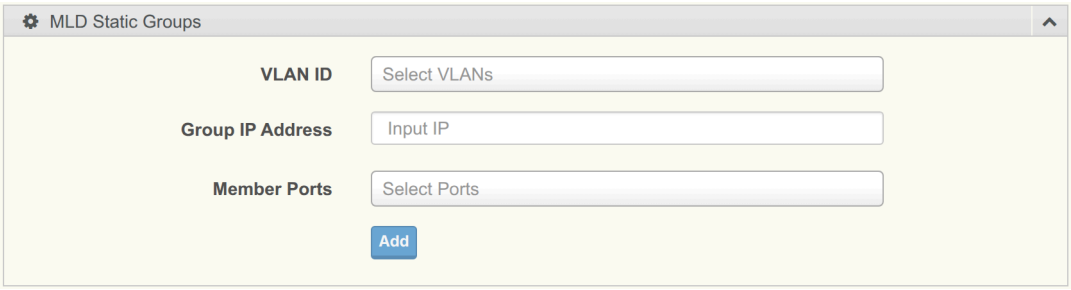


Figure 3.77 L2 Switching > Multicast > MLD Snooping > MLD Static Groups

The following table describes the items in the previous figure.

Item	Description
VLAN ID	Enter the VLAN ID to define the local MLD Static Group.
Group IP Address	Enter the IP address associated with the static group.
Member Ports	Enter the ports designated with the static group.
Add	Click **Add** to add a MLD static group.

The following figure displays the **MLD Static Groups Status** settings.



Figure 3.78 L2 Switching > Multicast > MLD Snooping > MLD Static Groups Status

The following figure displays the dialog that opens when **Edit** is clicked.

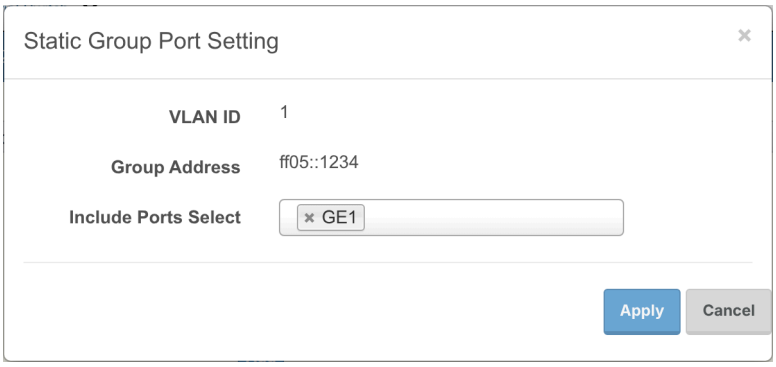


Figure 3.79 L2 Switching > Multicast > MLD Snooping > MLD Static Groups > Static Group Port Setting

Multicast Groups

The following figure displays the **Multicast Groups** settings.

To access this page, click **L2 Switching > Multicast > MLD Snooping > Multicast Groups**.

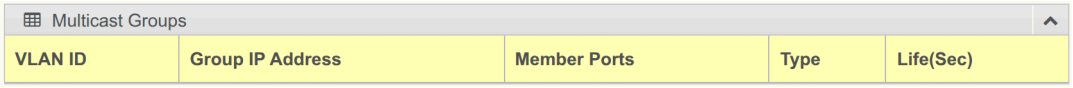


Figure 3.80 L2 Switching > Multicast > MLD Snooping > Multicast Groups

Router Ports

The following figure displays the **Router Ports** settings.

To access this page, click **L2 Switching > Multicast > MLD Snooping > Router Ports**.

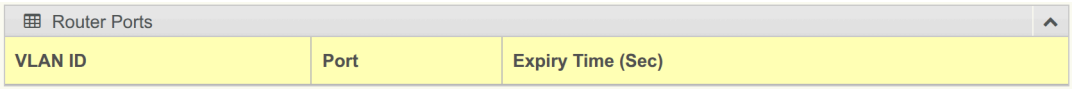


Figure 3.81 L2 Switching > Multicast > MLD Snooping > Router Ports

3.5.7 Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size of 1518 bytes. The Jumbo Frame function allows the configuration of Ethernet frame size.

To access this page, click **L2 Switching > Jumbo Frame**.



Figure 3.82 L2 Switching > Jumbo Frame

The following table describes the items in the previous figure.

Item	Description
Jumbo Frame (Bytes)	Enter the variable in bytes (1518 to 12288) to define the jumbo frame size.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Jumbo Frame Config** settings.

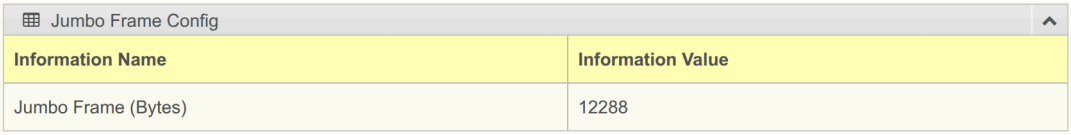


Figure 3.83 L2 Switching > Jumbo Frame Config

3.5.8 Spanning Tree

The Spanning Tree Protocol (STP) is a network protocol to ensure loop-free topology for any bridged Ethernet local area network.

3.5.8.1 Global Settings

The STP Global Settings page allows you to set the STP status, select the configuration for a BPDU packet, choose the path overhead, force version and set the configuration revision range.

To access this page, click **L2 Switching > Spanning Tree > Global Settings**.

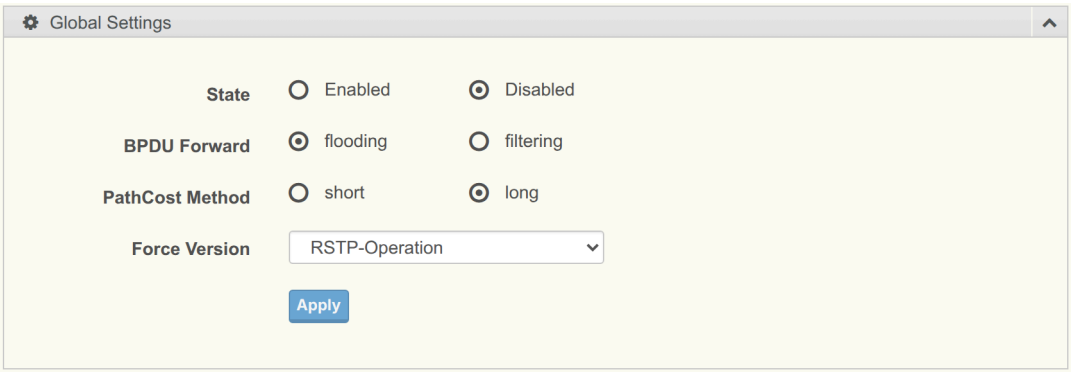


Figure 3.84 L2 Switching > Spanning Tree > Global Settings

The following table describes the items in the previous figure.

Item	Description
Enabled	Click the radio-button to enable or disable the STP status.
BPDU Forward	Select **flooding** or **filtering** to designate the type of BPDU packet.
PathCost Method	Select short or long to define the method of used for path cost calculations.
Force Version	Click the drop-down menu to select the operating mode for STP. ■ STP-Compatible: 802.1D STP operation. ■ RSTP-Operation: 802.1w operation. ■ MSTP-Operation: 802.1s operation.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **STP Information** settings.

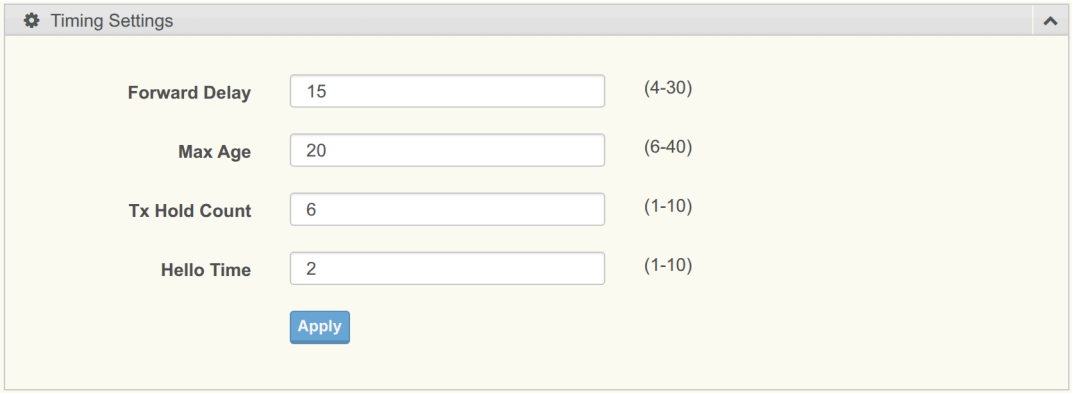
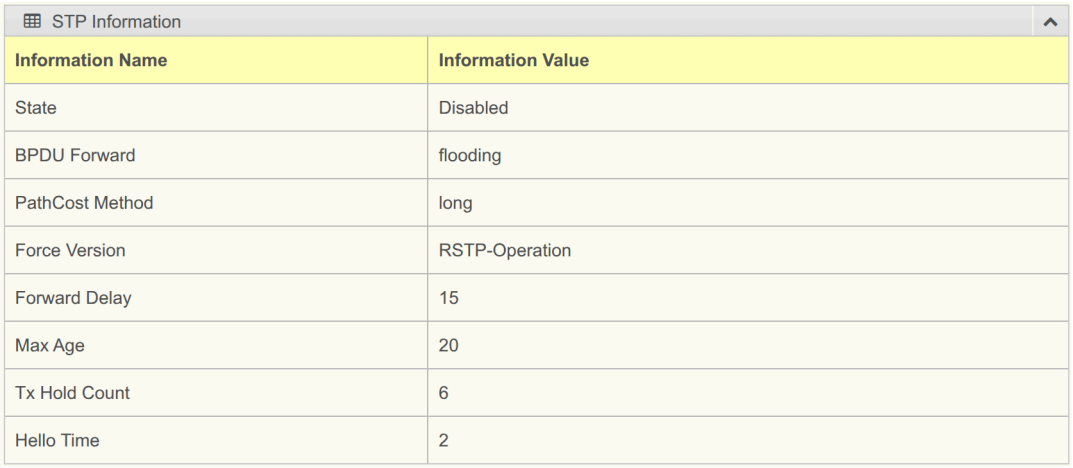


Figure 3.85 L2 Switching > Spanning Tree > Timing Settings

The following figure displays the **STP Information** settings.



Information Name	Information Value
State	Disabled
BPDU Forward	flooding
PathCost Method	long
Force Version	RSTP-Operation
Forward Delay	15
Max Age	20
Tx Hold Count	6
Hello Time	2

Figure 3.86 L2 Switching > Spanning Tree > STP Information

3.5.8.2 Port Settings

The STP Port Settings page allows you to configure the ports for the setting, port's contribution, configure edge port, and set the status of the BPDU filter.

To access this page, click **L2 Switching > Spanning Tree > Port Settings**.

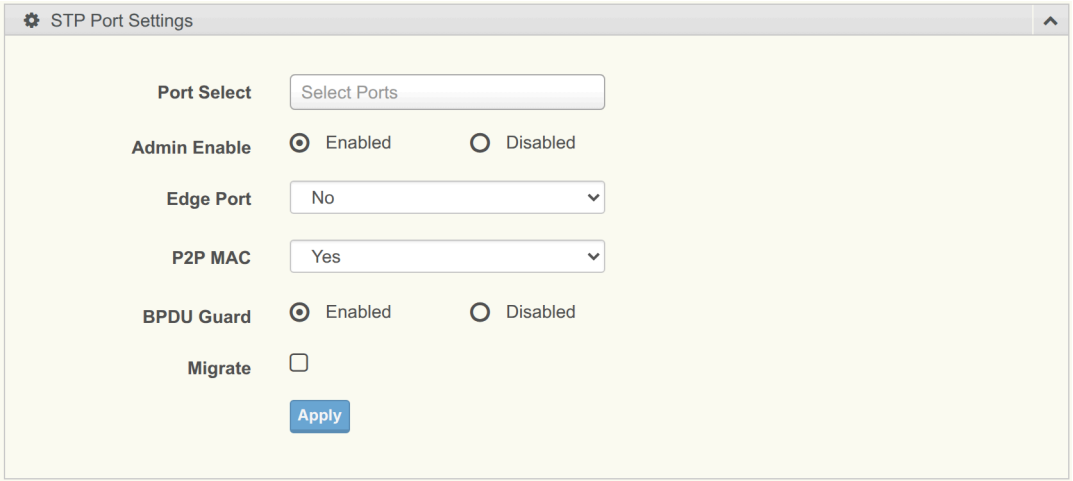


Figure 3.87 L2 Switching > Spanning Tree > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select the port list to specify the ports that apply to this setting.

Item	Description
Admin Enable	Select **Enabled** or **Disabled** to setup the admin profile for the STP port.
Edge Port	Click the drop-down menu to set the edge port configuration. ■ No: Force to false state (as link to a bridge). ■ Yes: Force to true state (as link to a host).
P2P MAC	Click the drop-down menu to set the Point-to-Point port configuration. ■ No: Force to false state. ■ Yes: Force to true state.
BPDU Guard	Select **Enabled** or **Disabled** to setup the BPDU guard. When the function is enabled, an edge port that receives a BPDU packet is disabled.
Migrate	Click the check box to enable the migrate function. Forces the port to use the new MST/RST BPDUs, requiring the switch to test on the LAN segment. for the presence of legacy devices, which are not able to understand the new BPDU formats.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **STP Port Status** settings.

STP Port Status

Port	Admin Enable	Edge Port	P2P MAC	BPDU Guard
GE1	Enable	No	No	Disable
GE2	Enable	No	No	Disable
GE3	Enable	No	No	Disable
GE4	Enable	No	No	Disable
GE5	Enable	No	No	Disable
GE6	Enable	No	No	Disable
GE7	Enable	No	No	Disable
GE8	Enable	No	No	Disable
TGE1	Enable	No	No	Disable
TGE2	Enable	No	No	Disable
TGE3	Enable	No	No	Disable
TGE4	Enable	No	No	Disable
Trunk1	Enable	No	No	Disable
Trunk2	Enable	No	No	Disable
Trunk3	Enable	No	No	Disable
Trunk4	Enable	No	No	Disable
Trunk5	Enable	No	No	Disable
Trunk6	Enable	No	No	Disable
Trunk7	Enable	No	No	Disable
Trunk8	Enable	No	No	Disable

Figure 3.88 L2 Switching > Spanning Tree > STP Port Status

3.5.8.3 Bridge Settings

The STP Bridge Settings page allows you to configure the priority, forward delay, maximum age, Tx hold count, and the hello time for the bridge.

To access this page, click **L2 Switching > Spanning Tree > Bridge Settings**.



Figure 3.89 L2 Switching > Spanning Tree > Bridge Settings

The following table describes the items in the previous figure.

Item	Description
Priority	Click the drop-down menu to select the STP bridge priority.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Bridge Status** settings.

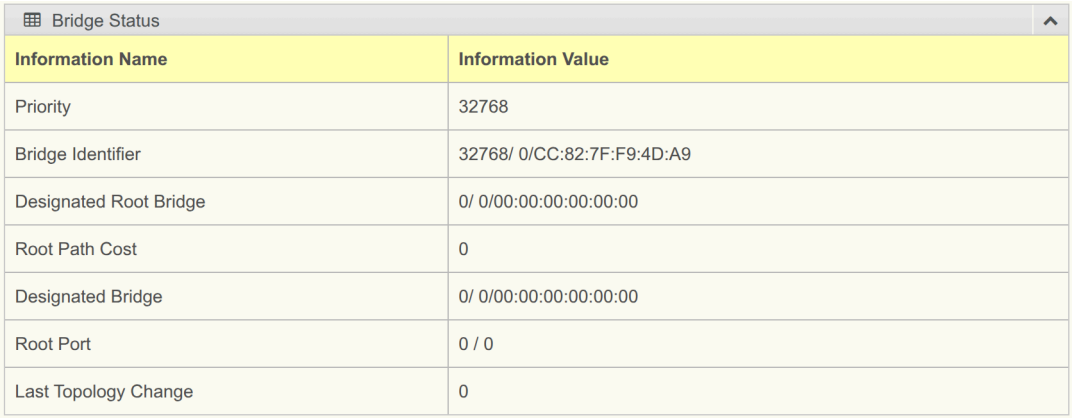


Figure 3.90 L2 Switching > Spanning Tree > Bridge Status

3.5.8.4 Advanced Port Settings

The STP Port Advanced Settings page allows you to select the port list to apply this setting.

To access this page, click **L2 Switching > Spanning Tree > Advanced Port Settings**.

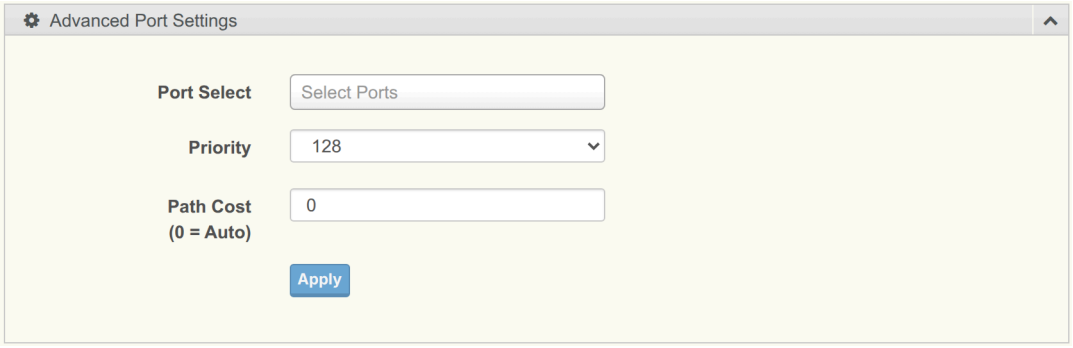


Figure 3.91 L2 Switching > Spanning Tree > Advanced Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Select the port to designate the STP settings.
Priority	Click the drop-down menu to designate a priority.
Path Cost(0 = Auto)	Set the port's cost contribution. For a root port, the root path cost for the bridge. (0 means Auto).

Item	Description
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **STP Port Status** settings.

STP Port Status

Port	Identifier (Priority / Port Id)	Path Cost Conf/Oper	Designated Root Bridge	Root Path Cost	Designated Bridge	Edge Port Conf/Oper	P2P MAC Conf/Oper	Port Role	Port State
GE1	128 / 1	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
GE2	128 / 2	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
GE3	128 / 3	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
GE4	128 / 4	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
GE5	128 / 5	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
GE6	128 / 6	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
GE7	128 / 7	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / Yes	Disabled	Forwarding
GE8	128 / 8	0 / 20000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
TGE1	128 / 9	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
TGE2	128 / 10	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
TGE3	128 / 11	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
TGE4	128 / 12	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
Trunk1	128 / 13	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
Trunk2	128 / 14	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
Trunk3	128 / 15	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
Trunk4	128 / 16	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
Trunk5	128 / 17	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
Trunk6	128 / 18	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
Trunk7	128 / 19	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled
Trunk8	128 / 20	0 / 2000	0 / 00:00:00:00:00:00	0	0 / 00:00:00:00:00:00	No / No	Auto / No	Disabled	Disabled

Figure 3.92 L2 Switching > Spanning Tree > STP Port Status

3.5.8.5 MST Config Identification

The MST Config Identification page allows you to configure the identification setting name and the identification range.

To access this page, click **L2 Switching > Spanning Tree > MST Config Identification**.

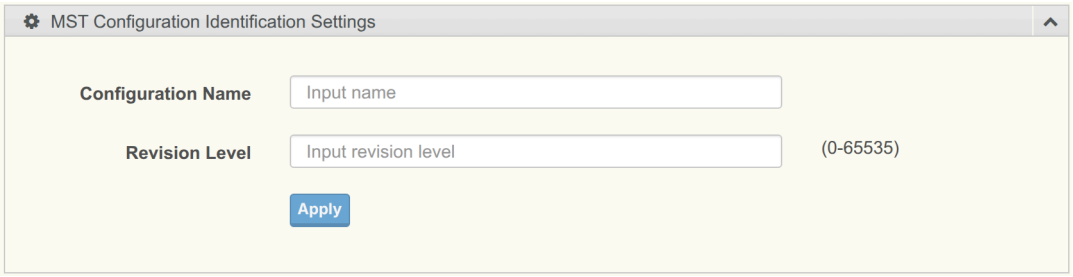


Figure 3.93 L2 Switching > Spanning Tree > MST Config Identification

The following table describes the items in the previous figure.

Item	Description
Configuration Name	Enter the identifier used to identify the configuration currently being used. It may be up to 32 characters.
Revision Level	Enter the identifier for the Revision Configuration, range: 0 to 65535 (default: 0).
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **MST Configuration Identification Information** settings.

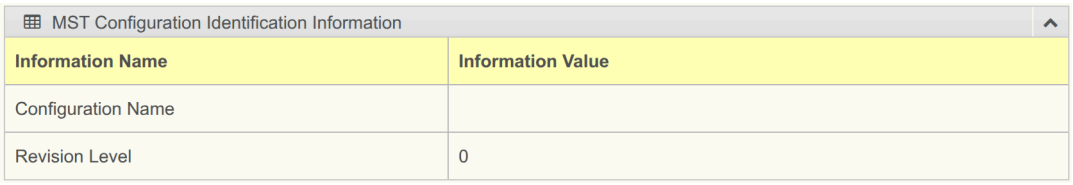


Figure 3.94 L2 Switching > Spanning Tree > MST Configuration Identification Information

3.5.8.6 MST Instance Settings

The MST Instance Priority Settings allows you to specify the MST instance and the bridge priority in that instance.

To access this page, click **L2 Switching > Spanning Tree > MST Instance Settings**.

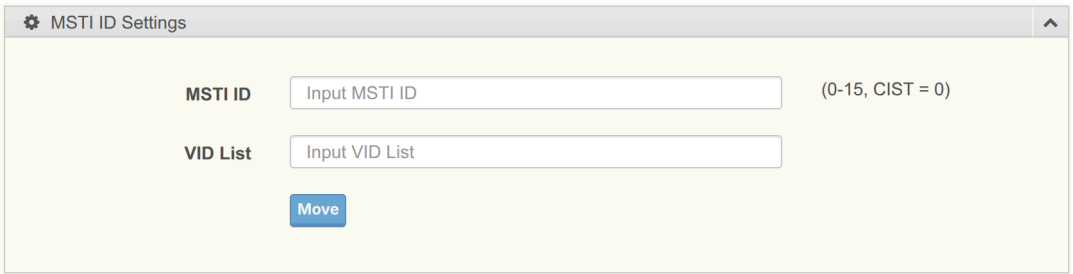


Figure 3.95 L2 Switching > Spanning Tree > MST Instance Settings

The following table describes the items in the previous figure.

Item	Description
MSTI ID	Click the drop-down menu to specify the MST instance.
VID List	Enter the VLANs to be moved into the designated MST instance. A VLAN that is not assigned to any instance belongs to the CIST.
Move	Click **Move** to assign the listed VLANs to the designated MST instance and update the screen.

The following figure displays the **MSTI ID Information** settings.

MSTI ID Information

MSTI ID	VID List
CIST	1-4094

Figure 3.96 L2 Switching > Spanning Tree > MSTI ID Information

3.5.8.7 STP Statistics

The following figure displays the **STP Statistics** settings.

To access this page, click **L2 Switching > Spanning Tree > STP Statistics**.

STP Statistics

Port	Configuration BPDUs Received	TCN BPDUs Received	Configuration BPDUs Transmitted	TCN BPDUs Transmitted
GE1	0	0	0	0
GE2	0	0	0	0
GE3	0	0	0	0
GE4	0	0	0	0
GE5	0	0	0	0
GE6	0	0	0	0
GE7	0	0	0	0
GE8	0	0	0	0
TGE1	0	0	0	0
TGE2	0	0	0	0
TGE3	0	0	0	0
TGE4	0	0	0	0
Trunk1	0	0	0	0
Trunk2	0	0	0	0
Trunk3	0	0	0	0
Trunk4	0	0	0	0
Trunk5	0	0	0	0
Trunk6	0	0	0	0
Trunk7	0	0	0	0
Trunk8	0	0	0	0

Figure 3.97 L2 Switching > Spanning Tree > STP Statistics

3.5.9 X-Ring Pro

The X-Ring Pro function provides an improvement over Spanning Tree and Rapid Spanning Tree and a rapid auto recovery in the event that the network suffers a corrupt or broken link and prevents network loops.

3.5.9.1 X-Ring Pro Settings

The X-Ring Pro Settings page allows you to configure the status (enabled or disabled) of the function.

To access this page, click **L2 Switching > X-Ring Pro > X-Ring Pro Settings**.



Figure 3.98 L2 Switching > X-Ring Pro > X-Ring Pro Settings

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the X-Ring Pro mode.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Information** settings.



Figure 3.99 L2 Switching > X-Ring Pro > Information

3.5.9.2 X-Ring Pro Groups

The X-Ring Pro Groups page allows you to select the function and role for each ring ID and its connected ports.

To access this page, click **L2 Switching > X-Ring Pro > X-Ring Pro Groups**.

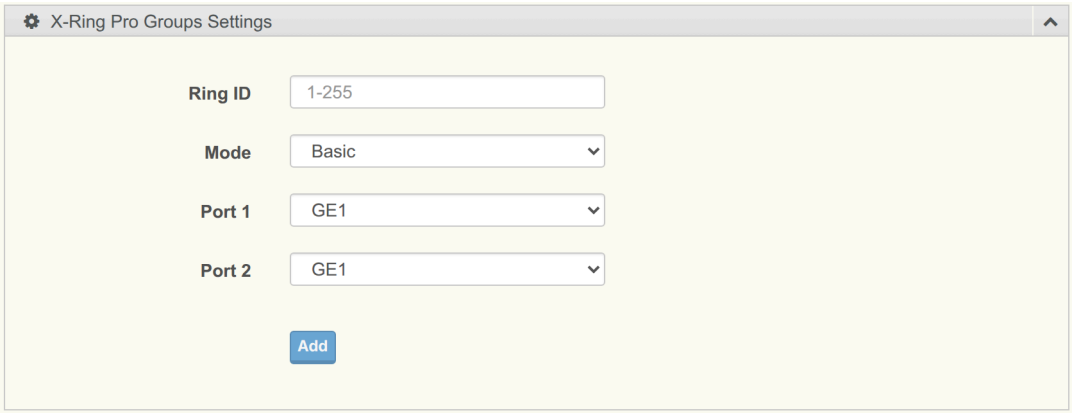


Figure 3.100 L2 Switching > X-Ring Pro > X-Ring Pro Groups

The following table describes the items in the previous figure.

Item	Description
Ring ID	Enter a number ranging from 1 to 255 to identify a given X-Ring Pro group.
Mode	Click the drop-down menu to select the topology of the group. The fields displayed below depend on the selected mode: ■ Basic: A simple ring built from two member ports. ■ Chain: A chain attached to an existing ring; the Role field designates the position of this switch in the chain. ■ Couple: Two rings joined through a single port. ■ Pair: Two rings joined through a redundant pair of ports. ■ R-Pair: A pair with the roles of the two ports reversed.

Item	Description
Role	Click the drop-down menu to select the position of the switch in a chain: Head, Member or Tail. The field is displayed in Chain mode only.
Port 1	Click the drop-down menu to define the first port of the group.
Port 2	Click the drop-down menu to define the second port of the group.
Master Ring ID	Click the drop-down menu to designate the ring to which this group is joined. The field is displayed in Couple, Pair and R-Pair modes.
detect-pair-link	Click the check box to make the switch monitor the state of the paired link. The field is displayed in Pair and R-Pair modes.
Port	Click the drop-down menu to define the port that joins the two rings. The field is displayed in Couple, Pair and R-Pair modes.
Group ID	Enter a number to identify the coupling group shared by the two switches that join the rings.
Add	Click **Add** to add the entry and update the screen.

The following figure displays the **Ring Information** settings.

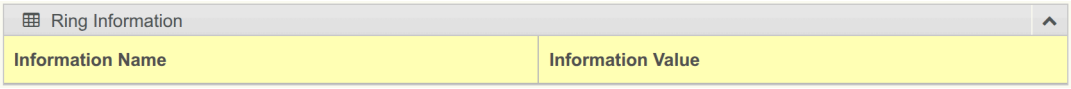


Figure 3.101 L2 Switching > X-Ring Pro > Ring Information

3.5.10 Loopback Detection

The Loopback Detection function is used to detect looped links. By sending detection frames and then checking to see if the frames returned to any port on the device, the function is used to detect loops.

3.5.10.1 Global Settings

The Global Settings page allows you to configure the state (enabled or disabled) of the function, select the interval at which frames are transmitted and the delay before recovery.

To access this page, click **L2 Switching > Loopback Detection > Global Settings**.

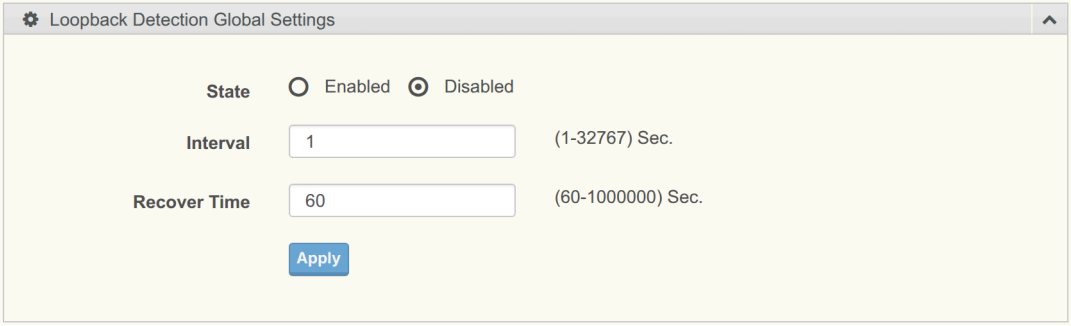


Figure 3.102 L2 Switching > Loopback Detection > Global Settings

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the loopback mode.
Interval	Enter the variable in seconds (1 to 32767) to set the interval at which frames are transmitted.
Recover Time	Enter the variable in seconds (60 to 1000000) to define the delay before recovery.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Loopback Detection Global Information** settings.

To access this page, click **L2 Switching > Loopback Detection > Loopback Detection Global Information**.

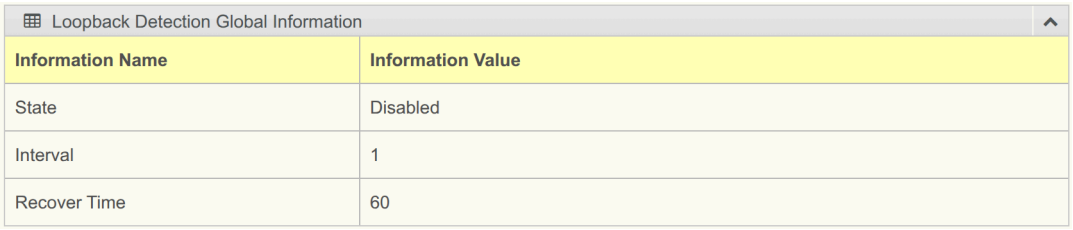


Figure 3.103 L2 Switching > Loopback Detection > Loopback Detection Global Information

3.5.10.2 Port Settings

The Port Settings page allows you to select ports that are detected by the loopback detection function and configure their status (enabled or disabled).

To access this page, click **L2 Switching > Loopback Detection > Port Settings**.

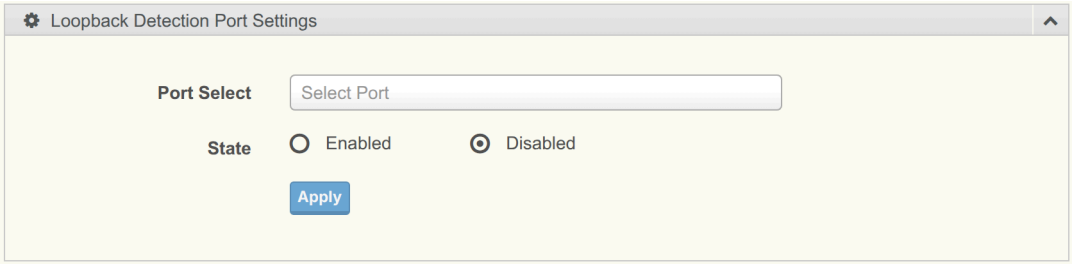


Figure 3.104 L2 Switching > Loopback Detection > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port to define the local loopback detection setting.
Enabled	Select **Enabled** or **Disabled** to setup the Loopback Detection function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Loopback Detection Port Information** settings.

Loopback Detection Port Information

Port	State	Loop Status
GE1	Disabled	Normal
GE2	Disabled	Normal
GE3	Disabled	Normal
GE4	Disabled	Normal
GE5	Disabled	Normal
GE6	Disabled	Normal
GE7	Disabled	Normal
GE8	Disabled	Normal
TGE1	Disabled	Normal
TGE2	Disabled	Normal
TGE3	Disabled	Normal
TGE4	Disabled	Normal

Figure 3.105 L2 Switching > Loopback Detection > Loopback Detection Port Information

3.6 L3 Routing

The L3 Routing menu allows you to configure the Layer 3 functions of the switch: network address translation (NAT) between VLAN interfaces, and static routes to destinations that are not directly connected.

3.6.1 NAT

The NAT menu allows you to translate addresses as traffic passes between VLAN interfaces. Source NAT (SNAT) rewrites the source address of outgoing traffic; destination NAT (DNAT) rewrites the destination address of incoming traffic. Rules are evaluated in list order, so the insert position determines precedence.

3.6.1.1 SNAT

The SNAT page allows you to rewrite the source IP address of traffic leaving a designated VLAN interface, so that hosts on an internal subnet can reach an external network through a single address.

To access this page, click **L3 Routing > NAT > SNAT**.

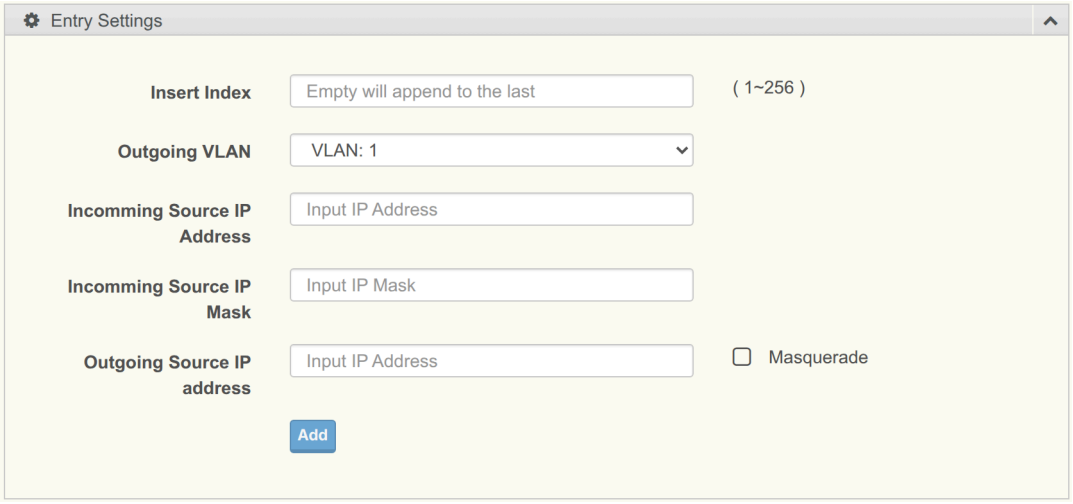


Figure 3.106 L3 Routing > NAT > SNAT

The following table describes the items in the previous figure.

Item	Description
Insert Index	Enter a value to specify the position at which the rule is inserted in the rule list, ranging from 1 to 256. Leave the field empty to append the rule to the end of the list.
Outgoing VLAN	Click the drop-down menu to select the VLAN interface through which the translated traffic leaves the switch.
Incomming Source IP Address	Enter a value to specify the source IP address to be translated.
Incomming Source IP Mask	Enter a value to specify the subnet mask applied to the source IP address, so that one rule can cover a range of hosts.
Outgoing Source IP address	Enter a value to specify the source IP address written into the outgoing traffic. The field is unavailable when Masquerad is selected.
Masquerad	Click the check box to use the IP address of the outgoing VLAN interface as the translated source address. The switch follows the interface address automatically, so no fixed address needs to be entered.
Add	Click **Add** to add the entry and update the screen.

The following figure displays the **Entry Information** settings.



Figure 3.107 L3 Routing > NAT > Entry Information

3.6.1.2 DNAT

The DNAT page allows you to rewrite the destination IP address, and optionally the destination Layer 4 port, of traffic entering a designated VLAN interface. This allows a server on an internal subnet to be reached through an address on the external side of the switch.

To access this page, click **L3 Routing > NAT > DNAT**.

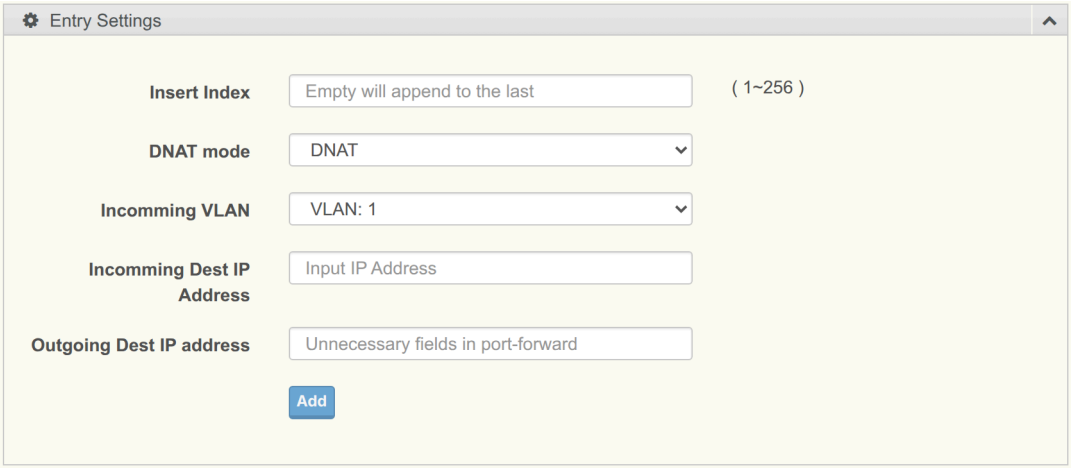


Figure 3.108 L3 Routing > NAT > DNAT

The following table describes the items in the previous figure.

Item	Description
Insert Index	Enter a value to specify the position at which the rule is inserted in the rule list, ranging from 1 to 256. Leave the field empty to append the rule to the end of the list.
DNAT mode	Click the drop-down menu to select the translation mode: ■ DNAT: Translate the destination IP address only. ■ Port Forward: Translate both the destination IP address and the destination Layer 4 port.
Incomming VLAN	Click the drop-down menu to select the VLAN interface on which the incoming traffic arrives.
Incomming Dest IP Address	Enter a value to specify the destination IP address to be translated.
IP Protocol	Click the drop-down menu to select the protocol matched by the rule: Any, TCP or UDP.
Incomming Dest L4 Port	Enter a value to specify the destination TCP or UDP port to be translated, ranging from 1 to 65535.
Outgoing Dest IP address	Enter a value to specify the destination IP address written into the forwarded traffic. The field is unnecessary in Port Forward mode.
Outgoing Dest L4 Port	Enter a value to specify the destination TCP or UDP port written into the forwarded traffic, ranging from 1 to 65535.
Add	Click **Add** to add the entry and update the screen.

The following figure displays the **Entry Information** settings.



Figure 3.109 L3 Routing > NAT > Entry Information

3.6.2 Static Route

The Static Route page allows you to define routes to destinations that are not directly connected to the switch. A static route is used when no dynamic routing protocol supplies a path to the destination.

To access this page, click **L3 Routing > Static Route**.

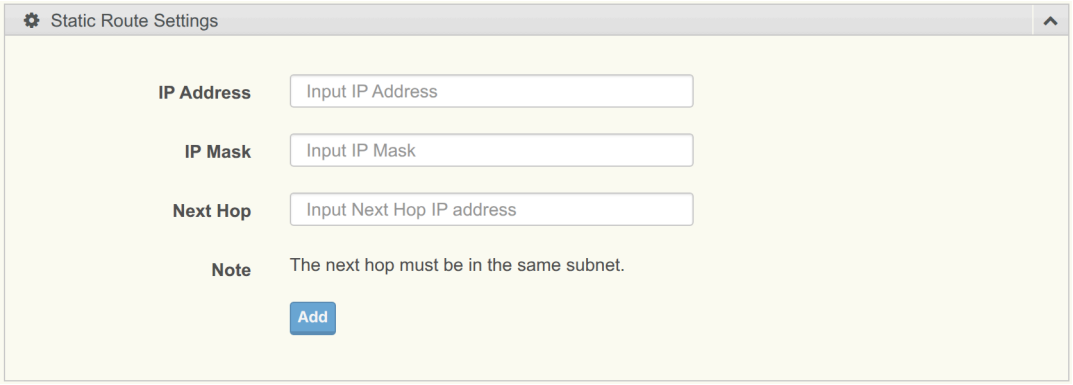


Figure 3.110 L3 Routing > Static Route

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter a value to specify the destination IP address of the route.
IP Mask	Enter a value to specify the subnet mask of the destination network.
Next Hop	Enter a value to specify the IP address of the next-hop router. The address must be reachable through one of the VLAN interfaces of the switch.
Note	A static reminder message stating that the next hop must be in the same subnet; this is not an input field.
Add	Click **Add** to add the entry and update the screen.

The following figure displays the **Static Route Config Information** settings.

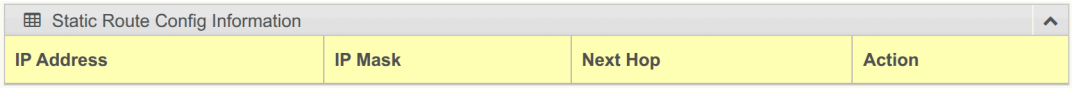


Figure 3.111 L3 Routing > Static Route Config Information

The following figure displays the **Default Route Information** settings.

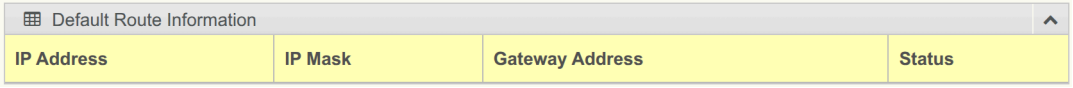


Figure 3.112 L3 Routing > Default Route Information

3.7 MAC Address Table

The MAC Address Table provides access to the Static MAC Settings, MAC Aging Time, and Dynamic Forwarding.

3.7.1 Static MAC

The Static MAC page allows you to configure the address for forwarding of packets, the VLAN ID of the listed MAC address and the designated Port.

To access this page, click **MAC Address Table > Static MAC**.

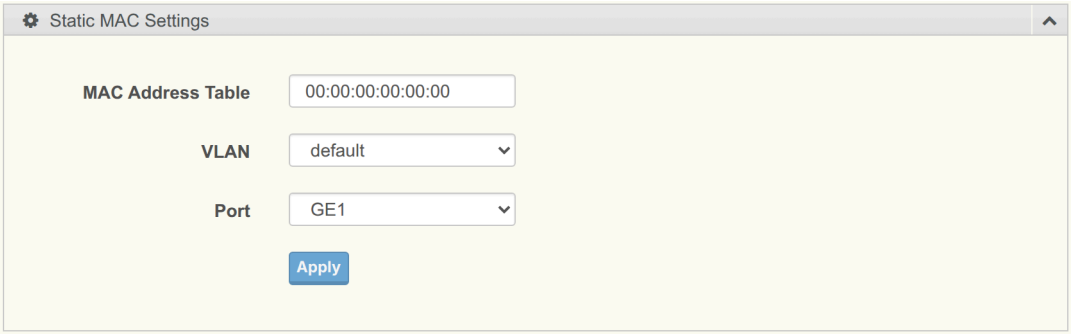


Figure 3.113 MAC Address Table > Static MAC

The following table describes the items in the previous figure.

Item	Description
MAC Address Table	Enter the MAC address to which packets are statically forwarded.
VLAN	Click the drop-down menu to select the VLAN ID number of the VLAN for which the MAC address is residing.
Port	Click the drop-down menu to select the port number.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Static MAC Status** settings.

To access this page, click **MAC Address Table > Static MAC Status**.

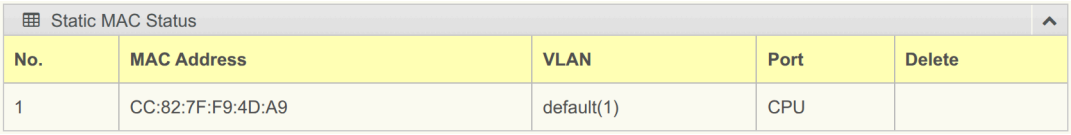


Figure 3.114 MAC Address Table > Static MAC Status

3.7.2 MAC Aging Time

The MAC Aging Time page allows you to set the MAC address of the aging time to study.

To access this page, click **MAC Address Table > MAC Aging Time**.

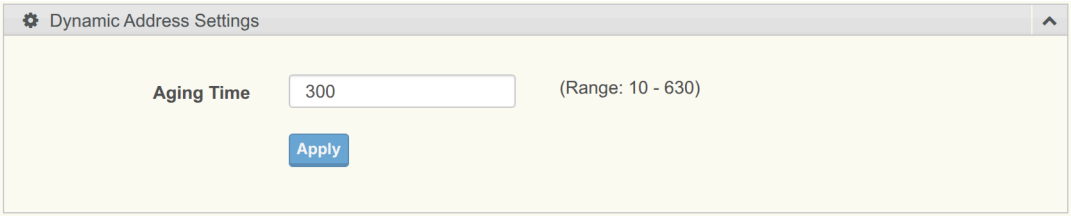


Figure 3.115 MAC Address Table > MAC Aging Time

The following table describes the items in the previous figure.

Item	Description
Aging Time	Enter the variable (10 to 630) to define the time required for aging.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Dynamic Address Status** settings.

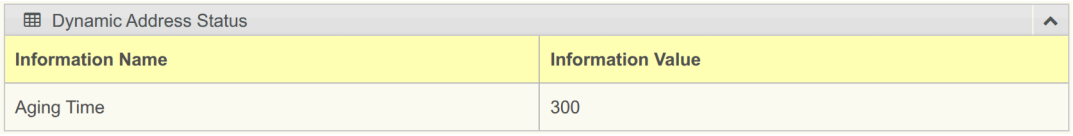


Figure 3.116 MAC Address Table > Dynamic Address Status

3.7.3 Dynamic Forwarding Table

The Dynamic Forwarding function allows you to configure an address tables, which contain the following:

- The port each hardware address is associated with
- The VLAN to show or clear dynamic MAC entries
- The MAC address selection

To access this page, click **MAC Address Table > Dynamic Forwarding Table**.

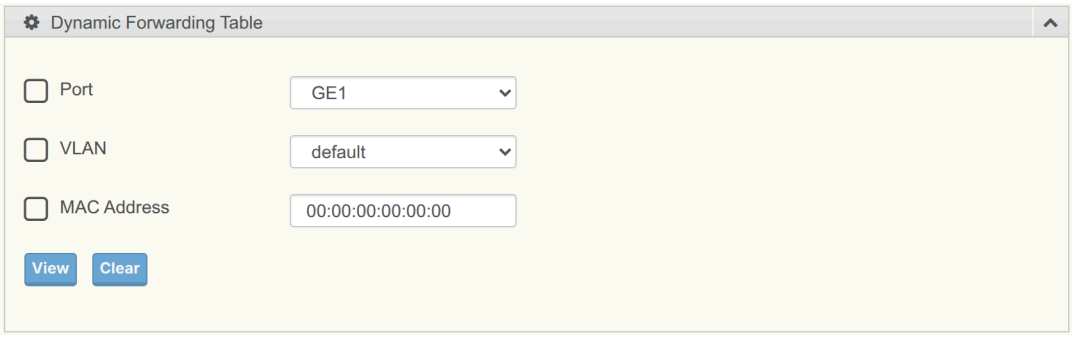


Figure 3.117 MAC Address Table > Dynamic Forwarding Table

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port number to show or clear dynamic MAC entries. If a port, VLAN or MAC address is not selected the whole dynamic MAC table is displayed or cleared.
VLAN	Click the drop-down menu to select the VLAN to show or clear dynamic MAC entries.
MAC Address	Enter the MAC address to show or clear dynamic MAC entries. If a port, VLAN or MAC address is not selected the whole dynamic MAC table is displayed or cleared.
View	Click **View** to display the MAC address information.
Clear	Click **Clear** to clear the MAC Address Information table.

The following figure displays the **MAC Address Information** settings.

To access this page, click **MAC Address Table > MAC Address Information**.

Click **Add to Static MAC** beside an entry to convert the dynamic entry into a static one.

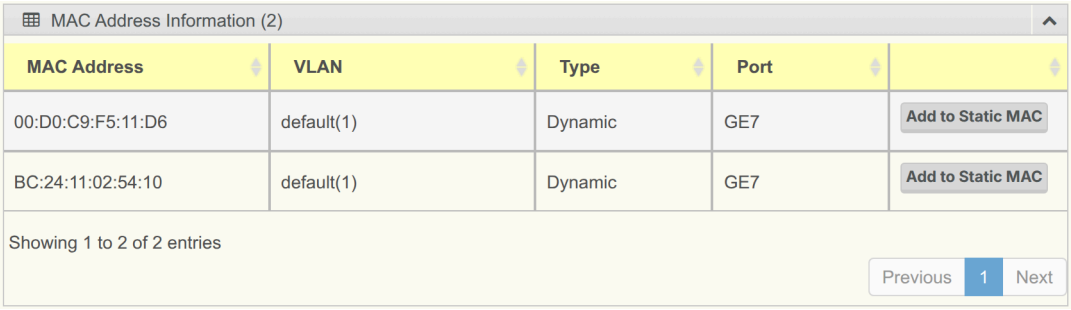


Figure 3.118 MAC Address Table > MAC Address Information

3.8 Security

The Security function allows for the configuration of Storm Control, Port Security, Protected Ports, DoS Prevention, Applications, 802.1x, and IP Security.

3.8.1 Storm Control

The Storm Control page allows you to setup the units and Preamble/IFG to manage the occurrence of packet flooding on the LAN and consequent traffic to prevent the degrading of network performance.

3.8.1.1 Global Settings

To access this page, click **Security > Storm Control > Global Settings**.

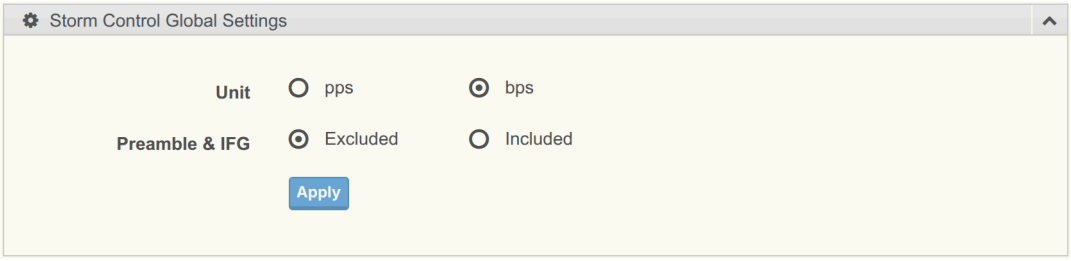


Figure 3.119 Security > Storm Control > Global Settings

The following table describes the items in the previous figure.

Item	Description
Unit	Select **pps** or **bps** control units for the Storm Control function.
Preamble & IFG	Select **Excluded** or **Included** to setup the Storm Control Global settings. ■ Excluded: exclude preamble & IFG (20 bytes) when count ingress storm control rate. ■ Included: include preamble & IFG (20 bytes) when count ingress storm control rate.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Storm Control Global Information** settings.

To access this page, click **Security > Storm Control > Storm Control Global Information**.

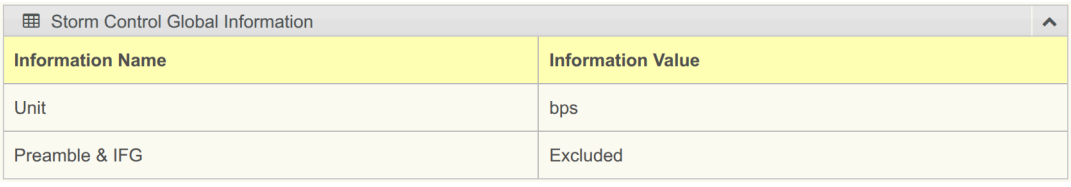


Figure 3.120 Security > Storm Control > Storm Control Global Information

3.8.1.2 Port Settings

The Port Settings page allows you to configure the port and the type of storm control association along with the value of the storm rate for the selected port.

To access this page, click **Security > Storm Control > Port Settings**.

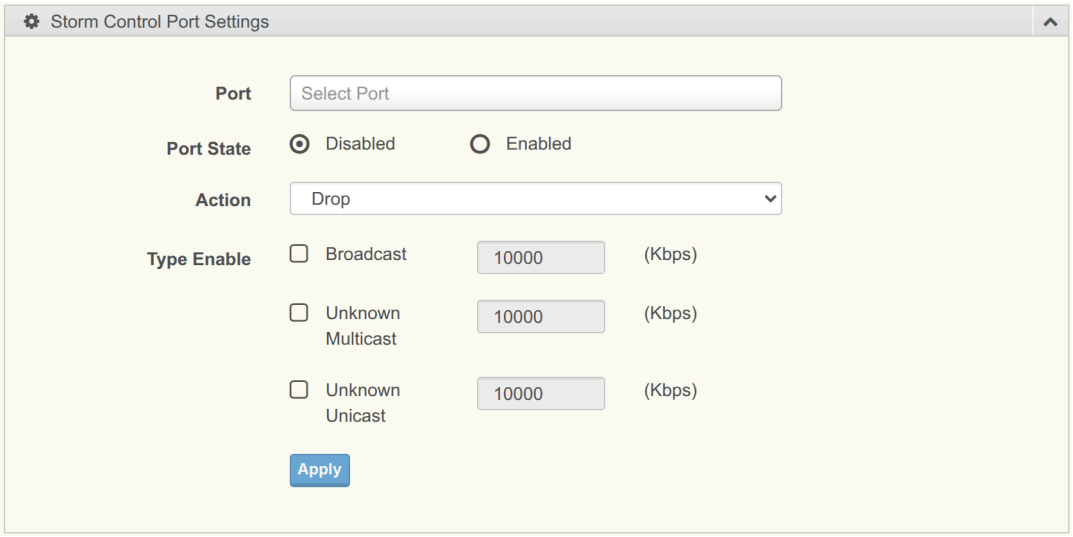


Figure 3.121 Security > Storm Control > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to designate the local port for the Storm Control function.
Port State	Select **Disabled** or **Enabled** to define the port state
Action	Click the drop-down menu to select the type of action to designate for the selected port during a Storm Control incident. The options are Drop and Shutdown.
Type Enable	Click the radio button to enable Broadcast, Unknown Multicast, or Unknown Unicast. ■ Broadcast: Select the variable in Kbps to define the broadcast bandwidth. ■ Unknown Multicast: Select the variable in Kbps to define the unknown multicast setting. ■ Unknown Unicast: Select the variable in Kbps to define the unknown unicast setting.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Storm Control Port Information** settings.

Storm Control Port Information

Port	Port State	Broadcast (Kbps)	Unknown Multicast (Kbps)	Unknown Unicast (Kbps)	Action
GE1	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE2	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE3	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE4	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE5	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE6	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE7	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
GE8	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
TGE1	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
TGE2	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
TGE3	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop
TGE4	Disabled	Off (10000)	Off (10000)	Off (10000)	Drop

Figure 3.122 Security > Storm Control > Storm Control Port Information

3.8.2 Port Security

The Port Security page allows you to configure port isolation behavior.

To access this page, click **Security > Port Security**.

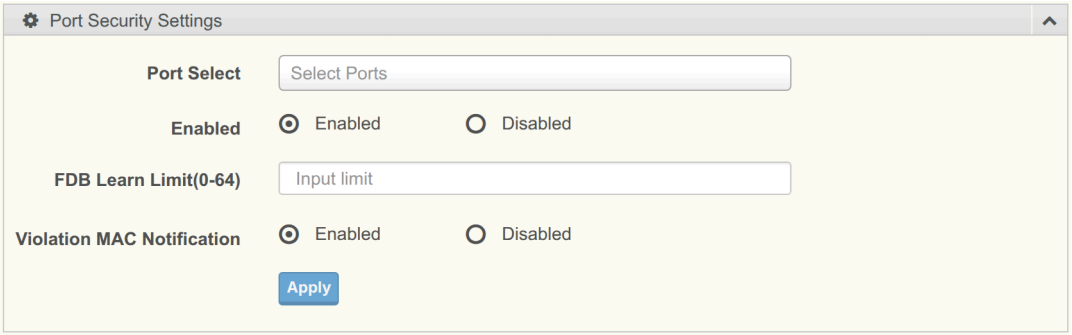


Figure 3.123 Security > Port Security

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter a single or multiple port numbers to configure.
Enabled	Select **Enabled** or **Disabled** to define the selected Port.
FDB Learn Limit (0-64)	Enter the variable (0 to 64) to set the learn limit for the FDB setting.
Violation MAC Notification	Select **Enabled** or **Disabled** to define the selected Port.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Port Security Information** settings.

Port Security Information

Port	Enabled	FDB Learn Limit	Violation MAC Notification
GE1	Disabled	0	Disabled
GE2	Disabled	0	Disabled
GE3	Disabled	0	Disabled
GE4	Disabled	0	Disabled
GE5	Disabled	0	Disabled
GE6	Disabled	0	Disabled
GE7	Disabled	0	Disabled
GE8	Disabled	0	Disabled
TGE1	Disabled	0	Disabled
TGE2	Disabled	0	Disabled
TGE3	Disabled	0	Disabled
TGE4	Disabled	0	Disabled

Figure 3.124 Security > Port Security Information

3.8.3 Protected Ports

The Protected Port page allows you to configure a single or multiple ports as a protected or unprotected type.

To access this page, click **Security > Protected Ports**.

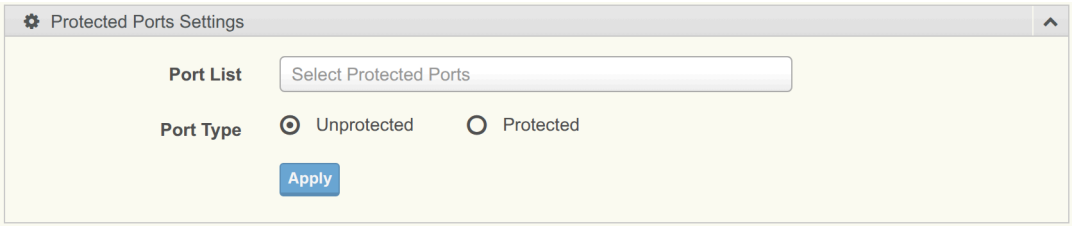


Figure 3.125 Security > Protected Ports

The following table describes the items in the previous figure.

Item	Description
Port List	Enter the port number to designate for the Protected Port setting.
Port Type	Select **Unprotected** or **Protected** to define the port type.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Protected Ports Status** settings.

Protected Ports Status

Protected Type	Port List
Protected Ports	
Unprotected Ports	all

Figure 3.126 Security > Protected Ports Status

3.8.4 DoS Prevention

The DoS Prevention page allows you to setup (enabled or disabled) the denial of service.

3.8.4.1 DoS Global Settings

The DoS Global Settings page allows you to configure (enabled or disabled) the setting for each function.

To access this page, click **Security > DoS Prevention > DoS Global Settings**.

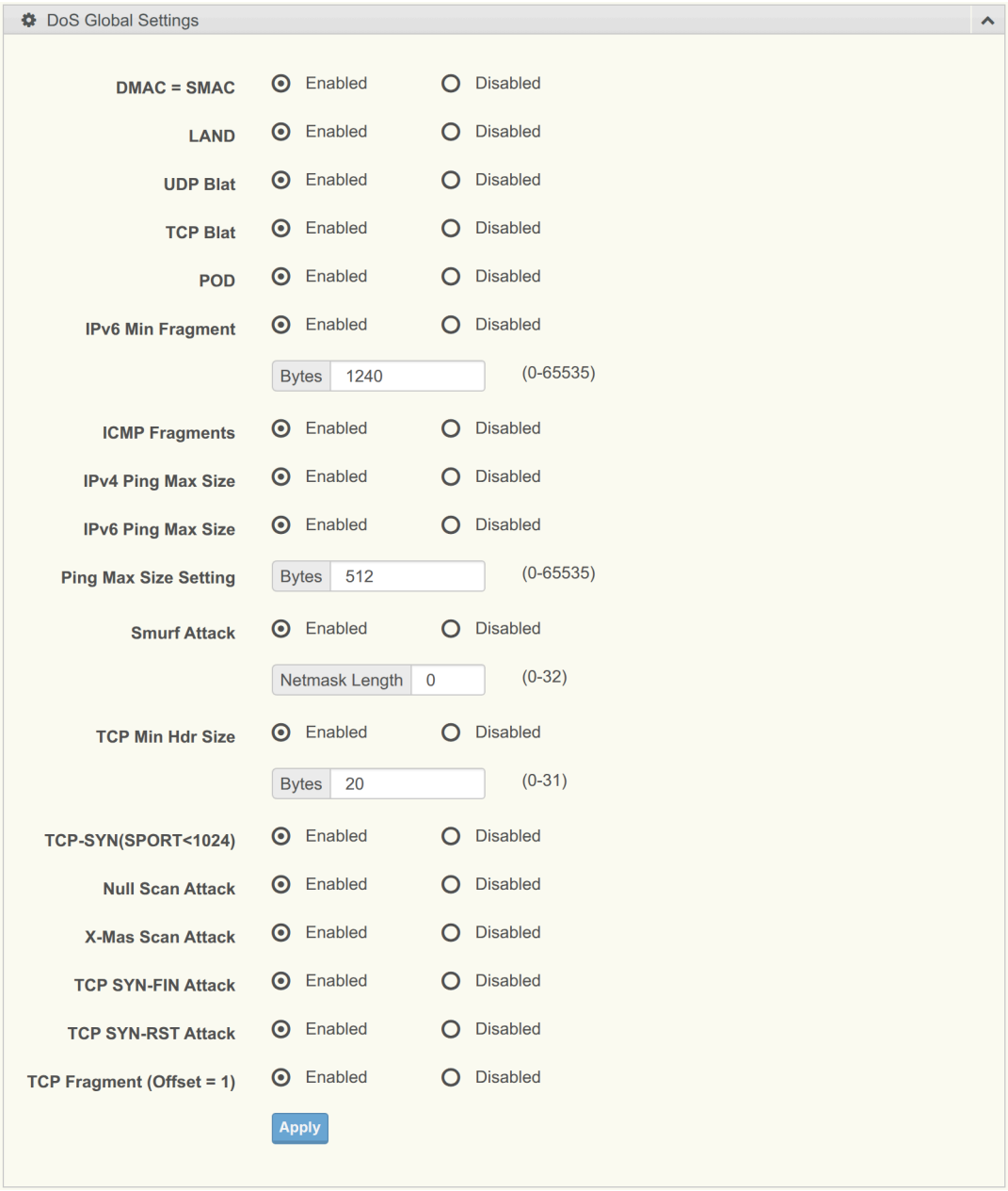


Figure 3.127 Security > DoS Prevention > DoS Global Settings

The following table describes the items in the previous figure.

Item	Description
DMAC = SMAC	Click **Enabled** or **Disabled** to define DMAC-SMAC for the DoS Global settings.
LAND	Click **Enabled** or **Disabled** to define LAND for the DoS Global settings.
UDP Blat	Click **Enabled** or **Disabled** to define UDP Blat for the DoS Global settings.
TCP Blat	Click **Enabled** or **Disabled** to define TCP Blat for the DoS Global settings.
POD	Click **Enabled** or **Disabled** to define POD for the DoS Global settings.

Item	Description
IPv6 Min Fragment	Click **Enabled** or **Disabled** to define minimum fragment size for the IPv6 protocol. Enter the variable in bytes (0 to 65535) to set the minimum fragment size when the function is enabled.
ICMP Fragments	Click **Enabled** or **Disabled** to define the ICMP Fragments function.
IPv4 Ping Max Size	Click **Enabled** or **Disabled** to set the maximum ping size for the IPv4 protocol.
IPv6 Ping Max Size	Click **Enabled** or **Disabled** to set a maximum ping size for the IPv6 protocol.
Ping Max Size Setting	Enter the variable in bytes (0 to 65535) to set the maximum ping size.
Smurf Attack	Click **Enabled** or **Disabled** to set the Smurf Attack function.
TCP Min Hdr Size	Click **Enabled** or **Disabled** to set the minimum header size. Enter the variable in bytes (0 to 31) to set the minimum header size.
TCP-SYN (SPORT < 1024)	Click **Enabled** or **Disabled** to set the TCP synchronization function (sport < 1021).
Null Scan Attack	Click **Enabled** or **Disabled** to set the Null Scan Attack function.
X-Mas Scan Attack	Click **Enabled** or **Disabled** to set the X-Mas Scan function.
TCP SYN-FIN Attack	Click **Enabled** or **Disabled** to set the TCP synchronization termination attack function.
TCP SYN-RST Attack	Click **Enabled** or **Disabled** to set the TCP synchronization reset attack function.
TCP Fragment (Offset = 1)	Click **Enabled** or **Disabled** to set the TCP fragment function (offset =1).
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **DoS Global Information** settings.

To access this page, click **Security > DoS Prevention > DoS Global Information**.

DoS Global Information

Information Name	Information Value
DMAC = SMAC	Enabled
Land Attack	Enabled
UDP Blat	Enabled
TCP Blat	Enabled
POD (Ping of Death)	Enabled
IPv6 Min Fragment Size	Enabled (1240 Bytes)
ICMP Fragment Packets	Enabled
IPv4 Ping Max Packet Size	Enabled (512 Bytes)
IPv6 Ping Max Packet Size	Enabled (512 Bytes)
Smurf Attack	Enabled (Netmask Length: 0)
TCP Min Header Length	Enabled (20 Bytes)
TCP Syn (SPORT < 1024)	Enabled
Null Scan Attack	Enabled
X-Mas Scan Attack	Enabled
TCP SYN-FIN Attack	Enabled
TCP SYN-RST Attack	Enabled
TCP Fragment (Offset = 1)	Enabled

Figure 3.128 Security > DoS Prevention > DoS Global Information

3.8.4.2 DoS Port Settings

The DoS Port Settings page allow you to configure DoS security (enabled or disabled) for the selected port.

To access this page, click **Security > DoS Prevention > DoS Port Settings**.

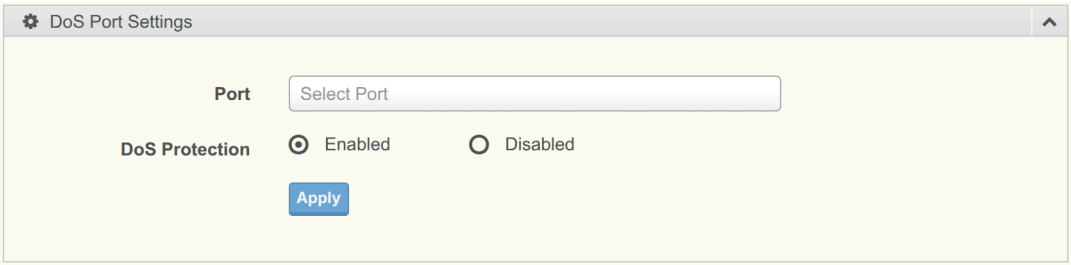


Figure 3.129 Security > DoS Prevention > DoS Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Select the port to configure for the DoS prevention function.
DoS Protection	Click **Enabled** or **Disabled** to set the DoS Port security function state.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **DoS Port Status** settings.

DoS Port Status

Port	DoS Protection
GE1	Disabled
GE2	Disabled
GE3	Disabled
GE4	Disabled
GE5	Disabled
GE6	Disabled
GE7	Disabled
GE8	Disabled
TGE1	Disabled
TGE2	Disabled
TGE3	Disabled
TGE4	Disabled
Trunk1	Disabled
Trunk2	Disabled
Trunk3	Disabled
Trunk4	Disabled
Trunk5	Disabled
Trunk6	Disabled
Trunk7	Disabled
Trunk8	Disabled

Figure 3.130 Security > DoS Prevention > DoS Port Status

3.8.5 Applications

The Applications function allows you to configure various types of AAA lists.

3.8.5.1 TELNET

The TELNET page allows you to combine all kinds of AAA lists with the Telnet line.

To access this page, click **Security > Applications > TELNET**.

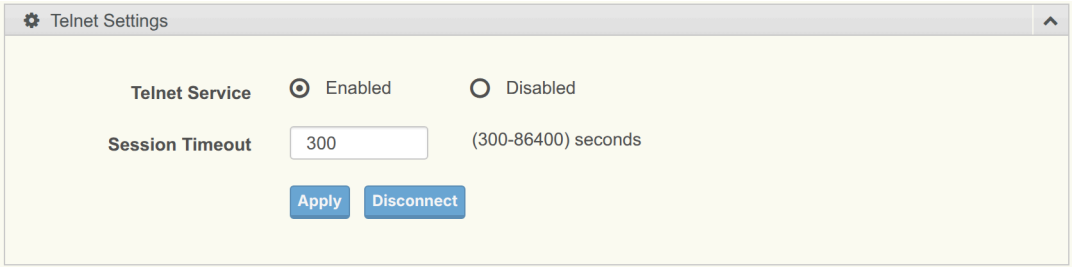


Figure 3.131 Security > Applications > TELNET

The following table describes the items in the previous figure.

Item	Description
Telnet Service	Click **Enabled** or **Disabled** to set remote access through the Telnet Service function.

Item	Description
Session Timeout	Enter a value to specify how long an idle session is kept open, in minutes.
Apply	Click **Apply** to save the values and update the screen.
Disconnect	Click **Disconnect** to disable the current Telnet service.

The following figure displays the **Telnet Information** settings.

Telnet Information

Information Name	Information Value
Telnet Service	Enabled
Session Timeout	300
Current Telnet Sessions Count	0

Figure 3.132 Security > Applications > Telnet Information

3.8.5.2 SSH

Secure Shell (SSH) is a protocol providing secure (encrypted) management connection to a remote device.

To access this page, click **Security > Applications > SSH**.

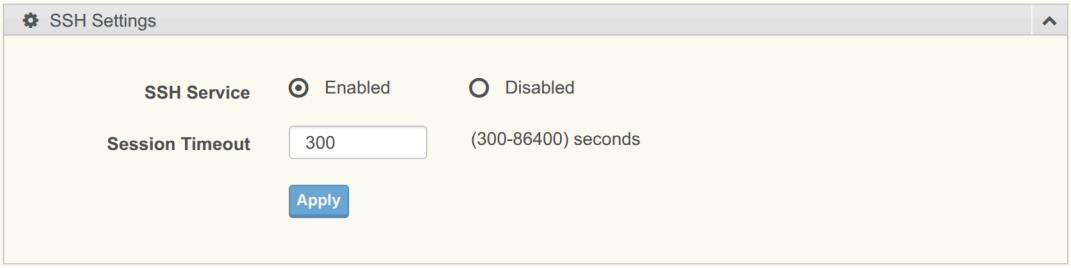


Figure 3.133 Security > Applications > SSH

The following table describes the items in the previous figure.

Item	Description
SSH Service	Click **Enabled** or **Disabled** to set up Ethernet encapsulation (remote access) through the Secure Shell (SSH) function.
Session Timeout	Enter a value to specify how long an idle session is kept open, in minutes.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **SSH Information** settings.

SSH Information

Information Name	Information Value
SSH	Enabled
Session Timeout	300

Figure 3.134 Security > Applications > SSH Information

3.8.5.3 HTTP

The HTTP page allows you to combine all kinds of AAA lists to the HTTP line. Attempts to access the switch's Web UI from HTTP are first authenticated.

To access this page, click **Security > Applications > HTTP**.

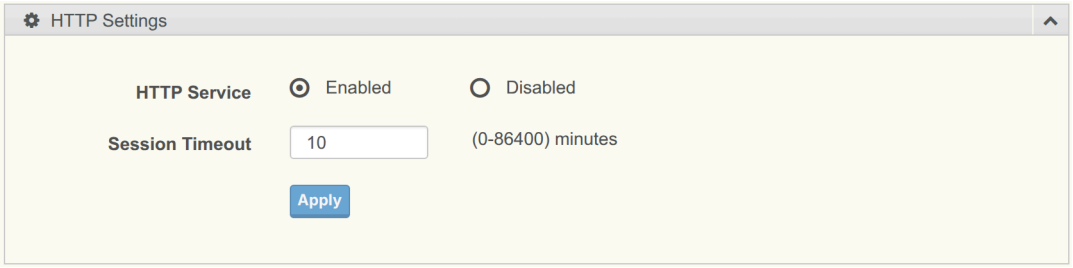


Figure 3.135 Security > Applications > HTTP

The following table describes the items in the previous figure.

Item	Description
HTTP Service	Click **Enabled** or **Disabled** to set up Ethernet encapsulation (remote access) through HTTP function.
Session Timeout	Enter the variable in minutes (0 to 86400) to define the timeout period for the HTTP session.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **HTTP Information** settings.



Figure 3.136 Security > Applications > HTTP Information

3.8.5.4 HTTPS

The HTTPS page allows you to combine all kinds of AAA lists on the HTTPS line. Attempts to access the switch's Web UI from HTTPS are first authenticated.

To access this page, click **Security > Applications > HTTPS**.

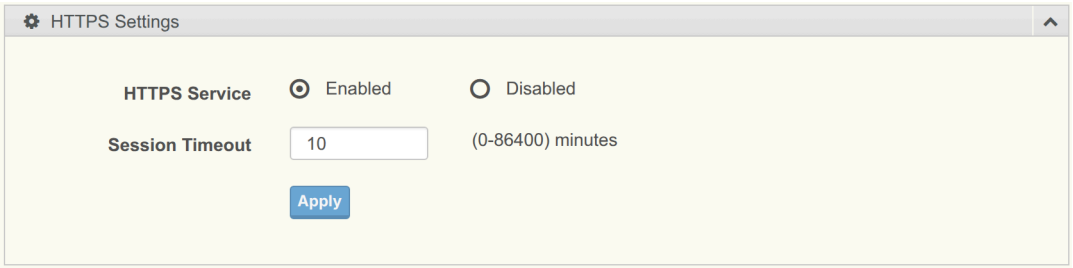


Figure 3.137 Security > Applications > HTTPS

The following table describes the items in the previous figure.

Item	Description
HTTPS Service	Click **Enabled** or **Disabled** to set up Ethernet encapsulation over HTTPS.
Session Timeout	Enter the variable in minutes (0 to 86400) to define the timeout period for the HTTP session.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **HTTPS Information** settings.



Figure 3.138 Security > Applications > HTTPS Information

3.8.6 802.1x

The 802.1x function provides port-based authentication to prevent unauthorized devices (clients) from gaining access to the network.

3.8.6.1 802.1x Global Settings

The 802.1x Global Settings page allows you to set the state (enabled or disabled) for the selected IP server address, port, accounting port and associated password, including a reauthentication period.

To access this page, click **Security > 802.1x > 802.1x Global Settings**.

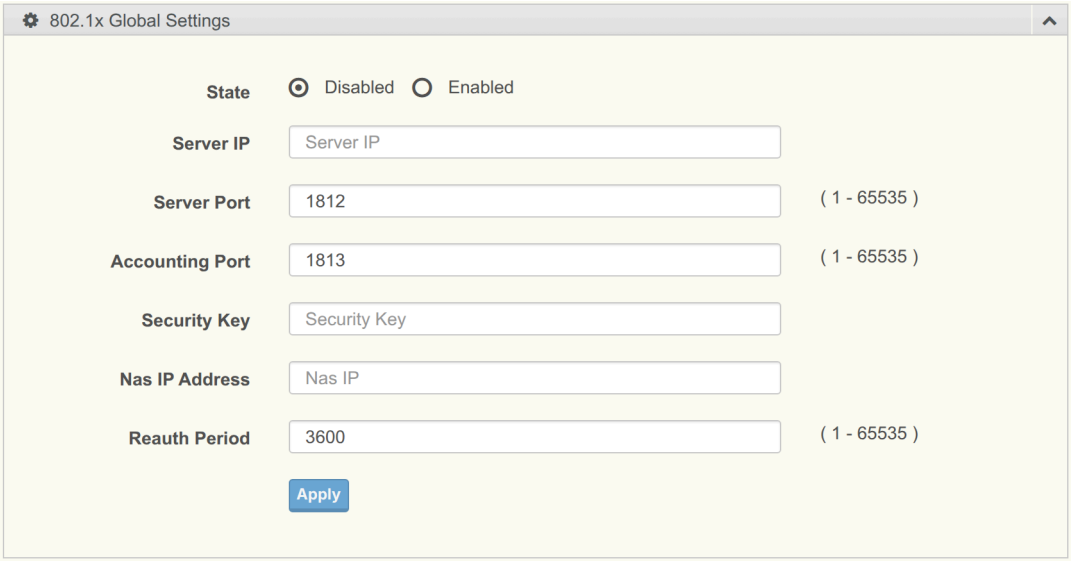


Figure 3.139 Security > 802.1x > 802.1x Global Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Enabled** or **Disabled** to set up 802.1x Setting function.
Server IP	Enter the IP address of the local server providing authentication function.
Server Port	Enter the port number (1 to 65535) assigned to the listed Server IP.
Accounting Port	Enter the port number (1 to 65535) assigned to the listed server IP configured to provide authorization and authentication for network access.
Security Key	Enter the variable to define the network security key used in authentication.
Nas IP Address	Enter a value to specify the IP address the switch presents to the RADIUS server as the network access server.
Reauth Period	Enter the variable in seconds to define the period of time between authentication attempts.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **802.1x Information** settings.

To access this page, click **Security > 802.1x > 802.1x Information**.

802.1x Information

Information Name	Information Value
State	Disabled
Server IP	
Server Port	1812
Accounting Port	1813
Nas IP Address	
Reauth Period	3600

Figure 3.140 Security > 802.1x > 802.1x Information

3.8.6.2 802.1x Port Configuration

The 802.1x Port Configuration page allows you to identify the authorization state for a port by using a MAC or Port authentication base.

To access this page, click **Security > 802.1x > 802.1x Port Configuration**.

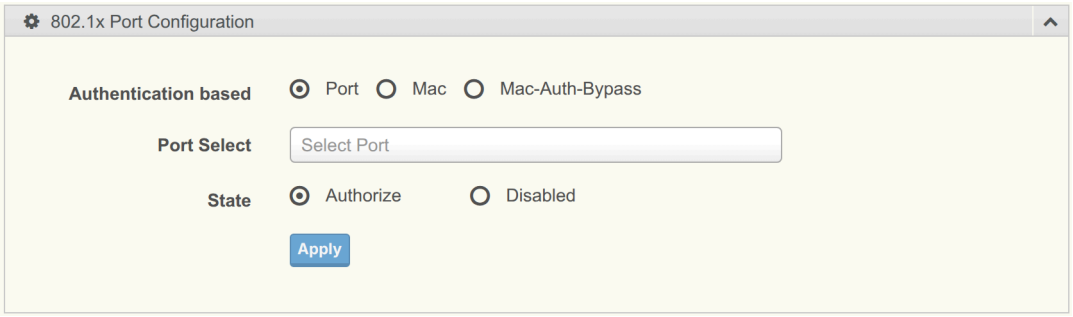


Figure 3.141 Security > 802.1x > 802.1x Port Configuration

The following table describes the items in the previous figure.

Item	Description
Authentication based	Click **Port, Mac** or **Mac-Auth-Bypass** to designate the type of configuration for the 802.1x Port setting.
Port Select	Enter the port number associated with the configuration setting.
State	Click **Authorize** or **Disabled** to define the listed port's state mode.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **802.1x Port Authorization** settings.

802.1x Port Authorization

Port	802.1x Port Authorization
GE1	Disabled
GE2	Disabled
GE3	Disabled
GE4	Disabled
GE5	Disabled
GE6	Disabled
GE7	Disabled
GE8	Disabled
TGE1	Disabled
TGE2	Disabled
TGE3	Disabled
TGE4	Disabled

Figure 3.142 Security > 802.1x > 802.1x Port Authorization

3.8.7 IP Security

This section provides you a means to configure the IP Security settings.

3.8.7.1 Global Settings

The Global Settings page allows you to set the IP Security status (enabled or disabled).

To access this page, click **Security > IP Security > Global Settings**.

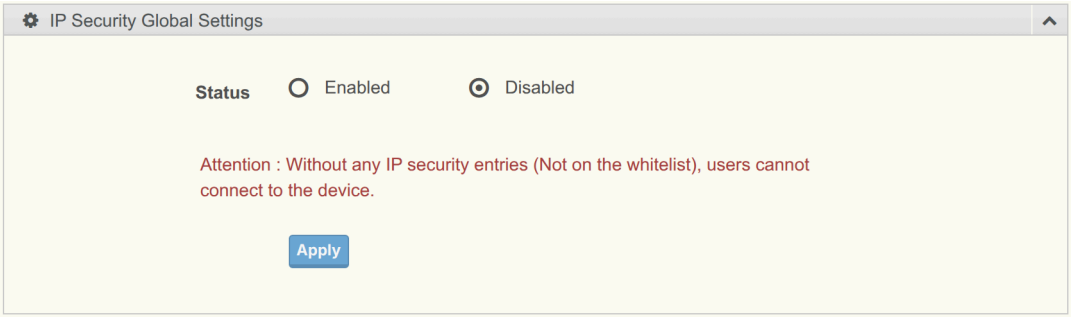


Figure 3.143 Security > IP Security > Global Settings

The following table describes the items in the previous figure.

Item	Description
Status	Click **Enabled** or **Disabled** to define the global setting for the IP security function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **IP Security Status** settings.

IP Security Status

Information Name	Information Value
IP Security	Disabled

Figure 3.144 Security > IP Security > IP Security Status

3.8.7.2 Entry Settings

Once the Global Setting is enabled, use the Entry Settings to define an IP Security entry.

To access this page, click **Security > IP Security > Entry Settings**.

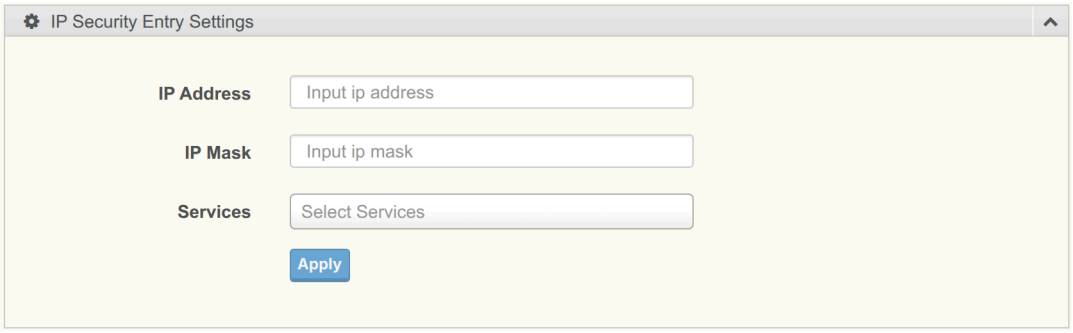


Figure 3.145 Security > IP Security > Entry Settings

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the source IP address to apply the IP Security function.
IP Mask	Enter the IP address for use in masking the previous IP Address.
Services	Enter the type of services to associate with the entry setting.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **IP Security Entry Information** settings.

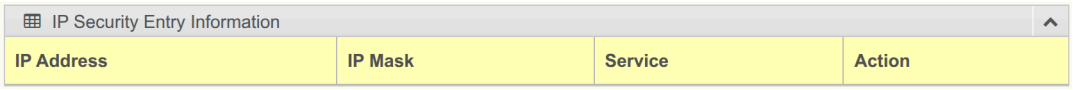


Figure 3.146 Security > IP Security > IP Security Entry Information

3.8.8 Security login

3.8.8.1 Security Login Global Settings

This function provides a means to enable or disable the global security settings for the system.

To access this page, click **Security > Security login > Security Login Global Settings**.

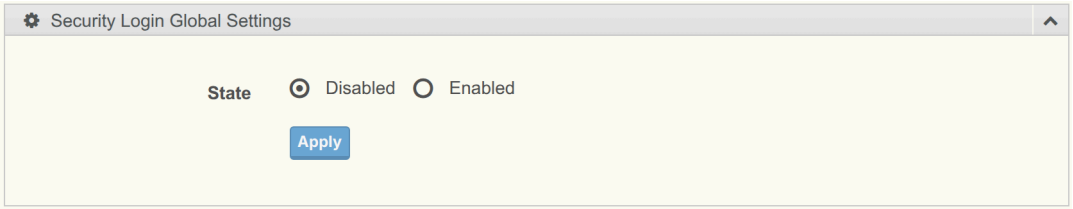


Figure 3.147 Security > Security login > Security Login Global Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Enabled** or **Disabled** to set up security login global setting status.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **RADIUS Settings** settings.

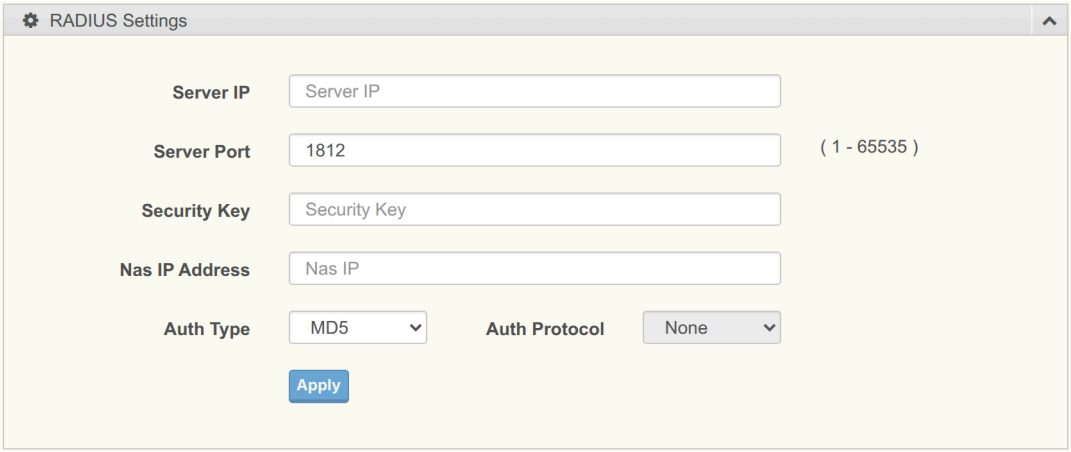


Figure 3.148 Security > Security login > RADIUS Settings

The following table describes the items in the previous figure.

Item	Description
Server IP	Enter the IP address of the local server providing authentication function.
Server Port	Enter the port number (1 to 65535) assigned to the listed Server IP.
Security Key	Enter the variable to define the network security key used in authentication.
Nas IP Address	Enter a value to specify the IP address the switch presents to the RADIUS server as the network access server.
Auth Protocol	Displays the authentication protocol automatically applied based on the selected **Auth Type** below; this field cannot be edited directly.
Auth Type	Click the drop down menu to select the Authentication type with option MD5, TTLS or PEAP. Each authentication type is mapping to specified authentication protocol as below: ■ MD5: Using authentication protocol with None. ■ TTLS: Using authentication protocol with TTLS. ■ PEAP: Using authentication protocol with PEAP.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **TACACS Settings** settings.

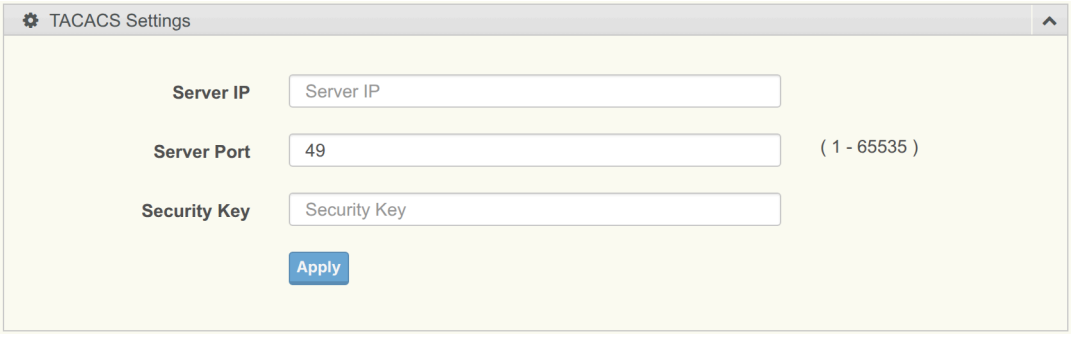


Figure 3.149 Security > Security login > TACACS Settings

The following table describes the items in the previous figure.

Item	Description
Server IP	Enter the IP address of the local server providing authentication function.
Server Port	Enter the port number (1 to 65535) assigned to the listed Server IP.

Item	Description
Security Key	Enter the variable to define the network security key used in authentication.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Global Information** settings.

To access this page, click **Security > Security Login > Global Settings > Global Information**.

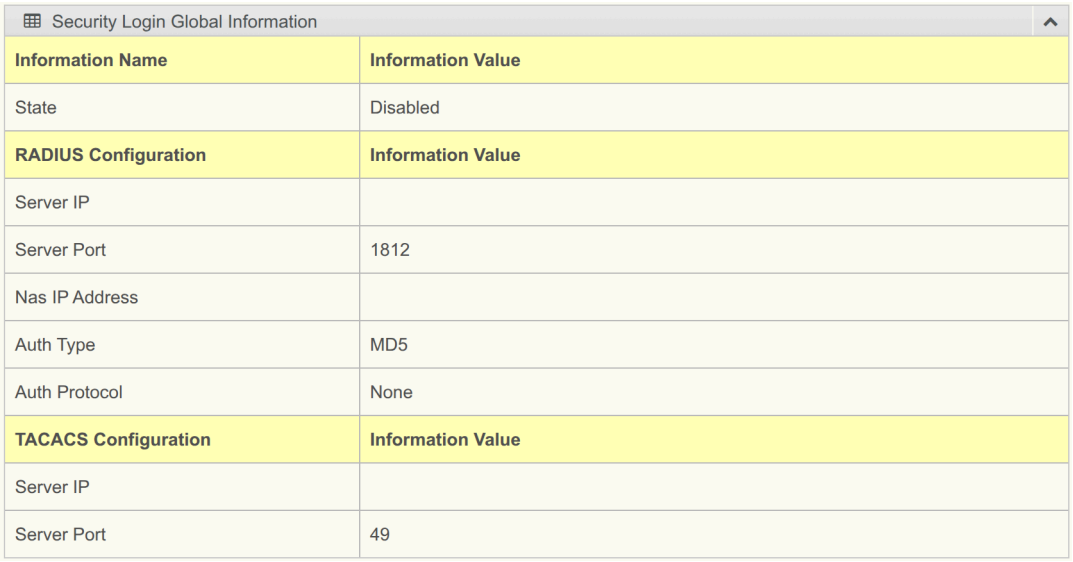


Figure 3.150 Security > Security login > Security Login Global Information

3.8.8.2 Security Login Access Control Settings

This function specifies the login authentication type for the system.

To access this page, click **Security > Security login > Security Login Access Control Settings**.



Figure 3.151 Security > Security login > Security Login Access Control Settings

The following table describes the items in the previous figure.

Item	Description
Login Type	Click to select the login type. Options include: None Used, RADIUS Only, RADIUS & Local, TACACS Only, TACACS & Local, RADIUS & TACACS or RADIUS & TACACS & Local.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Security Login type Settings** settings.

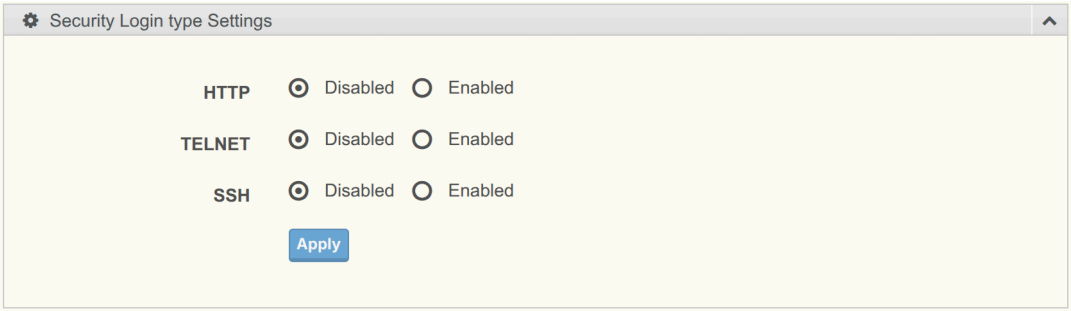


Figure 3.152 Security > Security login > Security Login type Settings

The following table describes the items in the previous figure.

Item	Description
HTTP	Click **Enabled** or **Disabled** to set up HTTP.
TELNET	Click **Enabled** or **Disabled** to set up HTTPS.
SSH	Click **Enabled** or **Disabled** to set up SSH.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Access Control Information** settings.

To access this page, click **Security > Security Login > Access Control Settings > Global Information**.

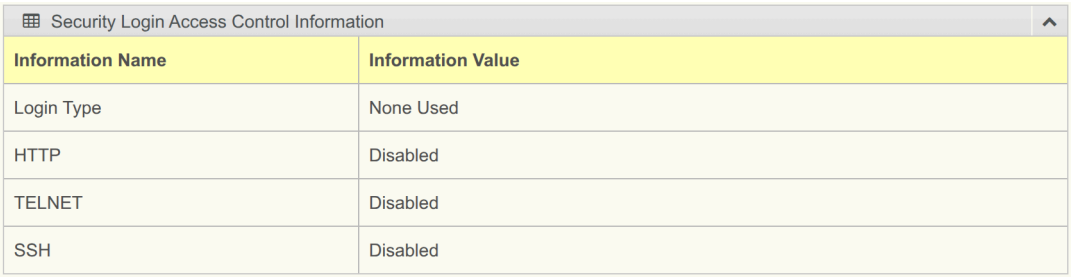


Figure 3.153 Security > Security login > Security Login Access Control Information

3.8.9 Access Control List

The Access Control List is the basic traffic filter for ingress and egress packets. Allow user to filter criteria for diverse protocols and deny access to specific source or destination IP/MAC addresses.

3.8.9.1 MAC ACL

Entry Settings

To access this page, click **Security > Access Control List > MAC ACL > Entry Settings**.

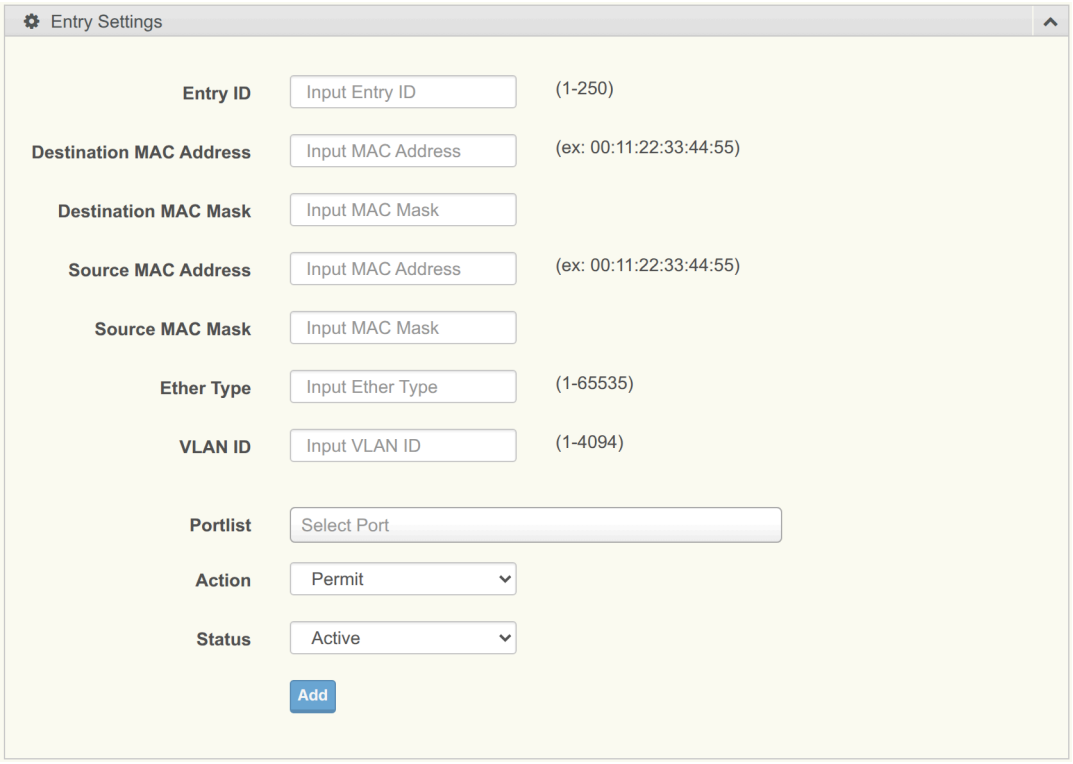


Figure 3.154 Security > Access Control List > MAC ACL > Entry Settings

The following table describes the items in the previous figure.

Item	Description
Entry ID	Type in the value designating the entry ID.
Destination MAC Address	Enter the MAC address to set destination MAC address.
Destination MAC Mask	Enter a value to specify the subnet mask for the destination MAC address.
Source MAC Address	Enter the MAC address to set source MAC address.
Source MAC Mask	Enter a value to specify the subnet mask for the source MAC address.
Ether Type	Enter a value to specify the DNS server for the interface.
VLAN ID	Type in the value designating the VLAN ID.
Portlist	Select the port to configure for the MAC ACL function.
Action	Click the drop down menu to select the MAC ACL action. Options include: Permit, Drop, Assign Queue, Redirect Port or Redirect Portlist.
Assign Queue	Click the drop down menu to select the queue. The function is only available when **Action** is **Assign Queue**.
Status	Click the drop down menu to select the MAC ACL status. Options include: Active or Inactive.
Add	Click **Add** to add a MAC ACL entry.

Entry List

The following figure displays the **Entry List** settings.

To access this page, click **Security > Access Control List > MAC ACL > Entry List**.

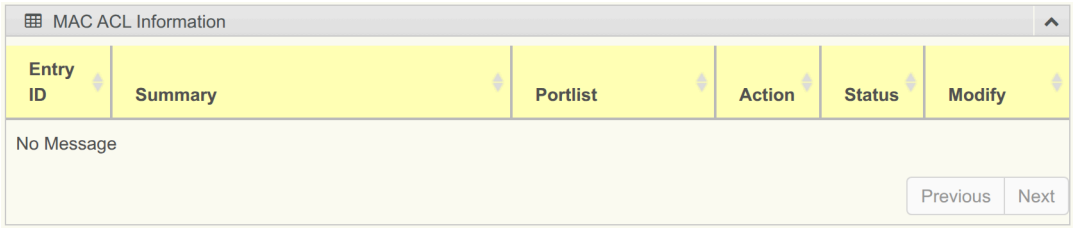


Figure 3.155 Security > Access Control List > MAC ACL > Entry List

3.8.9.2 IP ACL

Entry Settings

To access this page, click **Security > Access Control List > IP ACL > Entry Settings**.

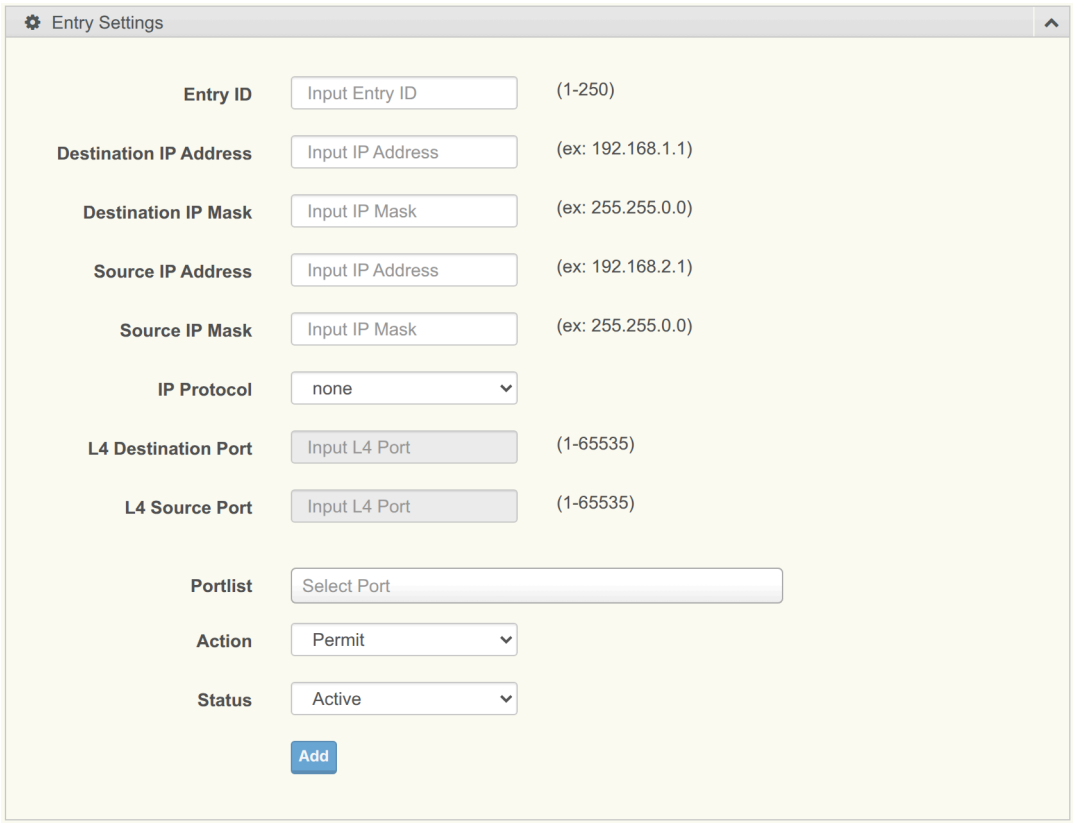


Figure 3.156 Security > Access Control List > IP ACL > Entry Settings

The following table describes the items in the previous figure.

Item	Description
Entry ID	Type in the value designating the entry ID.
Destination IP Address	Enter the IP address to set destination IP address.
Destination IP Mask	Enter a value to specify the subnet mask for the destination IP address.
Source IP Address	Enter the IP address to set source IP address.
Source IP Mask	Enter a value to specify the subnet mask for the source IP address.
IP Protocol	Click the drop down menu to select the IP protocol. Options include: none, ICMP, TCP or UDP.

Item	Description
L4 Destination Port	Enter a value to specify the L4 destination port.
L4 Source Port	Enter a value to specify the L4 source port.
Portlist	Select the port to configure for the IP ACL function.
Action	Click the drop down menu to select the IP ACL action. Options include: Permit, Drop or Assign Queue.
Assign Queue	Click the drop down menu to select the queue. The function is only available when **Action** is **Assign Queue**.
Redirect Port	Click the drop-down menu to select the port to which matched traffic is redirected. The field is only available when **Action** is **Redirect**.
Redirect Portlist	Select the ports to which matched traffic is redirected.
Status	Click the drop down menu to select the IP ACL status. Options include: Active or Inactive.
Add	Click **Add** to add an IP ACL entry.

Entry List

The following figure displays the **IP ACL Information** settings. Click Edit to edit the desired entry id or Delete to remove the desired entry id.

To access this page, click **Security > Access Control List > IP ACL > Entry List**.

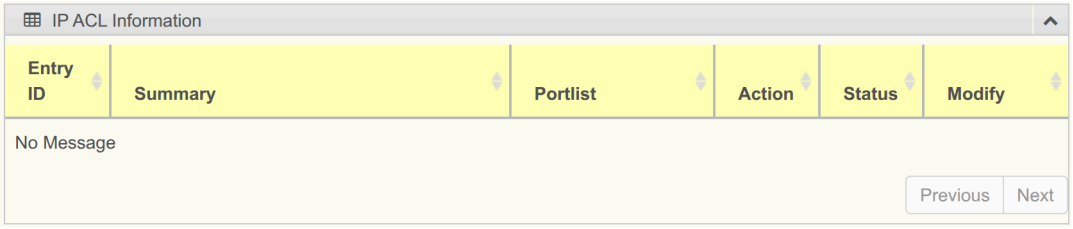


Figure 3.157 Security > Access Control List > IP ACL > Entry List

3.8.10 IP Source Guard

3.8.10.1 Global Settings

To access this page, click **Security > IP Source Guard > Global Settings**.



Figure 3.158 Security > IP Source Guard > Global Settings

The following table describes the items in the previous figure.

Item	Description
Portlist	Select the port to verify.
Modify	Click **Modify** to save the values and update the screen.

The following figure displays the **Global Information** settings.



Figure 3.159 Security > IP Source Guard > Global Information

3.8.10.2 Entry Settings

To access this page, click **Security > IP Source Guard > Entry Settings**.

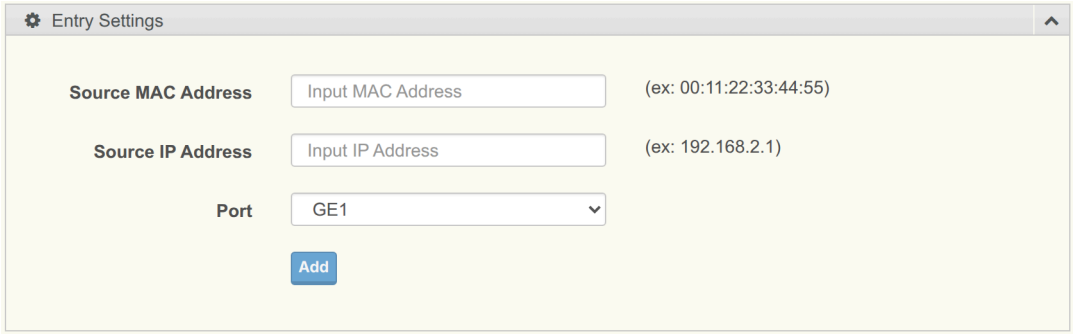


Figure 3.160 Security > IP Source Guard > Entry Settings

The following table describes the items in the previous figure.

Item	Description
Source MAC Address	Enter the MAC address to set source MAC address.
Source IP Address	Enter the IP address to set source IP address.
Port	Select the port to configure for the IP source guard.
Add	Click **Add** to add an IP source guard.

The following figure displays the **Entry Information** settings.

To access this page, click **Security > IP Source Guard > Entry Information**.



Figure 3.161 Security > IP Source Guard > Entry Information

3.8.11 ARP Spoofing

To access this page, click **Security > ARP Spoofing**.

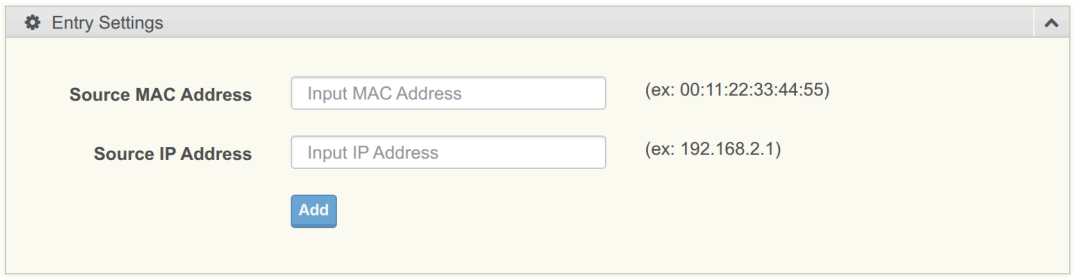


Figure 3.162 Security > ARP Spoofing

The following table describes the items in the previous figure.

Item	Description
Source MAC Address	Enter the MAC address to set source MAC address.
Source IP Address	Enter the IP address to set source IP address.
Add	Click **Add** to add an ARP spoofing.

The following figure displays the **Entry Information** settings.

To access this page, click **Security > Entry Information**.

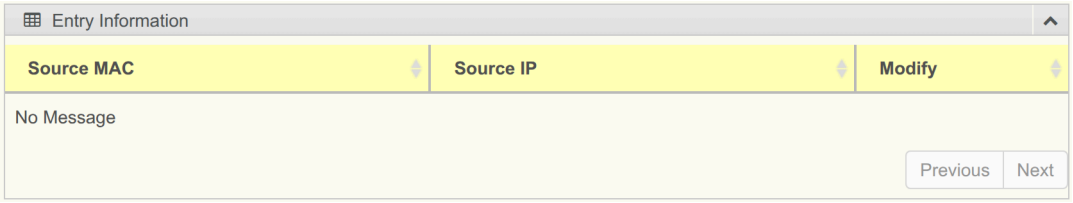


Figure 3.163 Security > Entry Information

The following table describes the items in the previous figure.

3.9 QoS

The QoS function allows you to configure settings for the switch QoS interface and how the switch connects to a remote server to get services.

3.9.1 General

Traditionally, networks operate on a best-effort delivery basis, all traffic has equal priority and an equal chance of being delivered in a timely manner. When there is congestion, all traffic has an equal chance of being dropped.

The QoS feature can be configured for congestion-management and congestion-avoidance to specifically manage the priority of the traffic delivery. Implementing QoS in the network makes performance predictable and bandwidth utilization much more effective.

The QoS implementation is based on the prioritization values in Layer 2 frames.

3.9.1.1 QoS Properties

The QoS Properties allows you to set the QoS mode.

To access this page, click **QoS > General > QoS Properties**.

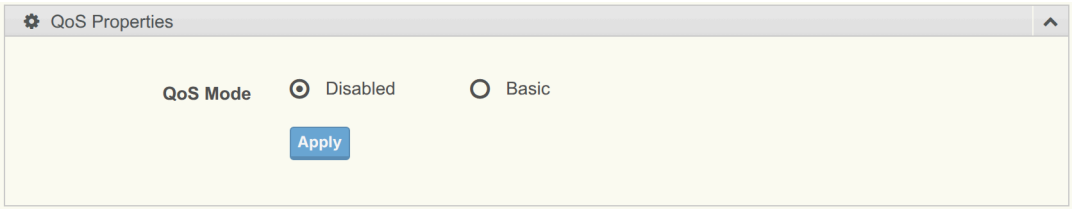


Figure 3.164 QoS > General > QoS Properties

The following table describes the items in the previous figure.

Item	Description
QoS Mode	Select **Disabled** or **Basic** to setup the QoS function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **QoS Global Information** settings.



Figure 3.165 QoS > General > QoS Global Information

3.9.1.2 QoS Settings

Once the QoS function is enabled, you can configure the available settings.

To access this page, click **QoS > General > QoS Settings**.

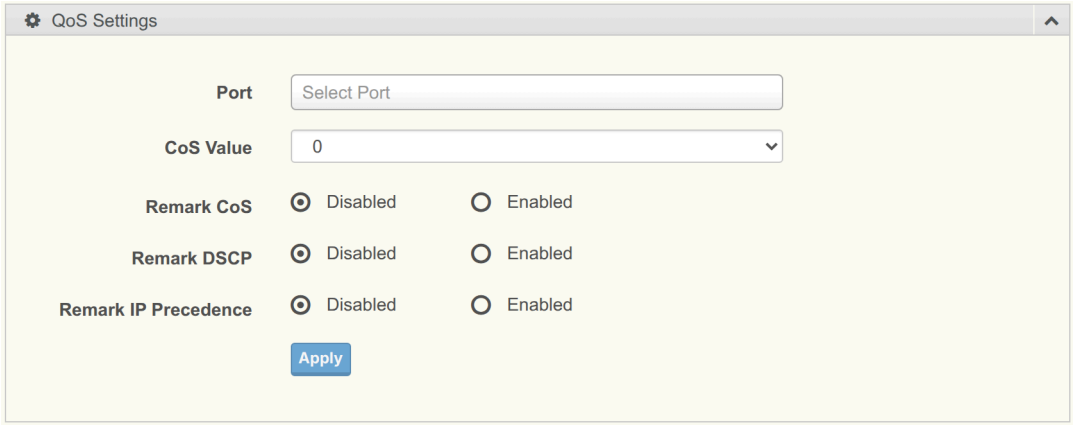


Figure 3.166 QoS > General > QoS Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to associate with the QoS setting.
CoS Value	Click the drop-down menu to designate the Class of Service (CoS) value (0 to 7) for the Port entry.
Remark CoS	Click **Disabled** or **Enabled** to setup the Remark CoS function. When enabled the LAN (preassigned priority values) is marked at Layer 2 boundary to CoS values.
Remark DSCP	Click **Disabled** or **Enabled** to setup the DSCP remark option for the QoS function.
Remark IP Precedence	Click **Disabled** or **Enabled** to setup the Remark IP Precedence for the QoS function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **QoS Status** settings.

To access this page, click **QoS > General > QoS Status**.

QoS Status

Port	CoS Value	Remark CoS	Remark DSCP	Remark IP Precedence
GE1	0	Disabled	Disabled	Disabled
GE2	0	Disabled	Disabled	Disabled
GE3	0	Disabled	Disabled	Disabled
GE4	0	Disabled	Disabled	Disabled
GE5	0	Disabled	Disabled	Disabled
GE6	0	Disabled	Disabled	Disabled
GE7	0	Disabled	Disabled	Disabled
GE8	0	Disabled	Disabled	Disabled
TGE1	0	Disabled	Disabled	Disabled
TGE2	0	Disabled	Disabled	Disabled
TGE3	0	Disabled	Disabled	Disabled
TGE4	0	Disabled	Disabled	Disabled
Trunk1	0	Disabled	Disabled	Disabled
Trunk2	0	Disabled	Disabled	Disabled
Trunk3	0	Disabled	Disabled	Disabled
Trunk4	0	Disabled	Disabled	Disabled
Trunk5	0	Disabled	Disabled	Disabled
Trunk6	0	Disabled	Disabled	Disabled
Trunk7	0	Disabled	Disabled	Disabled
Trunk8	0	Disabled	Disabled	Disabled

Figure 3.167 QoS > General > QoS Status

3.9.1.3 QoS Scheduling

The switch support eight CoS queues for each egress port. For each of the eight queues, two types of scheduling can be configured: Strict Priority and Weighted Round Robin (WRR).

Strict Priority scheduling is based on the priority of queues. Packets in a high-priority queue are always sent first and packets in a low-priority queue are only sent after all the high priority queues are empty.

Weighted RoundRobin (WRR) scheduling is based on the user priority specification to indicate the importance (weight) of the queue relative to the other CoS queues. WRR scheduling prevents low-priority queues from being completely ignored during periods of high priority traffic. The WRR scheduler sends some packets from each queue in turn.

To access this page, click **QoS > General > QoS Scheduling**.

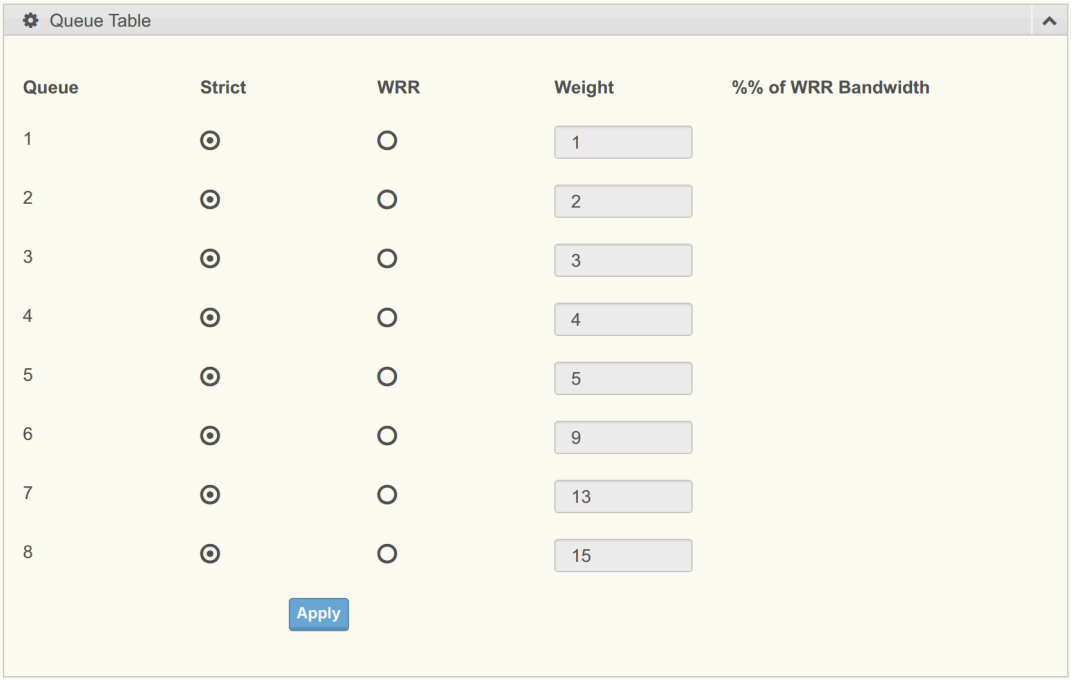


Figure 3.168 QoS > General > QoS Scheduling

The following table describes the items in the previous figure.

Item	Description
Queue	Queue entry for egress port.
Strict	Select Strict to assign the scheduling designation to the selected queue.
WRR	Select WRR to assign the scheduling designation to the selected queue.
Weight	Enter a queue priority (weight) relative to the defined entries (WRR only).
% of WRR Bandwidth	Displays the allotted bandwidth for the queue entry in percentage values.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Queue Information** settings.

To access this page, click **QoS > General > QoS Information**.



Figure 3.169 QoS > General > Queue Information

3.9.1.4 CoS Mapping

The CoS Mapping allows you to apply CoS mapping.

To access this page, click **QoS > General > CoS Mapping**.

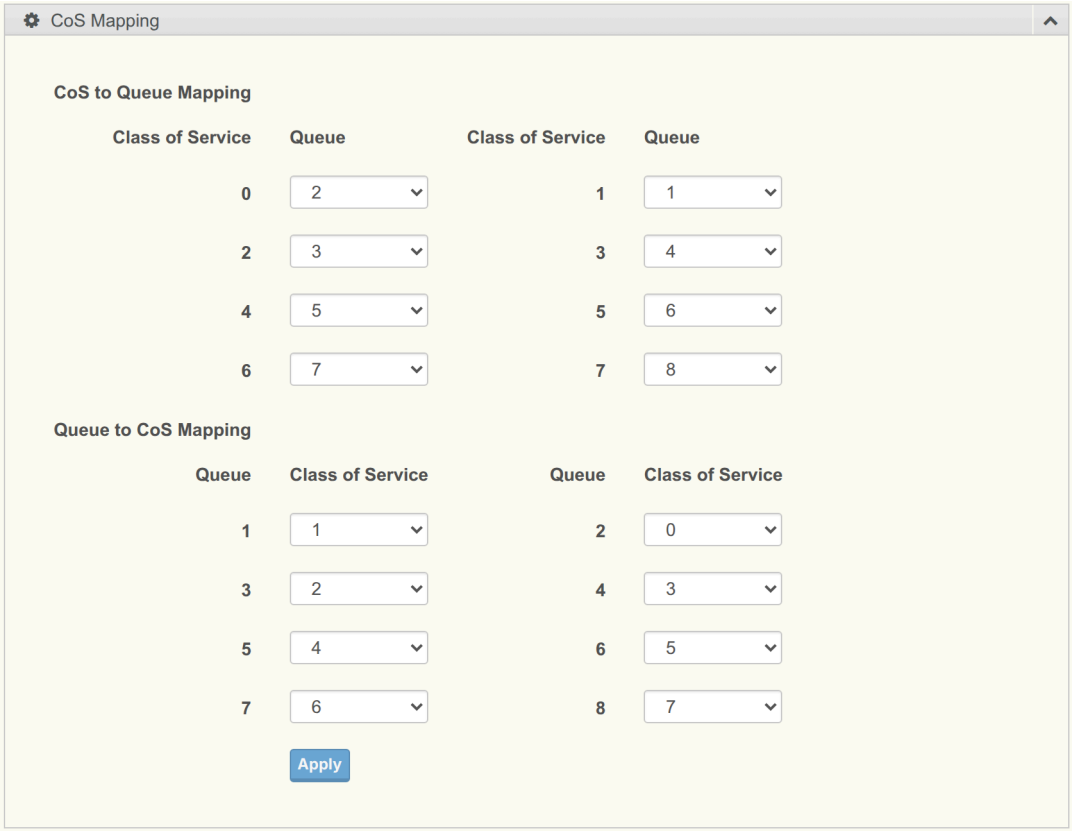


Figure 3.170 QoS > General > CoS Mapping

The following table describes the items in the previous figure.

Item	Description
CoS to Queue Mapping	
Class of Service	Displays the CoS for the queue entry.
Queue	Click the drop-down menu to select the queue priority for selected CoS.
Queue to CoS Mapping	
Queue	Displays the queue entry for CoS mapping.
Class of Service	Click the drop-down menu to select the CoS type
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **CoS Mapping Information** settings.

To access this page, click **QoS > General > CoS Mapping**.

CoS Mapping Information

CoS	Mapping to Queue
0	2
1	1
2	3
3	4
4	5
5	6
6	7
7	8

Figure 3.171 QoS > General > CoS Mapping Information

The following figure displays the **Queue Mapping Information** settings.

To access this page, click **QoS > General > CoS Mapping**.

Queue Mapping Information

Queue	Mapping to CoS
1	1
2	0
3	2
4	3
5	4
6	5
7	6
8	7

Figure 3.172 QoS > General > Queue Mapping Information

3.9.1.5 DSCP Mapping

The DSCP to Queue mapping function maps queue values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic. The following table shows the DSCP to Queue map.

If these values are not appropriate for your network, you need to modify them.

To access this page, click **QoS > General > DSCP Mapping**.

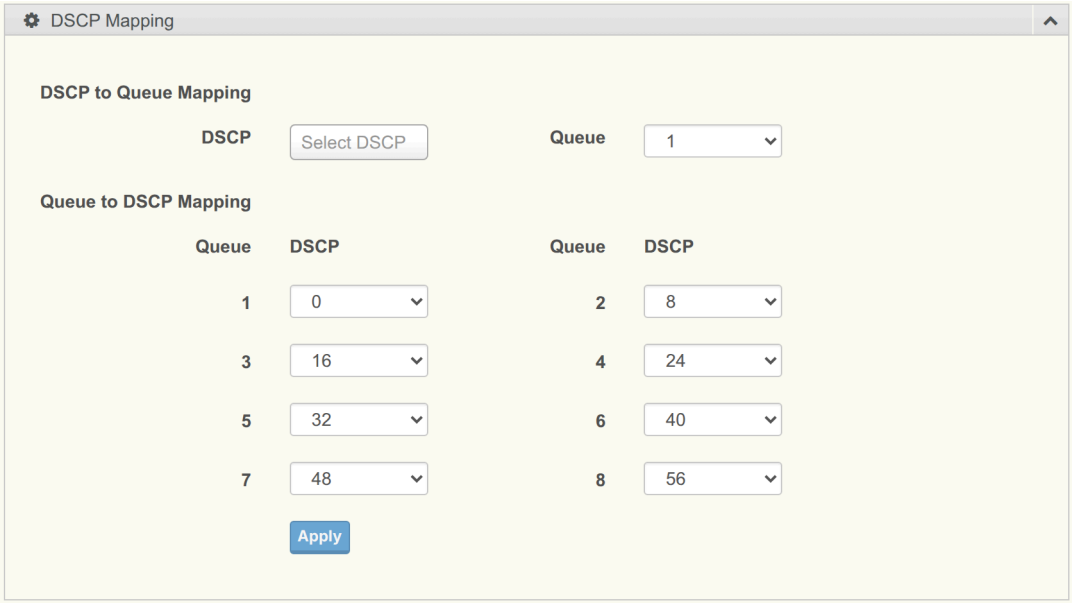


Figure 3.173 QoS > General > DSCP Mapping

The following table describes the items in the previous figure.

Item	Description
DSCP to Queue Mapping	
DSCP	Enter the DSCP entry to define the precedence values.
Queue	Click the drop-down menu to select the queue designation for the DSCP value.
Queue to DSCP Mapping	
Queue	Displays the queue value for the DSCP map.
DSCP	Enter the DSCP entry to define the precedence values.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **DSCP Mapping Information** settings.

DSCP Mapping Information

DSCP	Mapping to Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	2
10	2
11	2
12	2
13	2
14	2
15	2
16	3
17	3
18	3
19	3
20	3
21	3
22	3
23	3
24	4
25	4
26	4
27	4
28	4
29	4
30	4
31	4

Figure 3.174 QoS > General > DSCP Mapping Information (DSCP 0–31)

DSCP Mapping Information

DSCP	Mapping to Queue
32	5
33	5
34	5
35	5
36	5
37	5
38	5
39	5
40	6
41	6
42	6
43	6
44	6
45	6
46	6
47	6
48	7
49	7
50	7
51	7
52	7
53	7
54	7
55	7
56	8
57	8
58	8
59	8
60	8
61	8
62	8
63	8

Figure 3.174 QoS > General > DSCP Mapping Information (DSCP 32–63)

The following figure displays the **Queue Mapping Information** settings.

Queue Mapping Information

Queue	Mapping to DSCP
1	0
2	8
3	16
4	24
5	32
6	40
7	48
8	56

Figure 3.175 QoS > General > Queue Mapping Information

3.9.1.6 IP Precedence Mapping

The IP Precedence Mapping allows you to set IP Precedence mapping.

To access this page, click **QoS > General > IP Precedence Mapping**.

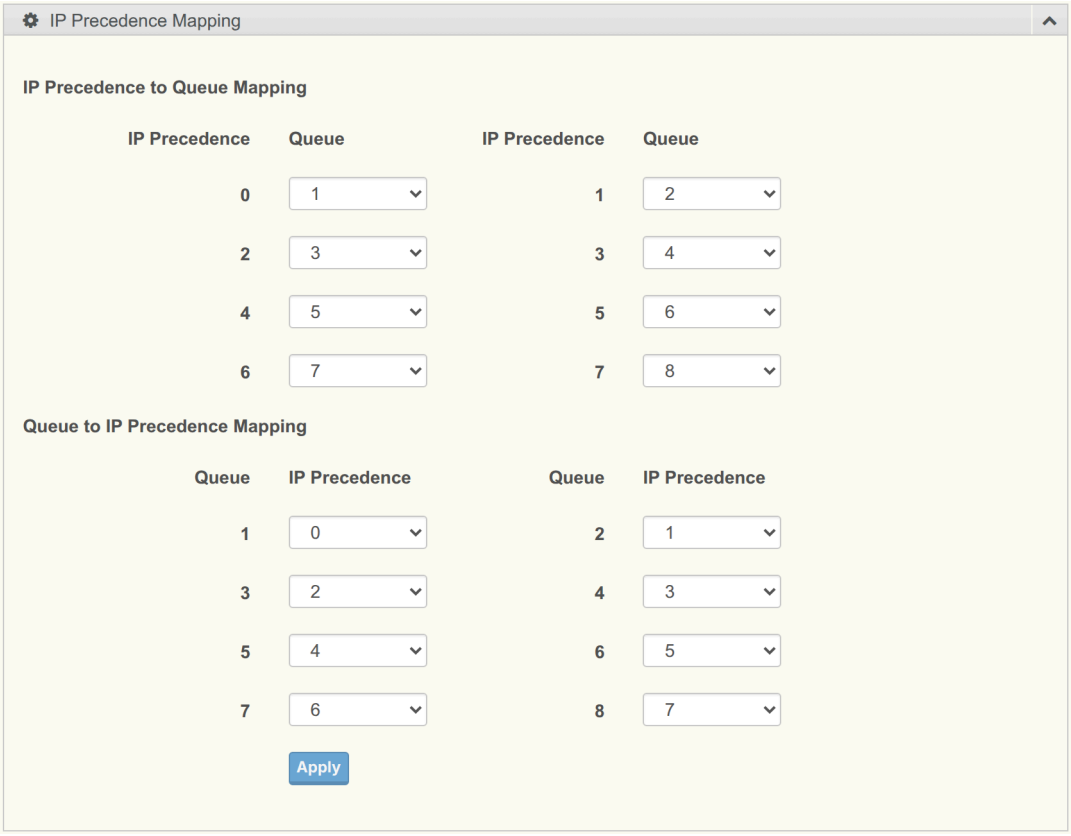


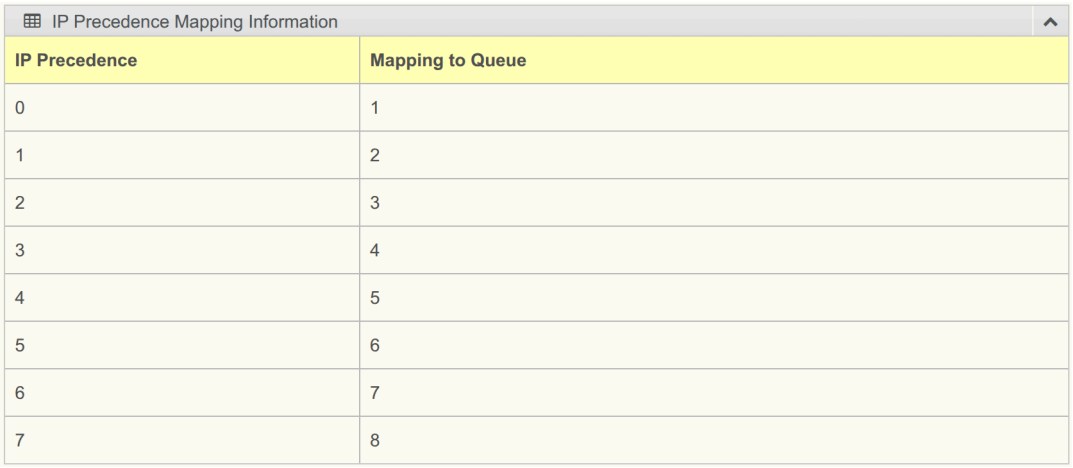
Figure 3.176 QoS > General > IP Precedence Mapping

The following table describes the items in the previous figure.

Item	Description
IP Precedence to Queue Mapping	
IP Precedence	Displays the IP precedence value for the queue map.
Queue	Click the drop-down menu to map a queue value to the selected IP precedence.
Queue to IP Precedence Mapping	

Item	Description
Queue	Displays the queue entry for mapping IP precedence values.
IP Precedence	Click the drop-down menu to map an IP precedence value to the selected queue.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **IP Precedence Mapping Information** settings.

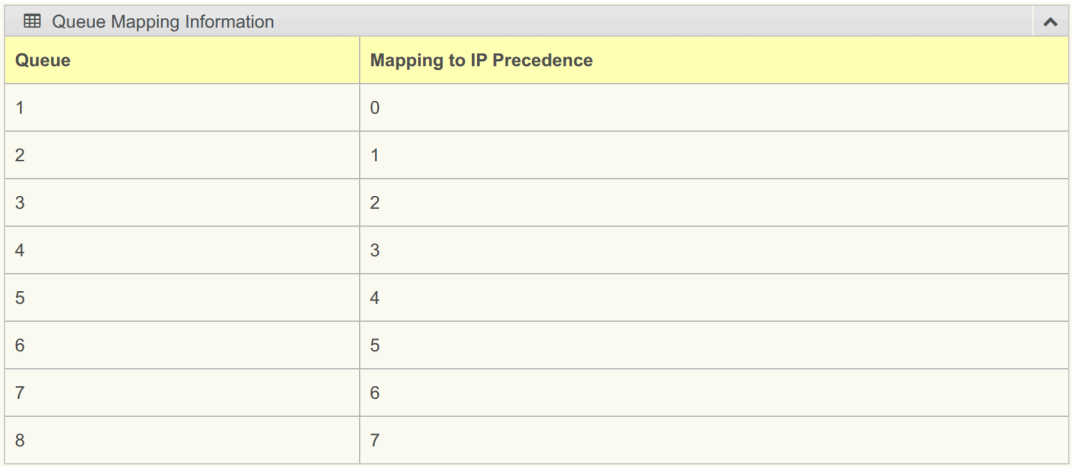


IP Precedence Mapping Information

IP Precedence	Mapping to Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

Figure 3.177 QoS > General > IP Precedence Mapping Information

The following figure displays the **Queue Mapping Information** settings.



Queue Mapping Information

Queue	Mapping to IP Precedence
1	0
2	1
3	2
4	3
5	4
6	5
7	6
8	7

Figure 3.178 QoS > General > Queue Mapping Information

3.9.2 Qos Basic Mode

Quality of Service (QoS) allows to give preferential treatment to certain types of traffic at the expense of others. Without QoS, the switch offers best-effort service to each packet, regardless of the packet contents or size sending the packets without any assurance of reliability, delay bounds, or throughput.

QoS mode supports two modes: 802.1p and DSCP.

3.9.2.1 Global Settings

The Global Settings page allows you to configure the trust mode to a port selection.

The function is only available when **QoS Properties** is set to **Basic**.

To access this page, click **QoS > Qos Basic Mode > Global Settings**.



Figure 3.179 QoS > Qos Basic Mode > Global Settings

The following table describes the items in the previous figure.

Item	Description
Trust Mode	Click the drop-down menu to select the trust state of the QoS basic mode. Settings: None, CoS/802.1p, DSCP, CoS/802.1p-DSCP and IP Precedence.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **QoS Information** settings.

To access this page, click **QoS > General > Global Settings**.

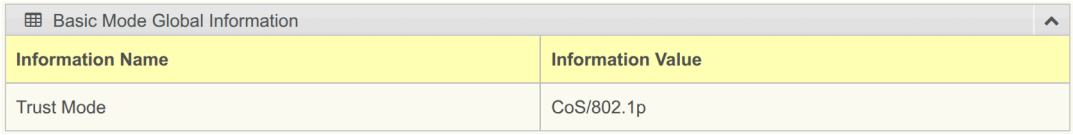


Figure 3.180 QoS > Qos Basic Mode > Basic Mode Global Information

3.9.2.2 Port Settings

The Port Settings page allows you to define a trust state (enabled or disabled) to a listed port.

To access this page, click **QoS > Qos Basic Mode > Port Settings**.

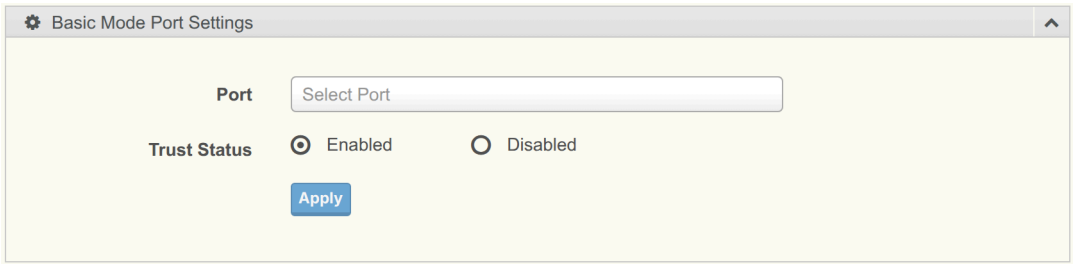


Figure 3.181 QoS > Qos Basic Mode > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number for the QoS basic mode setting.
Trust Status	Select **Enabled** or **Disabled** to set the port's trust state status.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Basic Mode Port Information** settings.

Basic Mode Port Information

Port	Trust Status
GE1	Enabled
GE2	Enabled
GE3	Enabled
GE4	Enabled
GE5	Enabled
GE6	Enabled
GE7	Enabled
GE8	Enabled
TGE1	Enabled
TGE2	Enabled
TGE3	Enabled
TGE4	Enabled
Trunk1	Enabled
Trunk2	Enabled
Trunk3	Enabled
Trunk4	Enabled
Trunk5	Enabled
Trunk6	Enabled
Trunk7	Enabled
Trunk8	Enabled

Figure 3.182 QoS > Qos Basic Mode > Basic Mode Port Information

3.9.3 Rate Limit

Rate Limits features control on a per port basis. Bandwidth control is supported for the following: Ingress Bandwidth Control, Egress Bandwidth Control and Egress Queue.

3.9.3.1 Ingress Bandwidth Control

The Ingress Bandwidth Control page allows you to configure the bandwidth control for a listed port.

To access this page, click **QoS > Rate Limit > Ingress Bandwidth Control**.

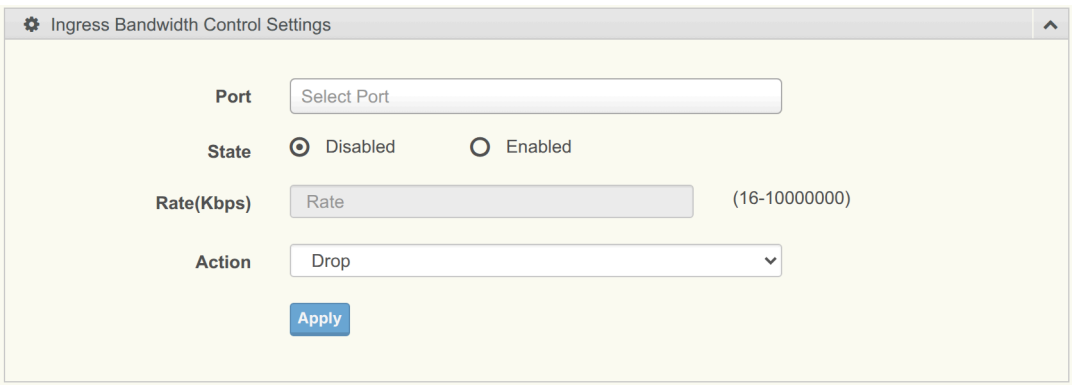


Figure 3.183 QoS > Rate Limit > Ingress Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number for the rate limit setup.
State	Select **Disabled** or **Enabled** to set the port's state status.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set as the bandwidth rate for the selected port.
Action	Select the Ingress port action to be Drop or Shutdown.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Ingress Bandwidth Control Status** settings.



Figure 3.184 QoS > Rate Limit > Ingress Bandwidth Control Status

3.9.3.2 Egress Bandwidth Control

The Egress Bandwidth Control page allows you to set the egress bandwidth control for a listed port.

To access this page, click **QoS > Rate Limit > Egress Bandwidth Control**.

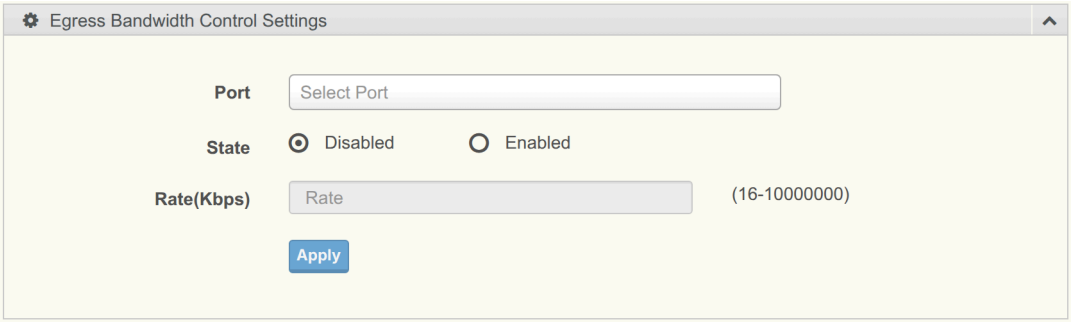


Figure 3.185 QoS > Rate Limit > Egress Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to set the Egress Bandwidth Control.
State	Select **Disabled** or **Enabled** to set the Egress Bandwidth Control state.

Item	Description
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set the Egress Bandwidth rate.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Egress Bandwidth Control Status** settings.
To access this page, click **QoS > Rate Limit > Egress Bandwidth Control**.

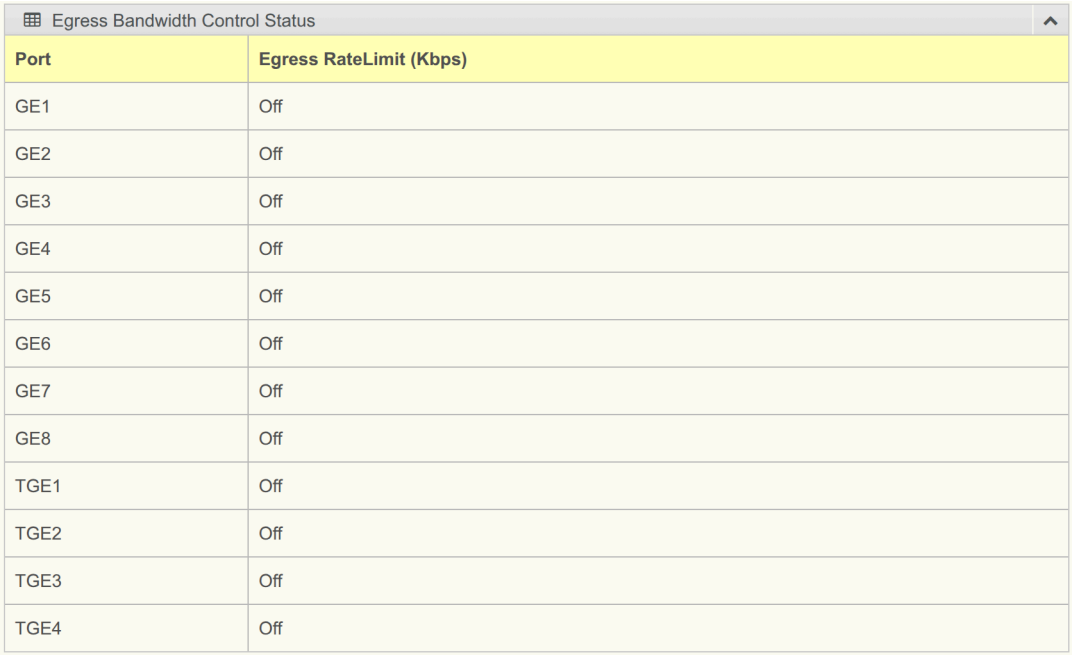


Figure 3.186 QoS > Rate Limit > Egress Bandwidth Control Status

3.9.3.3 Egress Queue

The Egress Queue page allows you to set the egress bandwidth parameters.
To access this page, click **QoS > Rate Limit > Egress Queue**.

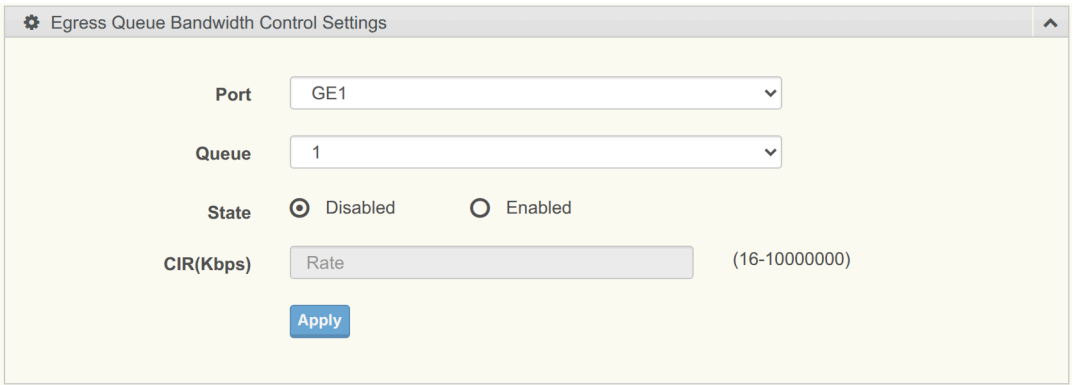


Figure 3.187 QoS > Rate Limit > Egress Queue

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port to define the Egress queue.
Queue	Click the drop-down menu to set the queue order for the Egress setting.
State	Click **Disabled** or **Enabled** to set the Egress queue state.

Item	Description
CIR (Kbps)	Enter the value in Kbps (16 to 1000000) to set the CIR rate for the Egress queue.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Egress Per Queue Status** settings.

GE1 Egress Per Queue Status

Queue Id	Egress RateLimit (Kbps)
1	Off
2	Off
3	Off
4	Off
5	Off
6	Off
7	Off
8	Off

Figure 3.188 QoS > Rate Limit > Egress Per Queue Status

3.10 Management

3.10.1 LLDP

LLDP is a one-way protocol without request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

3.10.1.1 LLDP System Settings

The LLDP System Settings allows you to configure the status (enabled or disabled) for the protocol, set the interval for frame transmission, set the hold time multiplier and the re-initialization delay.

To access this page, click **Management > LLDP > LLDP System Settings**.

Global Settings

Enabled	○ Enabled	◉ Disabled	
LLDP PDU Disable Action	○ Filtering	◉ Bridging	○ Flooding
Transmission Interval	30	(5-32767)	
Holdtime Multiplier	4	(2-10)	
Reinitialization Delay	2	(1-10)	
Transmit Delay	2	(1-8191)	

Apply

Figure 3.189 Management > LLDP > LLDP System Settings

The following table describes the items in the previous figure.

Item	Description
Enabled	Click **Enabled** or **Disabled** to set the Global Settings state.

Item	Description
LLDP PDU Disable Action	Click the drop-down menu to select how LLDP PDUs are handled while LLDP is globally disabled: ■ Filtering: Discard the received LLDP PDUs. ■ Bridging: Forward the received LLDP PDUs within the VLAN. ■ Flooding: Forward the received LLDP PDUs to all ports.
Transmission Interval	Select the interval at which frames are transmitted. The default is 30 seconds, and the valid range is 5 to 32768 seconds.
Holdtime Multiplier	Select the multiplier on the transmit interval to assign to TTL.
Reinitialization Delay	Select the delay length before re-initialization.
Transmit Delay	Select the delay after an LLDP frame is sent.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **LLDP Global Config** settings.

To access this page, click **Management > LLDP > LLDP System Settings**.

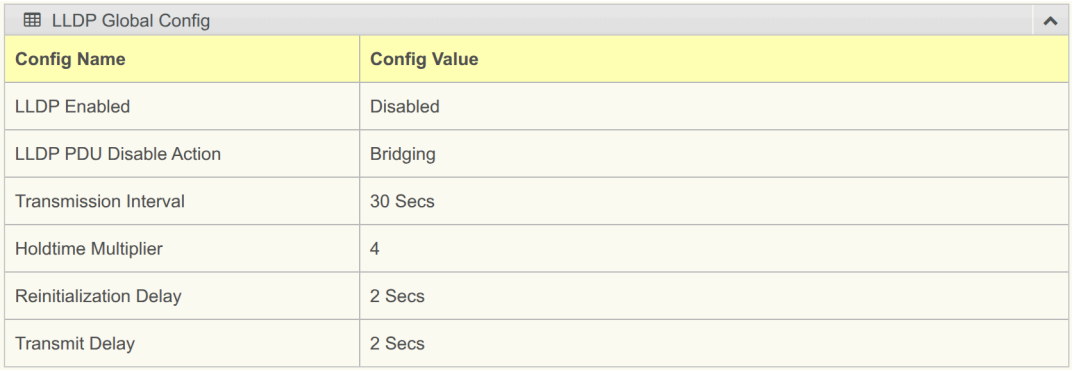


Figure 3.190 Management > LLDP > LLDP Global Config

3.10.1.2 LLDP Port Settings

The LLDP Port Settings page allows you to configure the state (enabled or disabled) of the selected port.

To access this page, click **Management > LLDP > LLDP Port Settings**.



Figure 3.191 Management > LLDP > LLDP Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port number associated with the LLDP setting.
State	Click the drop-down menu to select the LLDP port state.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Optional TLVs Selection** settings.



Figure 3.192 Management > LLDP > Optional TLVs Selection

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the port number associated with the TLV (optional) selection.

Item	Description
Optional TLV Select	Click the drop-down menu to select the LLDP optional TLVs to be carried (multiple selections are allowed). ■ System Name: To include system name TLV in LLDP frames. ■ Port Description: To include port description TLV in LLDP frames. ■ System Description: To include system description TLV in LLDP frames. ■ System Capability: To include system capability TLV in LLDP frames. ■ 802.3 MAC-PHY: To indicate the current duplex and bit rate settings of the device. ■ 802.3 Link Aggregation: To indicate the link can be aggregated. ■ 802.3 Maximum Frame Size: To indicate the maximum frame size capability of the MAC-PHY implementation. ■ Management Address: To select the advertising IP management address. ■ 802.1 PVID: To select to advertise the PVID in the TLV.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **LLDP Port Status** settings.

LLDP Port Status

Port	State	Selected Optional TLVs
GE1	TX&RX	802.1 PVID
GE2	TX&RX	802.1 PVID
GE3	TX&RX	802.1 PVID
GE4	TX&RX	802.1 PVID
GE5	TX&RX	802.1 PVID
GE6	TX&RX	802.1 PVID
GE7	TX&RX	802.1 PVID
GE8	TX&RX	802.1 PVID
TGE1	TX&RX	802.1 PVID
TGE2	TX&RX	802.1 PVID
TGE3	TX&RX	802.1 PVID
TGE4	TX&RX	802.1 PVID

Figure 3.193 Management > LLDP > LLDP Port Status

The following figure displays the **VLAN Name TLV VLAN Selection** settings.

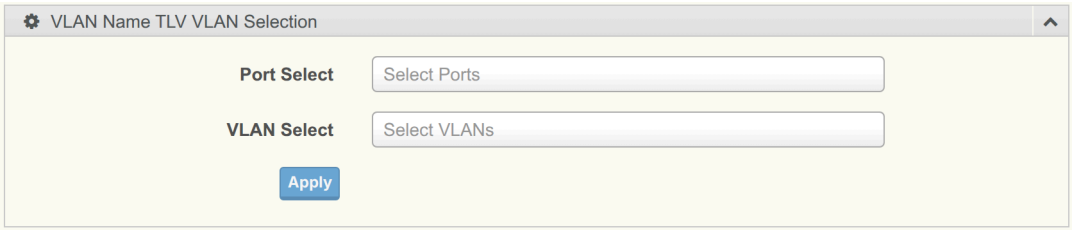


Figure 3.194 Management > LLDP > VLAN Name TLV VLAN Selection

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select the port to which the VLAN Name TLV applies.
VLAN Select	Click the drop-down menu to select the VLAN whose name is advertised in the VLAN Name TLV of the designated port.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **LLDP Port VLAN TLV Status** settings.

LLDP Port VLAN TLV Status

Port	Selected VLAN
GE1	
GE2	
GE3	
GE4	
GE5	
GE6	
GE7	
GE8	
TGE1	
TGE2	
TGE3	
TGE4	

Figure 3.195 Management > LLDP > LLDP Port VLAN TLV Status

3.10.1.3 LLDP Local Device Info

The LLDP Local Device Info page allows you to view information regarding network devices, providing that the switch has already obtained LLDP information on the devices.

The following figure displays the **Local Device Summary** settings.

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

Local Device Summary

Information Name	Information Value
Chassis ID Subtype	MAC Address
Chassis ID	CC:82:7F:F9:4D:A9
System Name	Switch
System Description	switch
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Interface name

Figure 3.196 Management > LLDP > LLDP Local Device Info

The following figure displays the **Port Status** settings. Click **Detail** beside a port to display the complete set of TLVs advertised on that port.

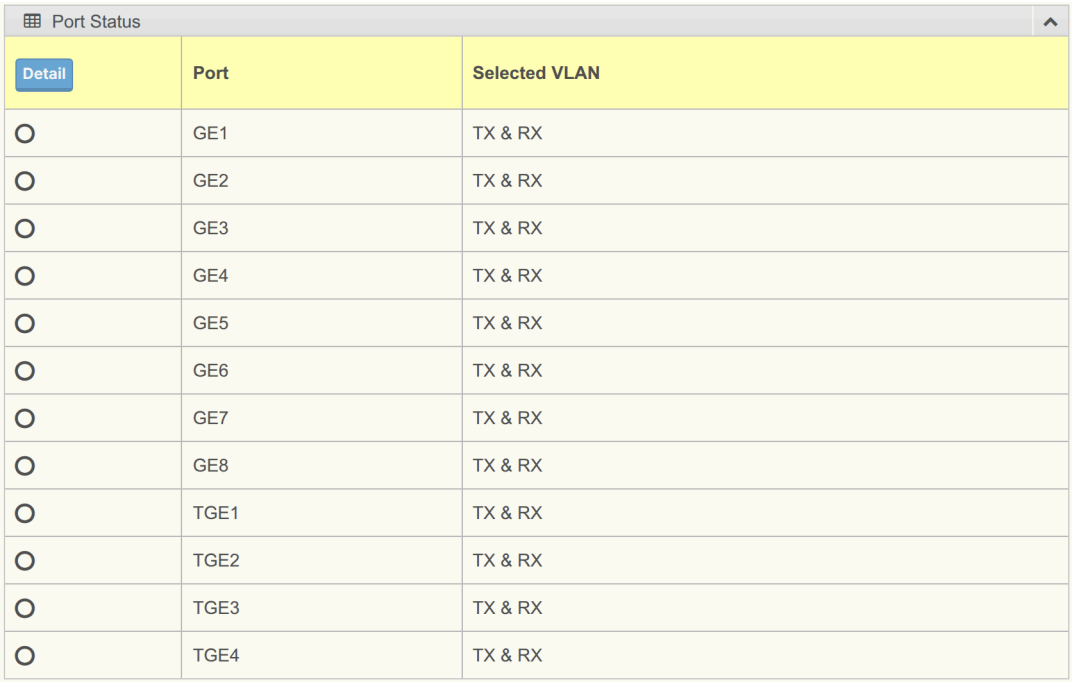


Figure 3.197 Management > LLDP > Port Status

3.10.1.4 LLDP Remote Device Info

The LLDP Remote Device Info page allows you to view information about remote devices, LLDP information must be available on the switch.

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

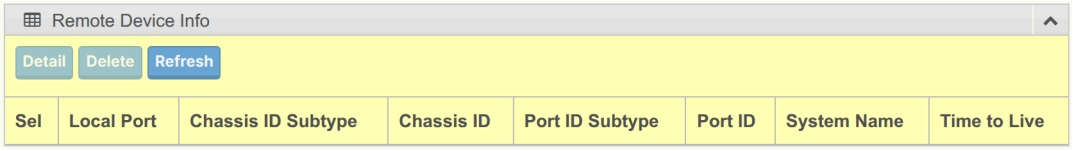


Figure 3.198 Management > LLDP > LLDP Remote Device Info

The following table describes the items in the previous figure.

Item	Description
Detail	Click to display the device details.
Delete	Click to delete the selected devices.
Refresh	Click to refresh the remote device information list.

3.10.1.5 LLDP Overloading

The following figure displays the **LLDP Overloading** settings.

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

LLDP Overloading

Port	Total (Bytes)	Left to Send (Bytes)	Status	Status			
				Mandatory TLVs	802.3 TLVs	Optional TLVs	802.1 TLVs
GE1	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE2	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE3	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE4	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE5	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE6	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE7	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
GE8	29	1459	Not Overloading	21(Transmitted)			8(Transmitted)
TGE1	30	1458	Not Overloading	22(Transmitted)			8(Transmitted)
TGE2	30	1458	Not Overloading	22(Transmitted)			8(Transmitted)
TGE3	30	1458	Not Overloading	22(Transmitted)			8(Transmitted)
TGE4	30	1458	Not Overloading	22(Transmitted)			8(Transmitted)

Figure 3.199 Management > LLDP > LLDP Overloading

3.10.2 SNMP

Simple Network Management Protocol (SNMP) is a protocol to facilitate the monitoring and exchange of management information between network devices. Through SNMP, the health of the network or status of a particular device can be determined.

3.10.2.1 SNMP Settings

The SNMP Settings page allows you to set the SNMP daemon state (enabled or disabled).

To access this page, click **Management > SNMP > SNMP Settings**.

SNMP Global Settings

State ○ Enabled ○ Disabled

Apply

Figure 3.200 Management > SNMP > SNMP Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Enabled** or **Disabled** to define the SNMP daemon.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **SNMP Information** settings.



Figure 3.201 Management > SNMP > SNMP Information

3.10.2.2 SNMP Community

The SNMP Community page provides configuration options for the community.

SNMP v1 and SNMP v2c use the group name (Community Name) certification. It's role is similar to the password function. If SNMP v1 and SNMP v2c are used, you can go directly from the configuration settings to this page to configure the SNMP community.

To access this page, click **Management > SNMP > SNMP Community**.



Figure 3.202 Management > SNMP > SNMP Community

The following table describes the items in the previous figure.

Item	Description
Community Name	Enter a community name (up to 20 characters).
Access Right	Click the radio box to specify the access level (read only or read write)
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Community Status** settings.

To access this page, click **Management > SNMP > SNMP Community**.

Click **Delete** beside an entry to remove that community.

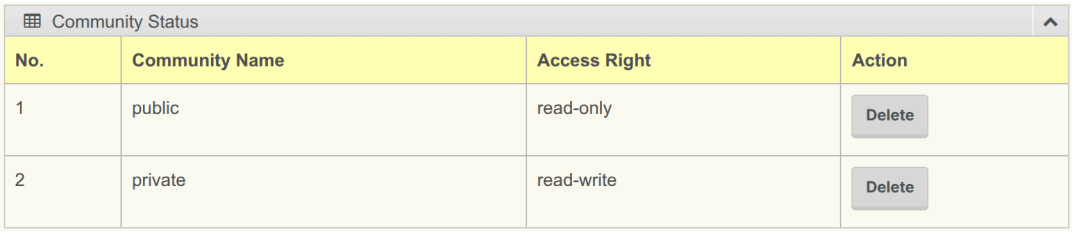


Figure 3.203 Management > SNMP > Community Status

3.10.2.3 SNMPv3 EngineID

To access this page, click **Management > SNMP > SNMPv3 EngineID**.



Figure 3.204 Management > SNMP > SNMPv3 EngineID

The following table describes the items in the previous figure.

Item	Description
SNMP EngineID	Enter the hexadecimal string to define the engine ID for SNMPv3 agent.

3.10.2.4 SNMPv3 Settings

The SNMPv3 Settings page allows you to create SNMP groups. The users have the same level of security and access control permissions as defined by the group settings.

To access this page, click **Management > SNMP > SNMPv3 Settings**.

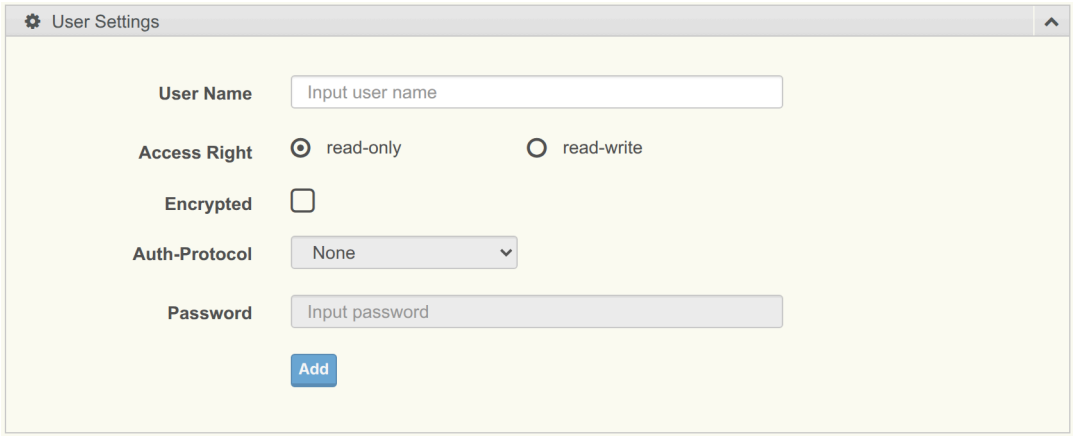


Figure 3.205 Management > SNMP > SNMPv3 Settings

The following table describes the items in the previous figure.

Item	Description
User Name	Enter a user name (up to 32 characters) to create an SNMP profile.
Access Right	Click **read-only** or **read-write** to define the access right for the profile.
Encrypted	Click the option to set the encrypted option for the user setting.
Auth-Protocol	Click the drop-down menu to select the authentication level: MD5 or SHA. The field requires a user password. ■ MD5: specify HMAC-MD5-96 authentication level ■ SHA: specify HMAC-SHA authentication protocol
Password	Enter the characters to define the password associated with the authentication protocol.
Add	Click **Add** to save the values and update the screen.

The following figure displays the **User Status** settings.

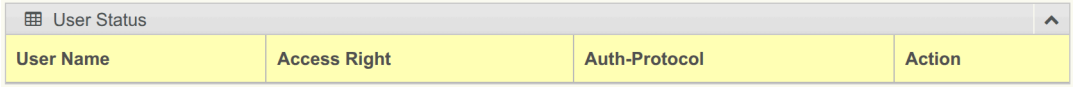


Figure 3.206 Management > SNMP > User Status

3.10.2.5 SNMP Trap

The SNMP Trap page allows you to set the IP address of the node and the SNMP credentials corresponding to the version that is included in the trap message.

To access this page, click **Management > SNMP > SNMP Trap**.

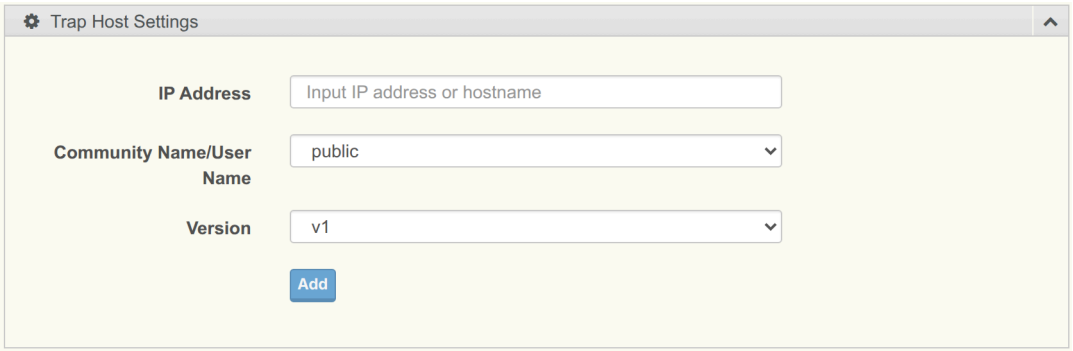


Figure 3.207 Management > SNMP > SNMP Trap

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the IP address to designate the SNMP trap host.
Community Name/ User Name	Click the drop-down menu to select a defined community name.
Version	Click the drop-down menu to designate the SNMP version credentials (v1, v2c - trap, v2c - inform, v2c - trap or v2c - inform).
Add	Click **Add** to save the values and update the screen.

The following figure displays the **Trap Host Status** settings.

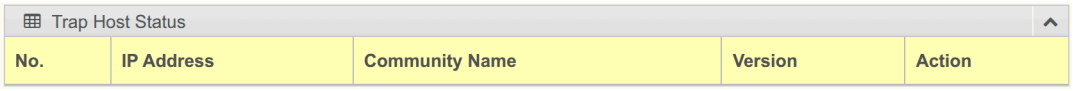


Figure 3.208 Management > SNMP > Trap Host Status

3.10.3 Power of Ethernet

Power Over Ethernet is the function supplying power to Powered Devices (PD) through the switch in the event that AC power is not readily available.

Power over Ethernet can be used for the following areas:

- Surveillance devices
- I/O sensors for security requirements
- Wireless access points

Power over Ethernet is available on the models whose name contains a P. On a model without Power over Ethernet, this menu is not displayed.

Series	Supported Models
EKI-87xx	EKI-8712G-4XFPI, EKI-8720G-4XFPI
EKI-95xx	Models ordered with a Power over Ethernet line card, for example EKI-9520G-RPW and EKI-9508G-MPW

3.10.3.1 PoE System Settings

The PoE System Settings page allows you to configure the overload disconnect and the maximum available wattage.

To access this page, click **Management > Power of Ethernet > PoE System Settings**.

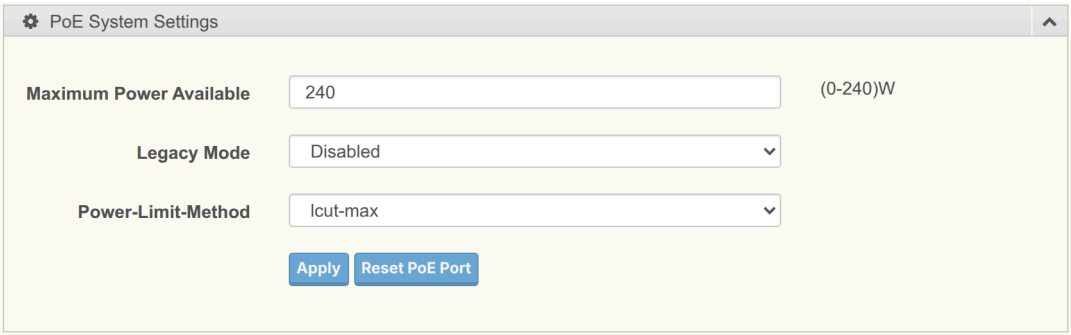


Figure 3.209 Management > Power of Ethernet > PoE System Settings

The following table describes the items in the previous figure.

Item	Description
Maximum Power Available	Select the value in Watts to set the maximum available power.
Legacy Mode	Select **Enabled** or **Disabled** to accept powered devices that do not comply with the IEEE detection signature.
Power-Limit-Method	Click the drop-down menu to select how the power limit of a port is determined: ■ user-defined-power-limit: Use the limit entered on the PoE Port Settings page. ■ power-limit-from-class: Use the class advertised by the powered device. ■ lcut-max: Use the maximum the port is able to deliver.
Apply	Click **Apply** to save the values and update the screen.
Reset PoE Port	Click **Reset PoE Port** to remove and restore the power delivered to the ports.

The following figure displays the **PoE System Information** settings.

PoE System Information

Information Name	Information Value
Actual Power Consumption	0.0 W
Current Power Available	240.0 W
Maximum Power Available	240.0 W
Legacy Mode	Disabled
Overload Disconnect Type	Overload Port First
PoE Port Power Limit Method(PLFC)	LCUT Max(According to port behavior)

Figure 3.210 Management > Power of Ethernet > PoE System Information

3.10.3.2 PoE Port Settings

The PoE Port Settings page allows you to configure the port status, its power limitations, legacy mode status, and power limit settings.

To access this page, click **Management > Power of Ethernet > PoE Port Settings**.

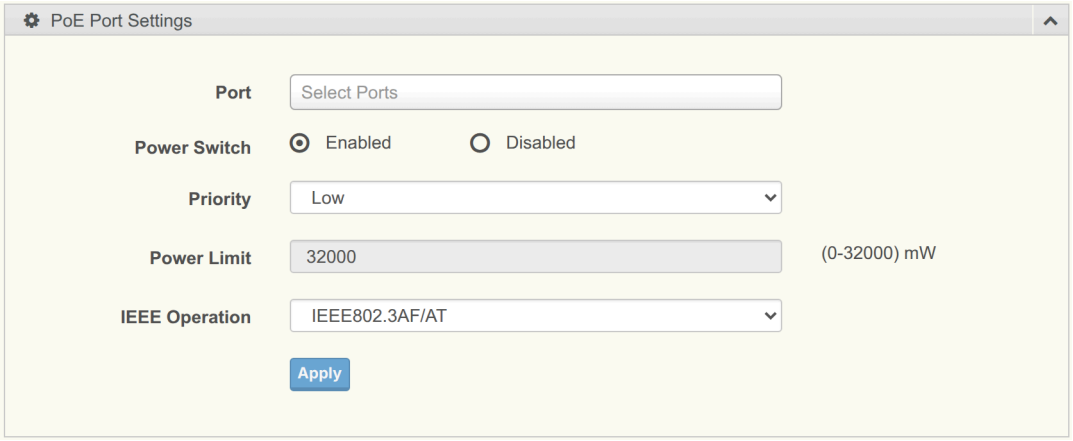


Figure 3.211 Management > Power of Ethernet > PoE Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select a PoE port.
Power Switch	Select **Enabled** or **Disabled** to designate the PoE port function by ports.
Priority	Click the drop-down menu to configure the power supply priority: **Critical, Low, Medium** or **High**. Default is **Low**.
Power Limit	Enter a number to set the port power current limitation to be given to the Powered Device (PD)
IEEE Operation	Click the drop-down menu to select the IEEE standard the port operates under when supplying power.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **PoE Port Config Information** settings.

PoE Port Config Information

Port	Switch State	Priority	Power Limit(W)	IEEE Operation Type
GE1	Enabled	Low	32.000	IEEE802.3AF/AT
GE2	Enabled	Low	32.000	IEEE802.3AF/AT
GE3	Enabled	Low	32.000	IEEE802.3AF/AT
GE4	Enabled	Low	32.000	IEEE802.3AF/AT
GE5	Enabled	Low	32.000	IEEE802.3AF/AT
GE6	Enabled	Low	32.000	IEEE802.3AF/AT
GE7	Enabled	Low	32.000	IEEE802.3AF/AT
GE8	Enabled	Low	32.000	IEEE802.3AF/AT

Figure 3.212 Management > Power of Ethernet > PoE Port Config Information

3.10.3.3 PoE Port Status

The following figure displays the **PoE Port Status** settings.

To access this page, click **Management > Power of Ethernet > PoE Port Status**.

PoE Port Status

Port	Current (mA)	Voltage (V)	Power (W)

Figure 3.213 Management > Power of Ethernet > PoE Port Status

3.10.3.4 PoE Failure Check

The PoE Failure Check page allows the switch to poll a powered device with ICMP requests and to act on the port when the device stops responding. This allows a device that has stopped responding, but is still drawing power, to be recovered without manual intervention.

To access this page, click **Management > Power of Ethernet > PoE Failure Check**.

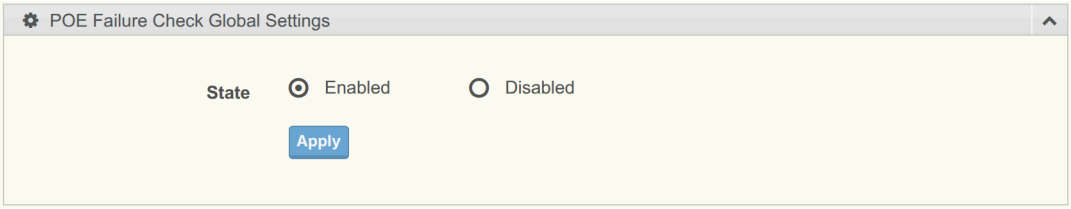


Figure 3.214 Management > Power of Ethernet > PoE Failure Check

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the PoE failure check function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **POE Failure Check Device Setting** settings.

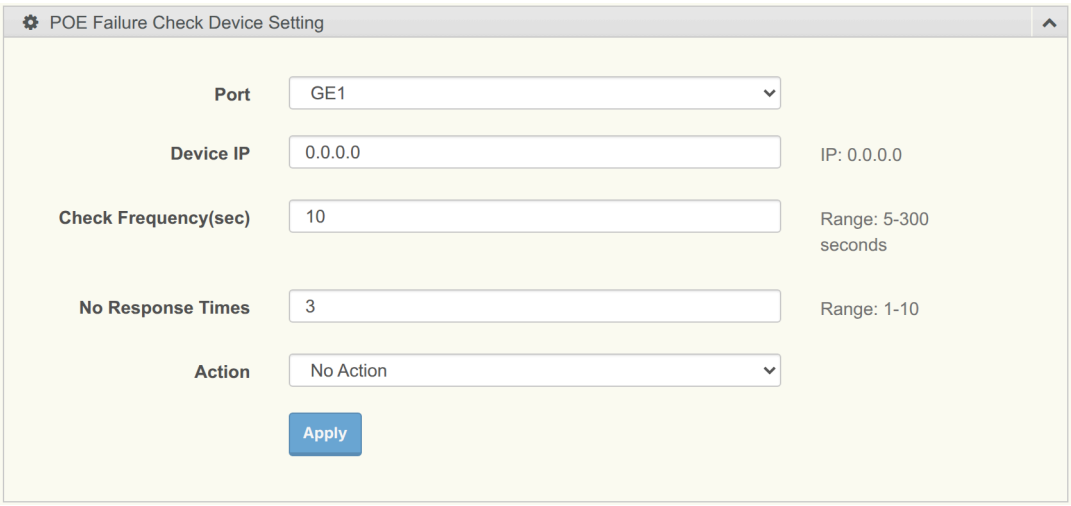


Figure 3.215 Management > Power of Ethernet > POE Failure Check Device Setting

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port on which the check is performed.
Device IP	Enter a value to specify the IP address of the powered device to be polled.
Check Frequency(sec)	Enter a value to specify the interval between two checks, in seconds.
No Response Times	Enter a value to specify how many consecutive failed checks are required before the action is taken.
Action	Click the drop-down menu to select the action taken when the device stops responding, such as restarting the power delivered to the port.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **POE Failure Check Entry Table** settings.

POE Failure Check Entry Table

Port	PoE Supported	Enable	Device IP	Check Frequency(sec)	No Response Times	Action	Modify
gi 1	YES	Disabled	0.0.0.0	0	0	None	None
gi 2	YES	Disabled	0.0.0.0	0	0	None	None
gi 3	YES	Disabled	0.0.0.0	0	0	None	None
gi 4	YES	Disabled	0.0.0.0	0	0	None	None
gi 5	YES	Disabled	0.0.0.0	0	0	None	None
gi 6	YES	Disabled	0.0.0.0	0	0	None	None
gi 7	YES	Disabled	0.0.0.0	0	0	None	None
gi 8	YES	Disabled	0.0.0.0	0	0	None	None

Figure 3.216 Management > Power of Ethernet > POE Failure Check Entry Table

3.10.3.5 PoE Failure Check Status

The PoE Failure Check Status page displays the current result of the PoE failure check for each port, including how many times the powered device has failed to respond. The information is for review only.

The following figure displays the **PoE Failure Check Status** settings. Click **Refresh** to update the screen.

To access this page, click **Management > Power of Ethernet > PoE Failure Check Status**.

PoE Failure Check Status

Port	Device IP	Status	Failure Count	No Response Times
Watchdog is disabled or no data available				

Refresh

Figure 3.217 Management > Power of Ethernet > PoE Failure Check Status

3.10.4 TCP Modbus

The TCP Modbus function allows for client-server communication between a switch module (server) and a device in the networking running MODBUS client software (client).

To access this page, click **Management > TCP Modbus**.

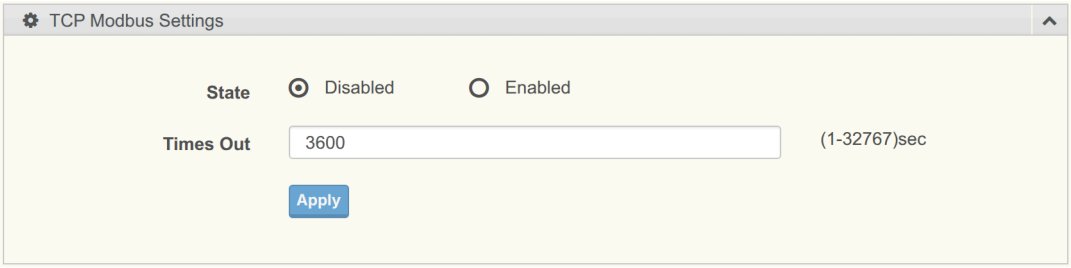


Figure 3.218 Management > TCP Modbus

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the TCP Modbus function.
Times Out	Enter a value to specify the time the switch waits before closing an idle TCP Modbus connection, in seconds.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **TCP Modbus Status** settings.

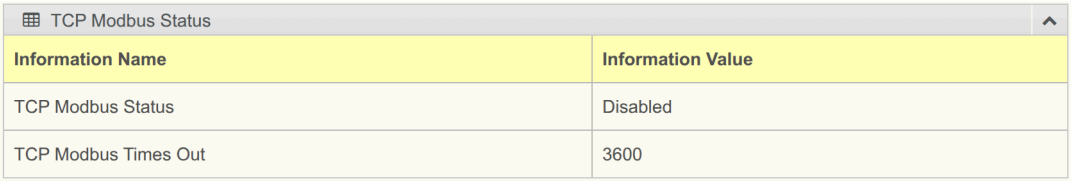


Figure 3.219 Management > TCP Modbus Status

3.10.5 DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is a network protocol enabling a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

3.10.5.1 Status Settings

The Status Settings page allows you to configure the DHCP server mode (enabled or disabled).

To access this page, click **Management > DHCP Server > Status Settings**.

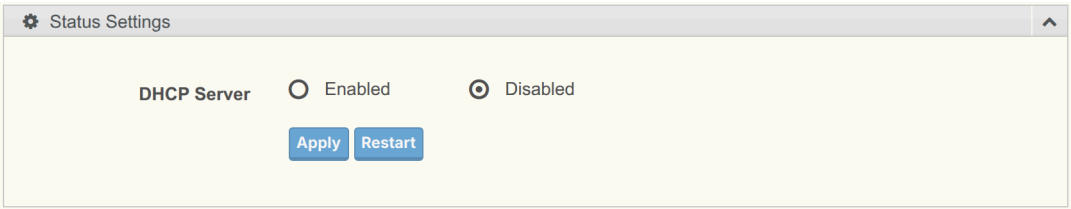


Figure 3.220 Management > DHCP Server > Status Settings

The following table describes the items in the previous figure.

Item	Description
DHCP Server	Select **Enable** or **Disable** to designate the DHCP server function type. When a new DHCP server mode is selected, the switch requires a system restart for the new mode to take effect.
Apply	Click **Apply** to save the values and update the screen.

Item	Description
Restart	Click **Restart** to have the switch perform a system restart function. In the event that the IP settings are changed, the DHCP server must be restarted for the IP settings to take effect.

The following figure displays the **Status Information** settings.



Figure 3.221 Management > DHCP Server > Status Information

3.10.5.2 Global Settings

The Global Settings page allows you to configure the global settings for the DHCP function.

To access this page, click **Management > DHCP Server > Global Settings**.

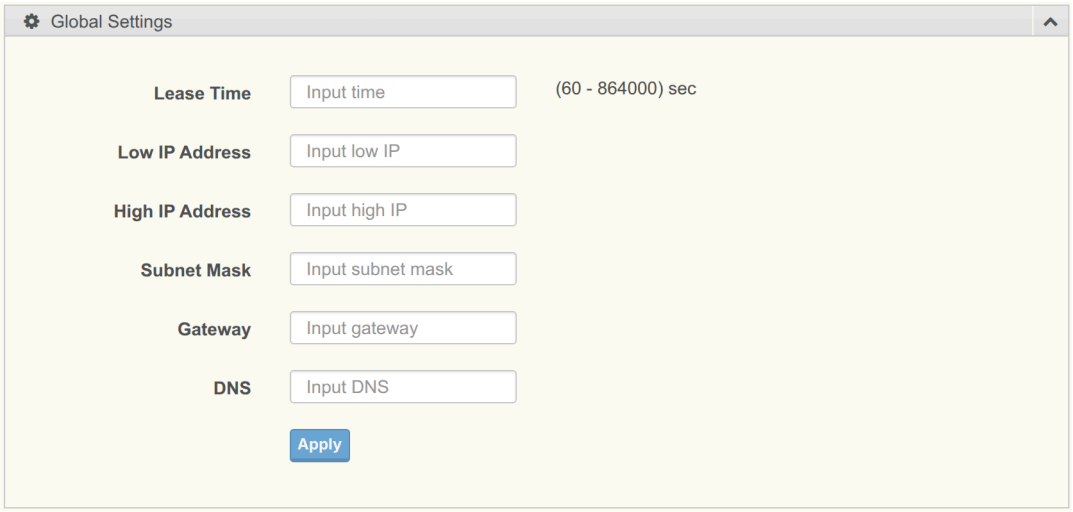


Figure 3.222 Management > DHCP Server > Global Settings

The following table describes the items in the previous figure.

Item	Description
Lease Time	Type in the value designating the lease time (60 - 864000) in seconds for each setting lease.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Global Information** settings.

To access this page, click **Management > DHCP Server > Global Settings**.

Click **Clear** to remove the addresses that the server has leased.

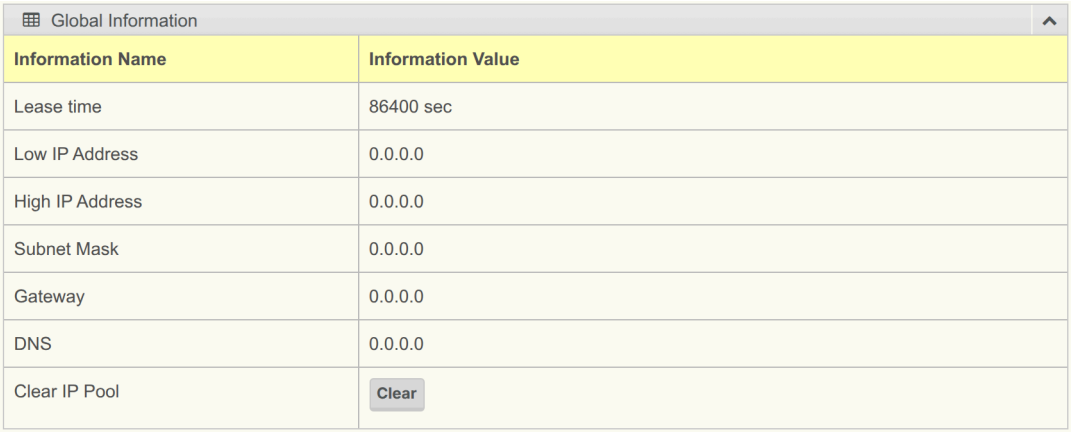


Figure 3.223 Management > DHCP Server > Global Information

3.10.5.3 Port Settings

The Port Settings page allows you to configure selected ports for the DHCP function.

To access this page, click **Management > DHCP Server > Port Settings**.

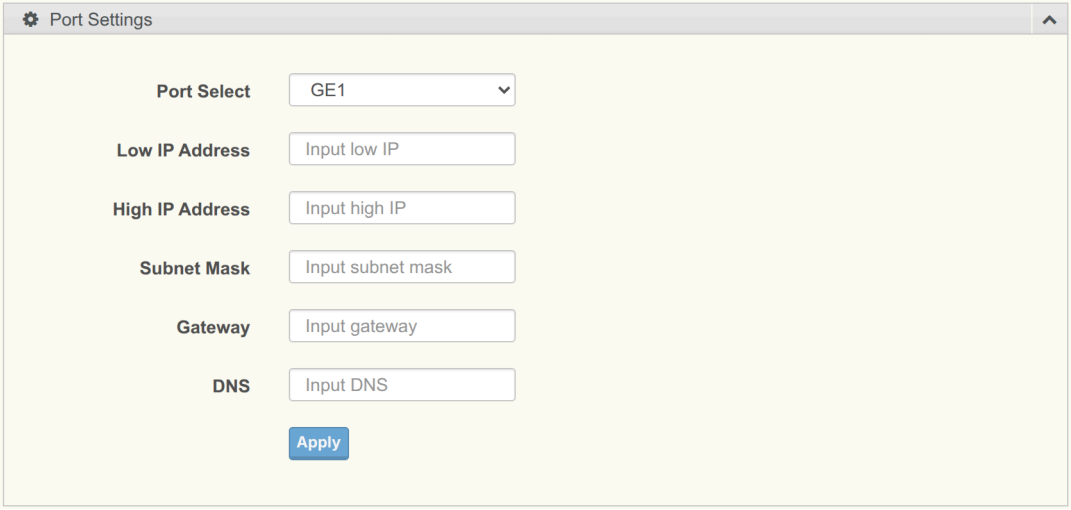


Figure 3.224 Management > DHCP Server > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Click the drop-down menu to select a pre-defined port to configure. The sub options are designated for the selected port.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Enter a value to specify the subnet mask assigned to the clients of this port.
Gateway	Enter a value to specify the default gateway assigned to the clients of this port.
DNS	Enter a value to specify the DNS server assigned to the clients of this port.
Apply	Click **Apply** to save the values and update the screen.

Click **Edit** beside a port to modify its address pool, or **Clear** to remove it.

The following figure displays the **Port Information** settings.

Port Information

Port	Low IP Address	High IP Address	Subnet Mask	Gateway	DNS	Modify
GE1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE3	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE4	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE5	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE6	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE7	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
GE8	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
TGE1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
TGE2	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
TGE3	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear
TGE4	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Edit Clear

Figure 3.225 Management > DHCP Server > Port Information

3.10.5.4 VLAN Settings

The VLAN Settings page allows you to define a separate DHCP address pool for each VLAN, so that clients receive an address, gateway and DNS server appropriate to the VLAN they are attached to.

To access this page, click **Management > DHCP Server > VLAN Settings**.

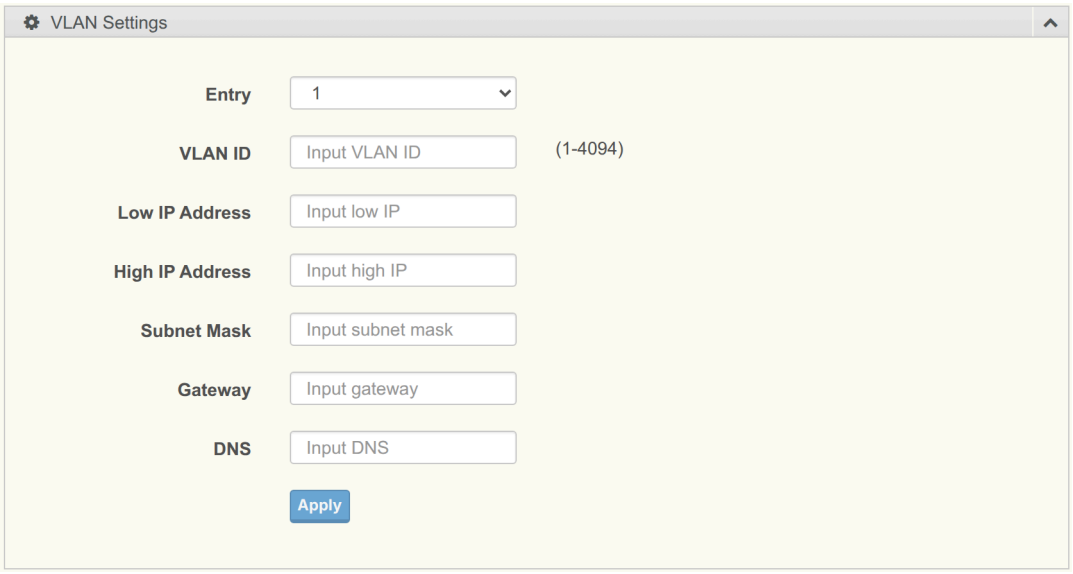


Figure 3.226 Management > DHCP Server > VLAN Settings

The following table describes the items in the previous figure.

Item	Description
Entry	Enter a value to specify the entry number of the address pool.

Item	Description
VLAN ID	Enter a value to specify the VLAN served by this address pool, ranging from 1 to 4094.
Low IP Address	Enter a value to specify the first address of the pool.
High IP Address	Enter a value to specify the last address of the pool.
Subnet Mask	Enter a value to specify the subnet mask assigned to the clients.
Gateway	Enter a value to specify the default gateway assigned to the clients.
DNS	Enter a value to specify the DNS server assigned to the clients.
Apply	Click **Apply** to save the values and update the screen.

Click **Edit** beside an entry to modify it, or **Clear** to remove it.

The following figure displays the **Entry Information** settings.

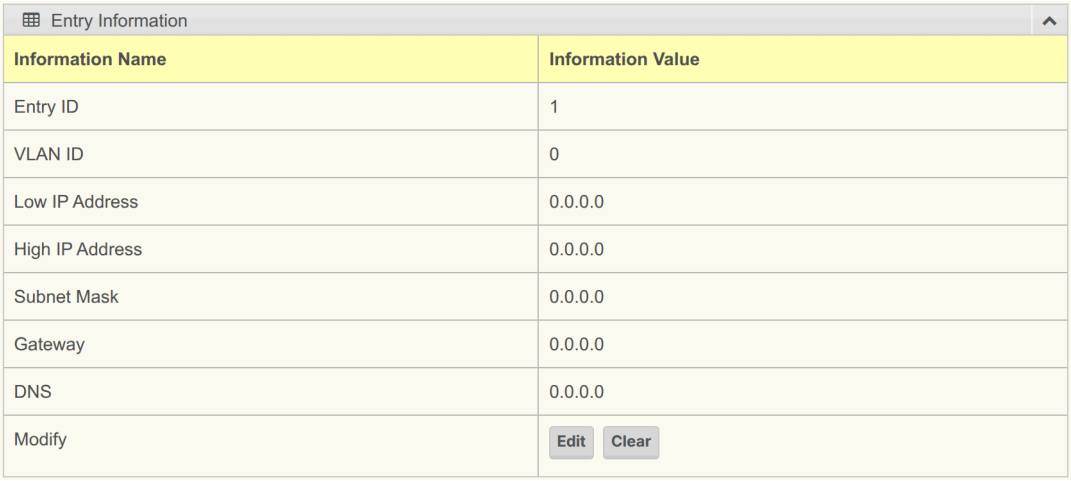


Figure 3.227 Management > DHCP Server > Entry Information

3.10.5.5 Option 82 Settings

The Option 82 Settings, also known as the DHCP relay agent information option, provide information about the network location of a DHCP client. In turn, the DHCP server uses the information to implement IP addresses or other parameters for the client.

To access this page, click **Management > DHCP Server > Option 82 Settings**.

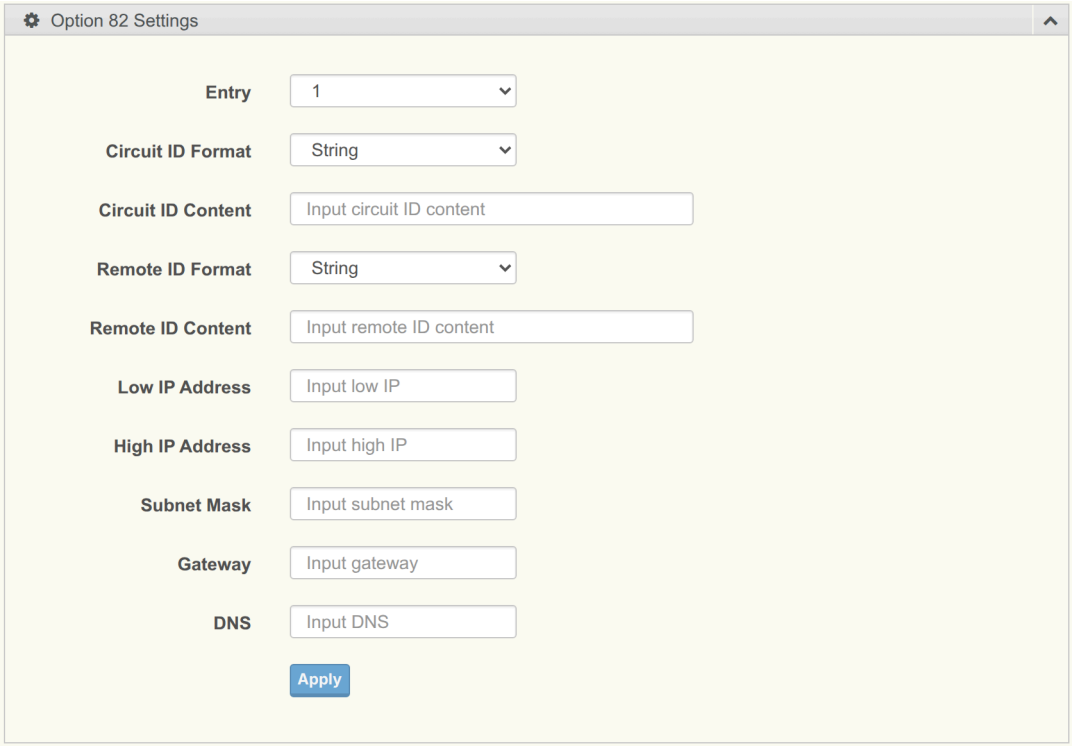


Figure 3.228 Management > DHCP Server > Option 82 Settings

The following table describes the items in the previous figure.

Item	Description
Entry	Click the drop-down menu to select an entry for the Option 82 setting.
Circuit ID Format	Click the drop-down menu to select the format of the circuit ID: string or hex.
Circuit ID Content	Enter the circuit ID string on the switch on which the request was received.
Remote ID Format	Click the drop-down menu to select the format of the remote ID: string or hex.
Remote ID Content	Enter the remote ID string of the host.
Low IP Address	Type in the value designating the lowest range in the IP address pool.
High IP Address	Type in the value designating the highest range in the IP address pool.
Subnet Mask	Type in the value designating the subnet mask for the IP address pool.
Gateway	Type in the value designating the gateway for the IP address pool.
DNS	Type in the value designating the DNS for the IP address pool.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Entry Information** settings.

To access this page, click **Management > DHCP Server > Option 82 Settings**.

Click **Edit** beside an entry to modify it, or **Clear** to remove it.

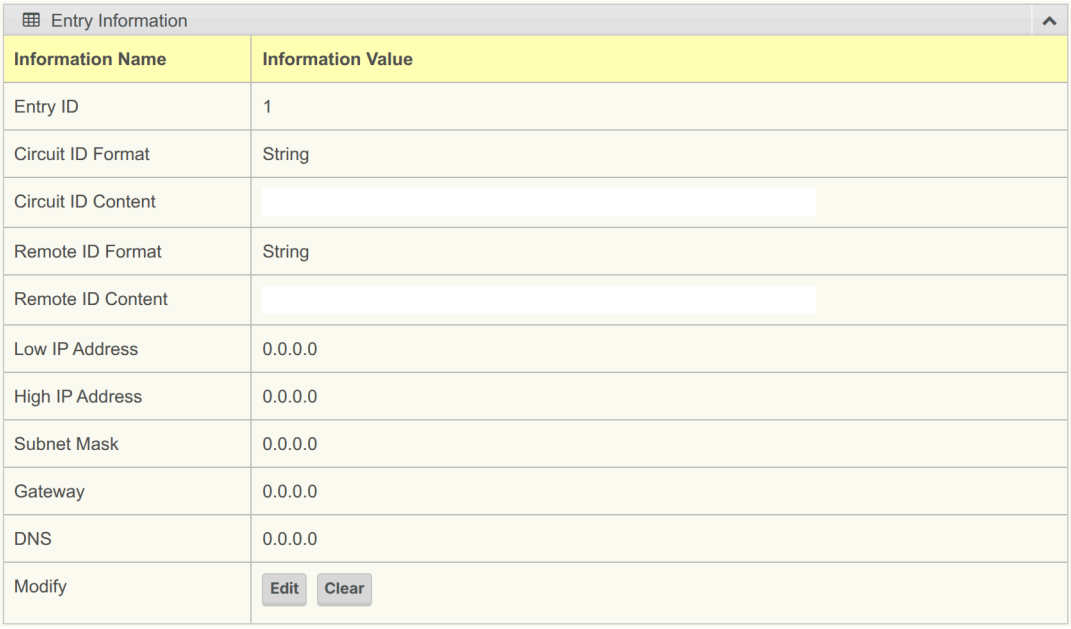


Figure 3.229 Management > DHCP Server > Entry Information

3.10.5.6 Client MAC Settings

To access this page, click **Management > DHCP Server > Client MAC Settings**.

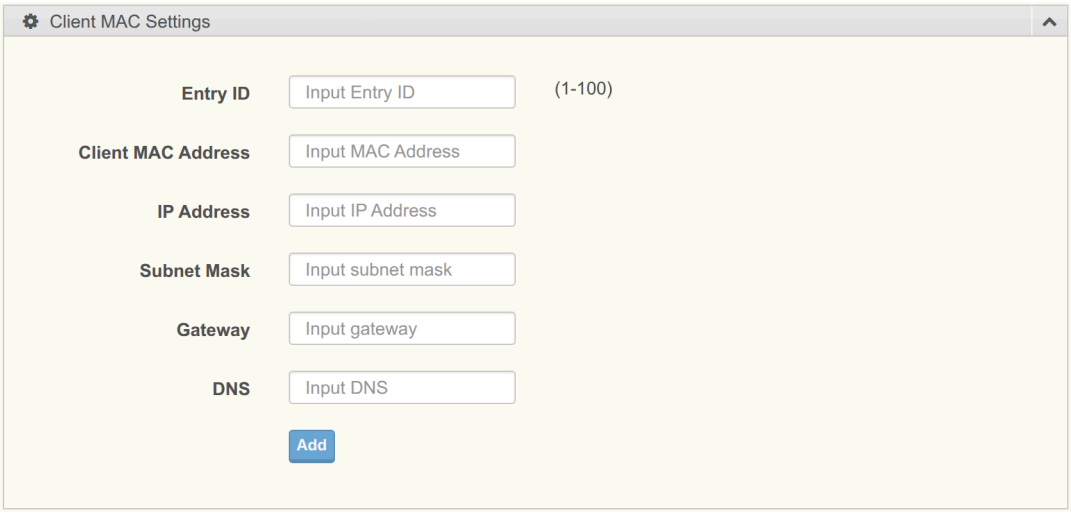


Figure 3.230 Management > DHCP Server > Client MAC Settings

The following table describes the items in the previous figure.

Item	Description
Entry ID	Type in the value designating the entry ID.
Client MAC Address	Enter the MAC address for DHCP server.
IP Address	Enter a value to specify the IP address of the interface.
Subnet Mask	Enter a value to specify the IP subnet mask for the interface.
Gateway	Enter a value to specify the gateway for the interface.
DNS	Enter a value to specify the DNS server for the interface.
Add	Click **Add** to add the entry and update the screen.

The following figure displays the **Client MAC Information** settings. Click **Detail** to display the detail information of desired entry id or **Delete** to delete the desired entry id.

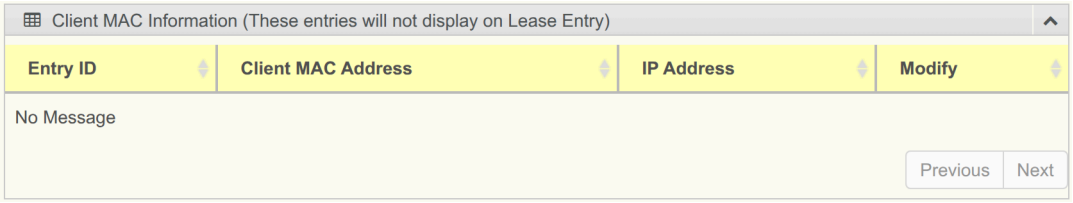


Figure 3.231 Management > DHCP Server > Client MAC Information

3.10.5.7 Lease Entry

The following figure displays the **Lease entry Table** settings.

To access this page, click **Management > DHCP Server > Lease Entry**.

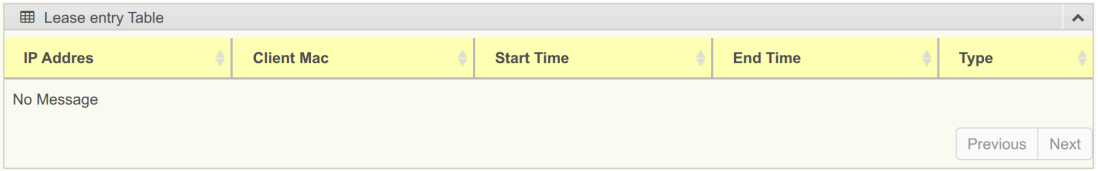


Figure 3.232 Management > DHCP Server > Lease Entry

3.10.6 SMTP Client

Simple Mail Transfer Protocol (SMTP) is a protocol to send e-mail messages between servers. SMTP is used to send messages from a mail client to a mail server. SMTP by default uses TCP port 25.

3.10.6.1 Global Settings

The Global Settings page allows you to set the active profile for the SMTP client.

To access this page, click **Management > SMTP Client > Global Settings**.



Figure 3.233 Management > SMTP Client > Global Settings

The following table describes the items in the previous figure.

Item	Description
Active Profile	Click the drop-down menu to select the profile status (None, 1 or 2).
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **SMTP Information** settings.



Figure 3.234 Management > SMTP Client > SMTP Information

3.10.6.2 Profile Settings

The Profile Settings page allows you to select the server IP, the server port, and sender mail for the listed profile.

To access this page, click **Management > SMTP Client > Profile Settings**.

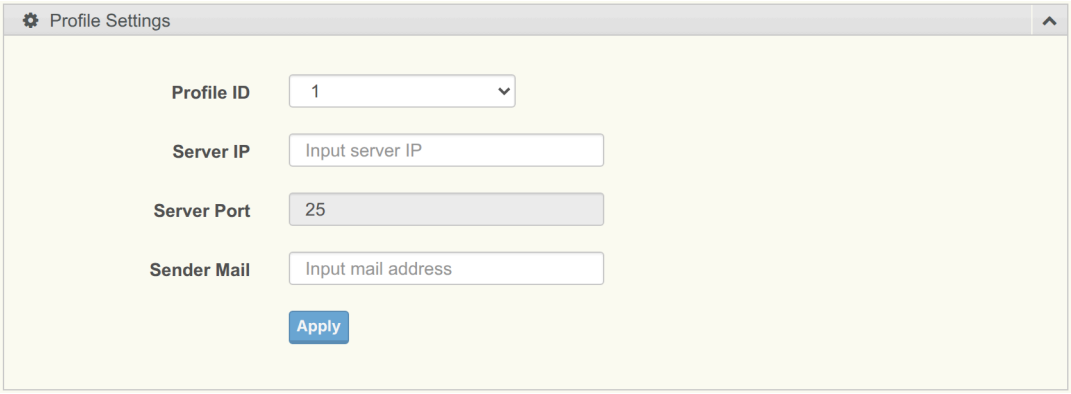


Figure 3.235 Management > SMTP Client > Profile Settings

The following table describes the items in the previous figure.

Item	Description
Profile ID	Click the drop-down menu to select the identification type for the profile (1 or 2).
Server IP	Enter the IP address to designate the server host.
Server Port	Enter the port number to designate the port associated with the server IP address.
Sender Mail	Enter the email address of the sender client.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Profile Target Mail Settings** settings.

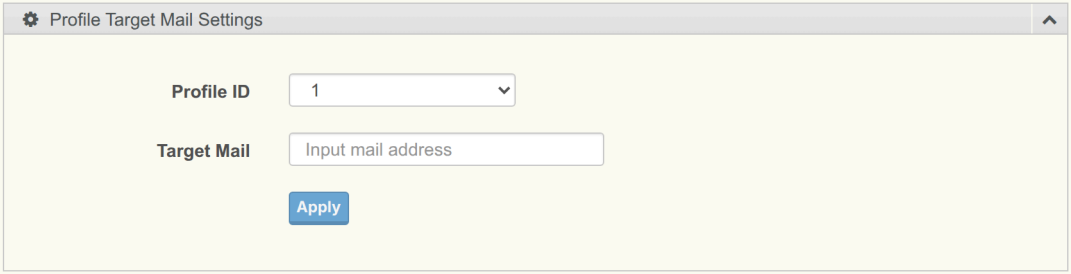


Figure 3.236 Management > SMTP Client > Profile Target Mail Settings

The following table describes the items in the previous figure.

Item	Description
Profile ID	Click the drop-down menu to select the identification type for the profile (1 or 2).
Target Mail	Enter the email address of the target client.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Profile Information** settings.

To access this page, click **Management > SMTP Client > Profile Settings > Profile Target Mail Settings**.

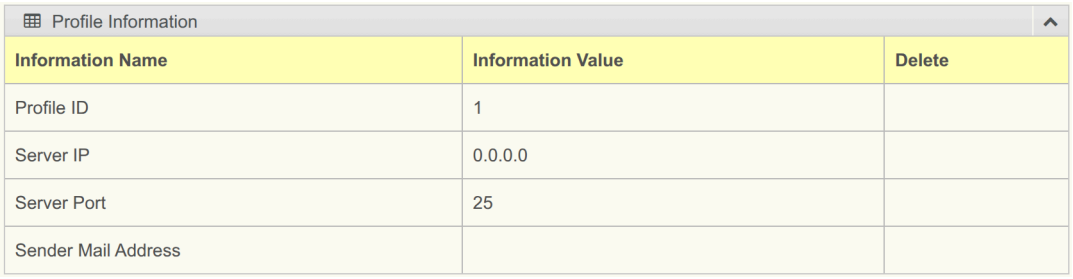


Figure 3.237 Management > SMTP Client > Profile Information

3.10.6.3 Sending Message

The Sending Message page allows you to setup the log message for use with the SMTP client.

To access this page, click **Management > SMTP Client > Sending Message**.

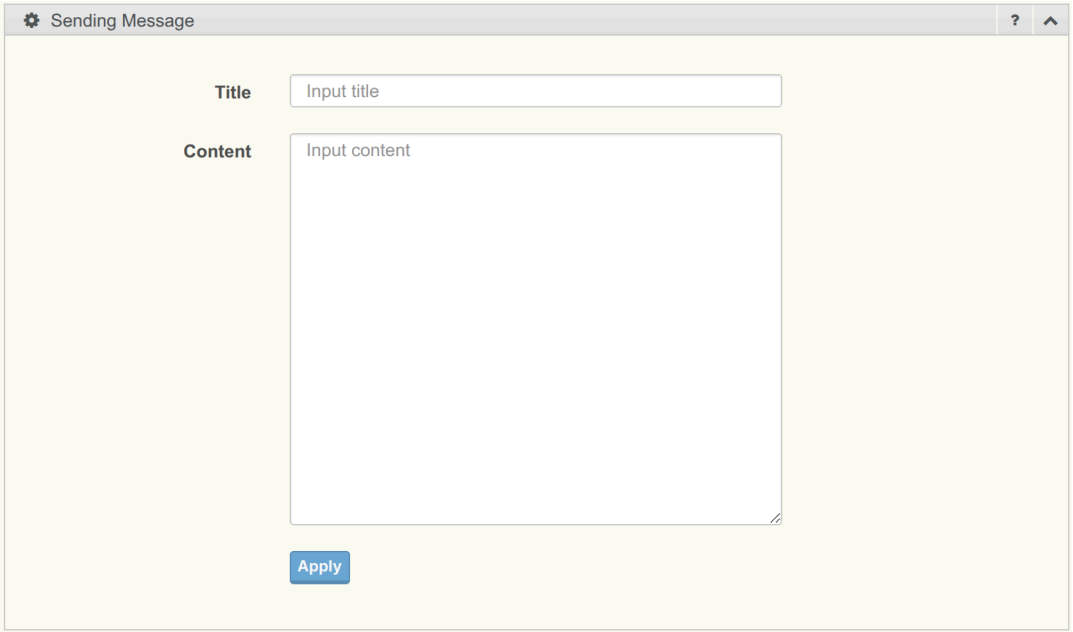


Figure 3.238 Management > SMTP Client > Sending Message

The following table describes the items in the previous figure.

Item	Description
Title	Assign the title of the email. The maximum length is 20 characters (alphanumeric, symbols (. (dot), _ (underline), - (dash line) and space).
Content	Assign the content of the email. The maximum length is 64 characters (alphanumeric, symbols (. (dot), _ (underline), - (dash line) and space).
Apply	Click **Apply** to save the values and update the screen.

3.10.7 NTP Server

To access this page, click **Management > NTP Server**.

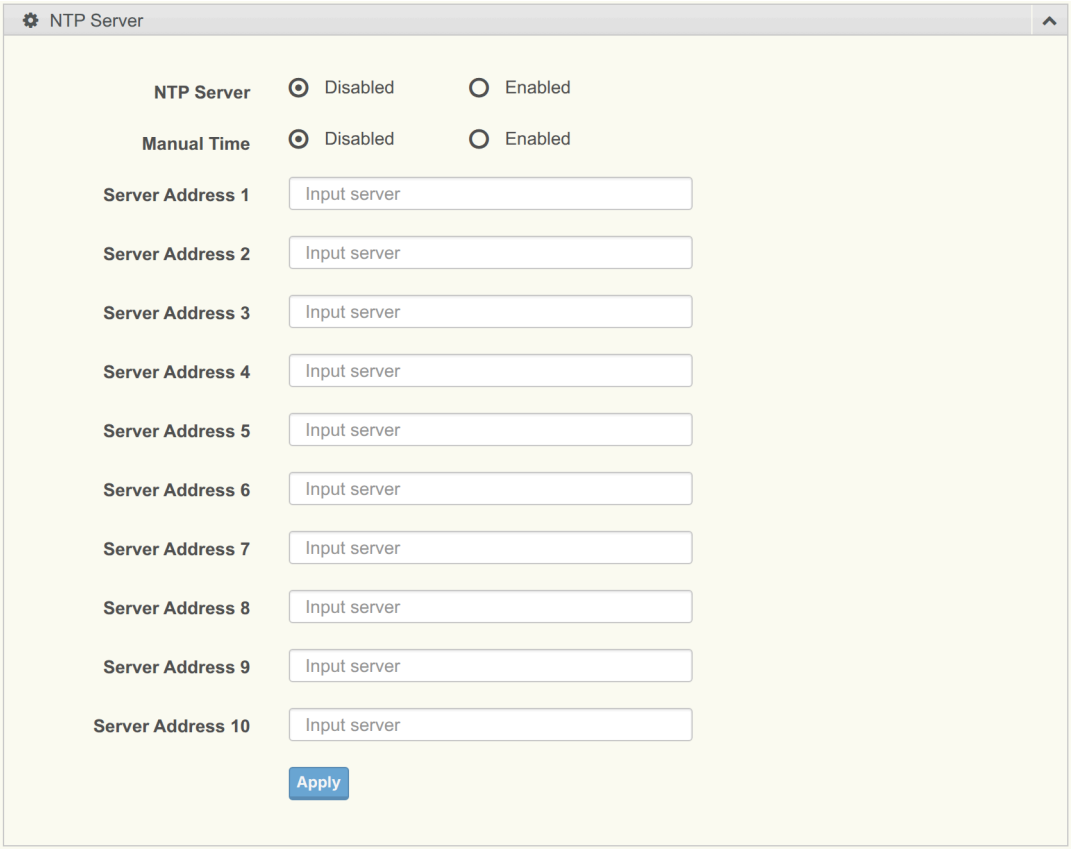


Figure 3.239 Management > NTP Server

The following table describes the items in the previous figure.

Item	Description
Link to System Time page	Click the link to open the System Time page, where the time source of the switch is selected.
NTP Server	Click the radio button to enable or disable the NTP server function.
Manual Time	Click the radio button to enable or disable the manual time function.
Server Address 1 ~ Server Address 10	Enter the address of the NTP server. This is a text string of up to 64 characters containing the encoded unicast IP address or hostname of a NTP server.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **NTP Server Status** settings.

NTP Server Status

Information Name	Information Value
NTP Server Status	Disabled
Manual Time	Disabled
Server Address	Information Value
Server 1	
Server 2	
Server 3	
Server 4	
Server 5	
Server 6	
Server 7	
Server 8	
Server 9	
Server 10	

Figure 3.240 Management > NTP Server Status

3.10.8 Goose

The Goose menu allows you to monitor GOOSE (Generic Object Oriented Substation Event) messages defined by IEC 61850. The switch learns the GOOSE publishers on the network, can lock the learned entries so that an unexpected publisher is rejected, and can give GOOSE traffic a dedicated egress priority.

3.10.8.1 Goose Settings

The Goose Settings page allows you to enable GOOSE message checking, to lock the learned GOOSE address table, and to define how long a learned entry is retained when the publisher stops transmitting.

To access this page, click **Management > Goose > Goose Settings**.

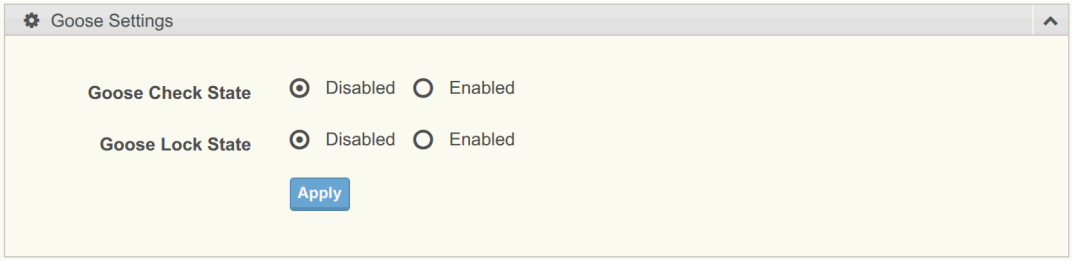


Figure 3.241 Management > Goose > Goose Settings

The following table describes the items in the previous figure.

Item	Description
Goose Check State	Select **Enabled** or **Disabled** to setup the GOOSE message checking function.
Goose Lock State	Select **Enabled** or **Disabled** to lock the GOOSE address table. When the table is locked, no new GOOSE publisher is learned.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Goose Age Configuration** settings.

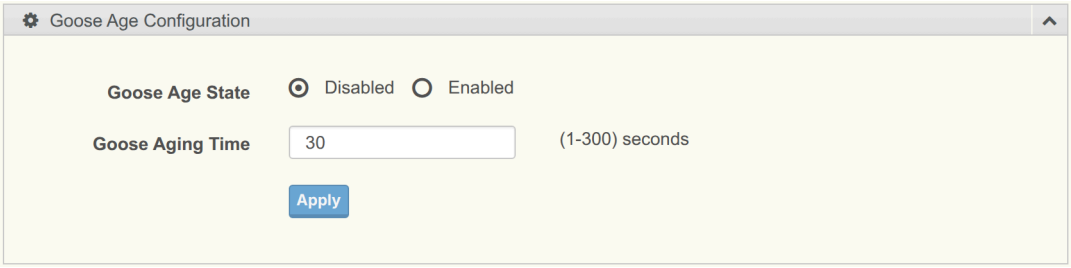


Figure 3.242 Management > Goose > Goose Age Configuration

The following table describes the items in the previous figure.

Item	Description
Goose Age State	Select **Enabled** or **Disabled** to setup the aging of learned GOOSE entries.
Goose Aging Time	Enter a value to specify how long a learned GOOSE entry is retained after the last message from the publisher, in seconds.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Goose Information** settings.

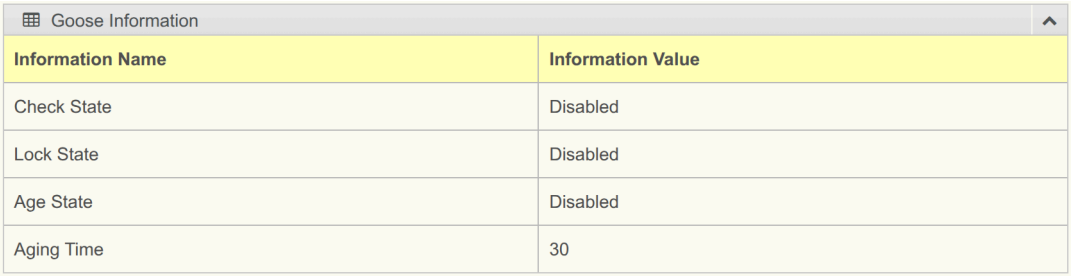


Figure 3.243 Management > Goose > Goose Information

3.10.8.2 Goose Qos Settings

The Goose Qos Settings page allows you to assign a dedicated egress queue priority to GOOSE traffic, so that substation event messages are not delayed by ordinary traffic.

To access this page, click **Management > Goose > Goose Qos Settings**.

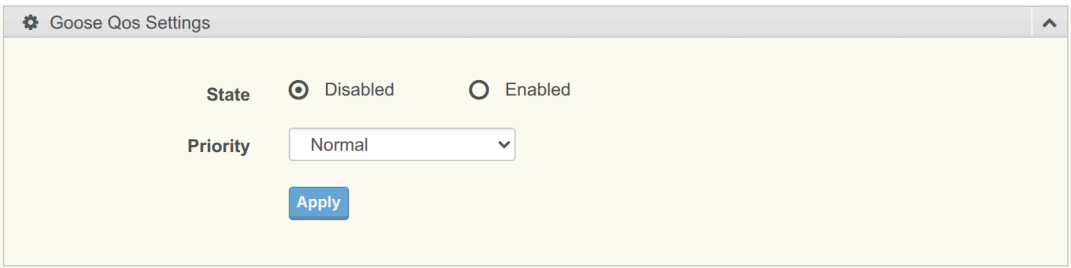


Figure 3.244 Management > Goose > Goose Qos Settings

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the GOOSE QoS function.
Priority	Click the drop-down menu to select the queue assigned to GOOSE traffic: Low, Normal, Medium or High.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Goose Qos Information** settings.

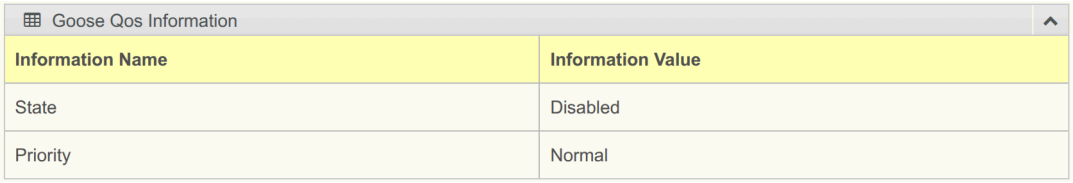


Figure 3.245 Management > Goose > Goose Qos Information

3.10.8.3 Goose MAC Table

The Goose MAC Table page allows you to add a GOOSE publisher to the address table by hand, so that the entry survives a lock of the table. The lower table lists the publishers currently known to the switch, whether they were learned dynamically or entered statically.

To access this page, click **Management > Goose > Goose MAC Table**.

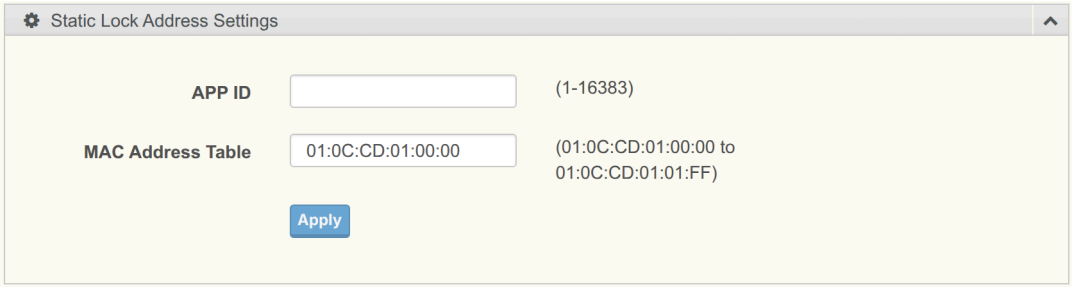


Figure 3.246 Management > Goose > Goose MAC Table

The following table describes the items in the previous figure.

Item	Description
APP ID	Enter a value to specify the application identifier of the GOOSE publisher.
MAC Address Table	Enter a value to specify the MAC address of the GOOSE publisher.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Goose Monitoring Table** settings.

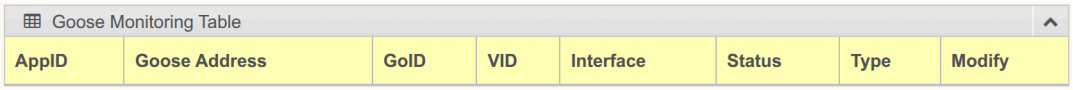


Figure 3.247 Management > Goose > Goose Monitoring Table

3.10.9 DNS Server

The DNS Server menu allows the switch to act as a DNS server for the hosts attached to it, resolving the names defined in its own host table.

3.10.9.1 DNS Server Settings

The DNS Server Settings page allows you to enable the DNS server function of the switch.

To access this page, click **Management > DNS Server > DNS Server Settings**.

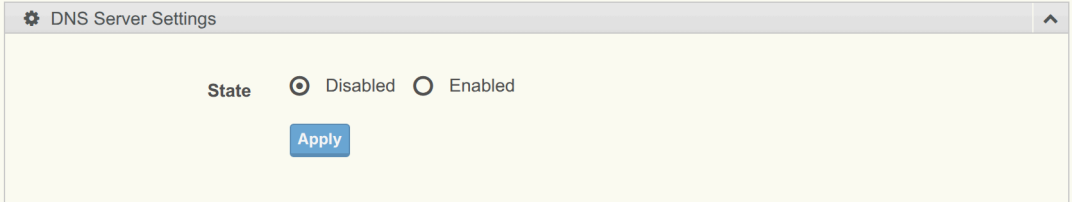


Figure 3.248 Management > DNS Server > DNS Server Settings

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the DNS server function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **DNS Server Information** settings.

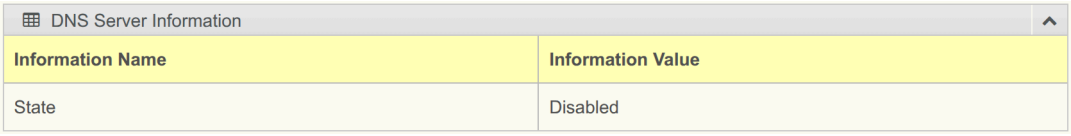


Figure 3.249 Management > DNS Server > DNS Server Information

3.10.9.2 DNS Server Host Table

The DNS Server Host Table page allows you to map a host name to an IP address, so that the switch can answer queries for that name.

To access this page, click **Management > DNS Server > DNS Server Host Table**.

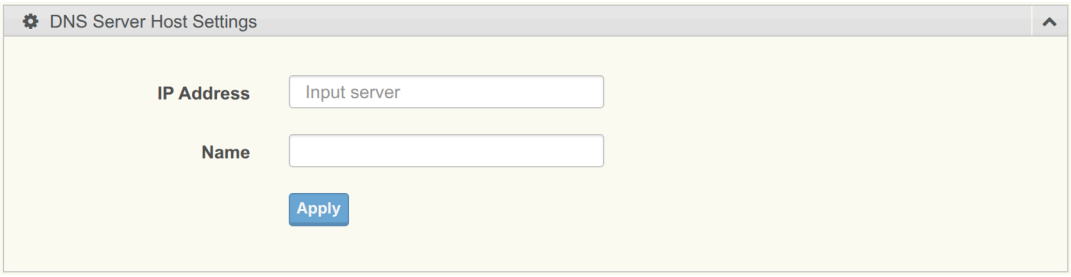


Figure 3.250 Management > DNS Server > DNS Server Host Table

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter a value to specify the IP address returned for the host name.
Name	Enter a value to specify the host name to be resolved.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **DNS Server Host Table** settings.

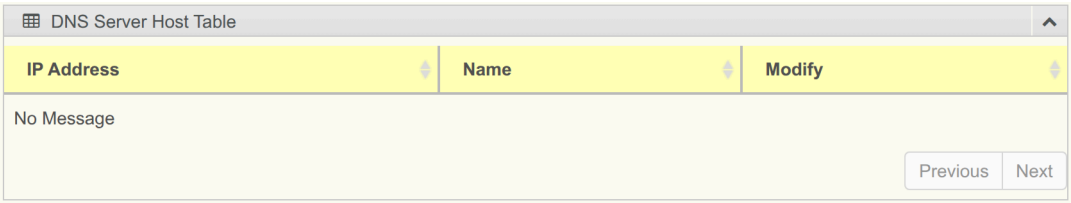


Figure 3.251 Management > DNS Server > DNS Server Host Table

3.11 Diagnostics

Through the Diagnostics function configuration of settings for the switch diagnostics is available.

3.11.1 Cable Diagnostic

The Cable Diagnostics page allows you to select the port for applying a copper test.

To access this page, click **Diagnostics > Cable Diagnostic**.



Figure 3.252 Diagnostics > Cable Diagnostic

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select a pre-defined port for diagnostic testing. Giga ports are displayed with a channel A to D designation.
Copper Test	Click **Copper Test** to display the test result for the selected port.

The following figure displays the **Test Results** settings.

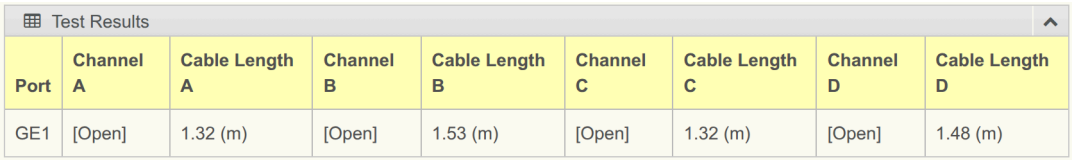


Figure 3.253 Diagnostics > Test Results

3.11.2 Ping Test

The Ping Test page allows you to configure the test log page.

To access this page, click **Diagnostics > Ping Test**.

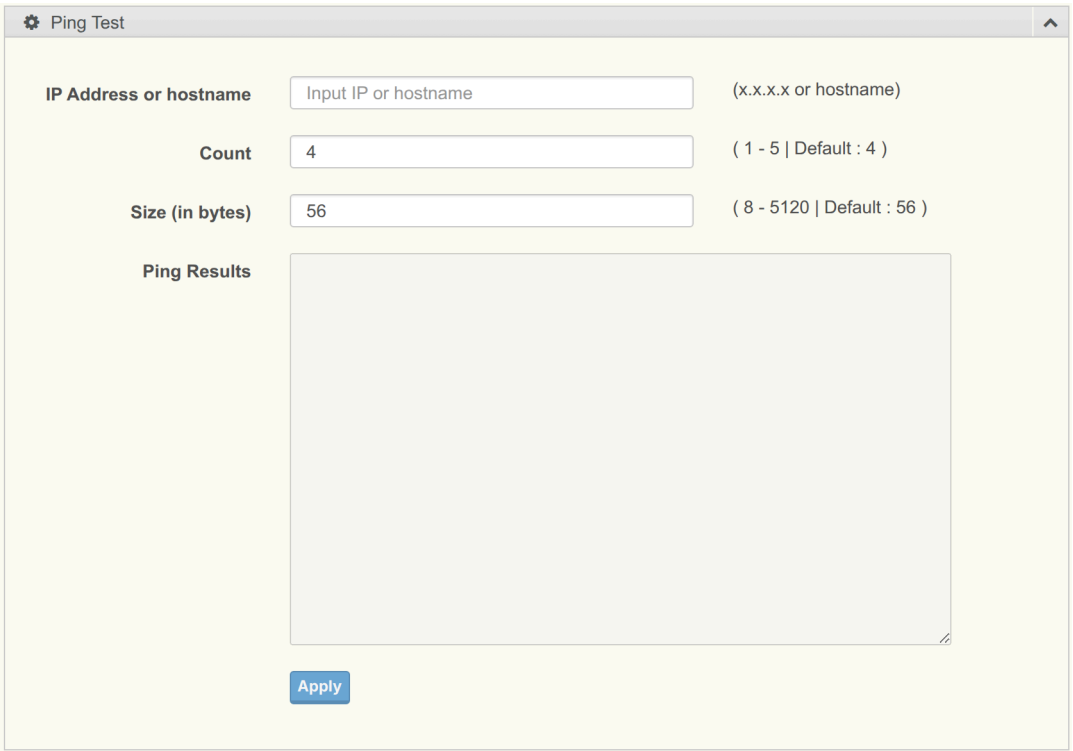


Figure 3.254 Diagnostics > Ping Test

The following table describes the items in the previous figure.

Item	Description
IP Address or host-name	Enter the IP address or host name of the station to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with periods. Each label must be between 1 and 63 characters long, maximum of 64 characters.
Count	Enter the number of echo requests to send. The default value is 4. The value ranges from 1 to 5. The count entered is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size entered is not retained across a power cycle.
Ping Results	Display the reply format of ping. PING 172.17.8.254 (172.17.8.254): 56 data bytes — 172.17.8.254 ping statistics — 4 packets transmitted, 0 packets received, 100% packet loss Or PING 172.17.8.93 (172.17.8.93): 56 data bytes 64 bytes from 172.17.8.93: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=3 ttl=128 time=0.0 ms — 172.17.8.93 ping statistics — 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
Apply	Click **Apply** to display ping result for the IP address.

3.11.3 IPv6 Ping Test

The IPv6 Ping Test page allows you to configure the Ping Test for IPv6.

To access this page, click **Diagnostics > IPv6 Ping Test**.

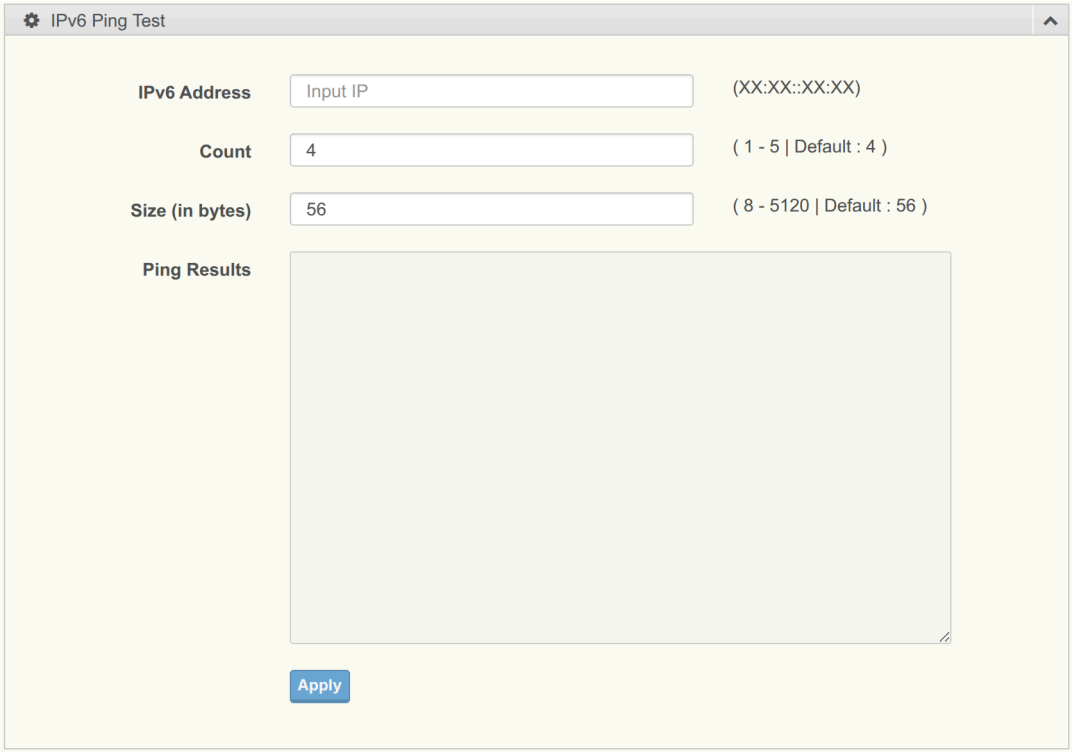


Figure 3.255 Diagnostics > IPv6 Ping Test

The following table describes the items in the previous figure.

Item	Description
IPv6 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. Host names 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 64 characters.
Count	Enter the number of echo requests you want to send. The default value is 4. The value ranges from 1 to 5. The count you enter is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size you enter is not retained across a power cycle.
Ping Results	Display the reply format of ping. PING 2222::777 (2222::777): 56 data bytes — 2222::777 ping statistics — 4 packets transmitted, 0 packets received, 100% packet loss Or PING 2222::717 (2222::717): 56 data bytes 64 bytes from 2222::717: icmp6_seq=0 ttl=128 time=10.0 ms 64 bytes from 2222::717: icmp6_seq=1 ttl=128 time=0.0 ms 64 bytes from 2222::717: icmp6_seq=2 ttl=128 time=0.0 ms 64 bytes from 2222::717: icmp6_seq=3 ttl=128 time=0.0 ms — 2222::717 ping statistics — 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.0/2.5/10.0 ms
Apply	Click **Apply** to display ping result for the IP address.

3.11.4 System Log

3.11.4.1 Logging Service

The Logging Service page allows you to setup the logging services feature for the system log.

To access this page, click **Diagnostics > System Log > Logging Service**.

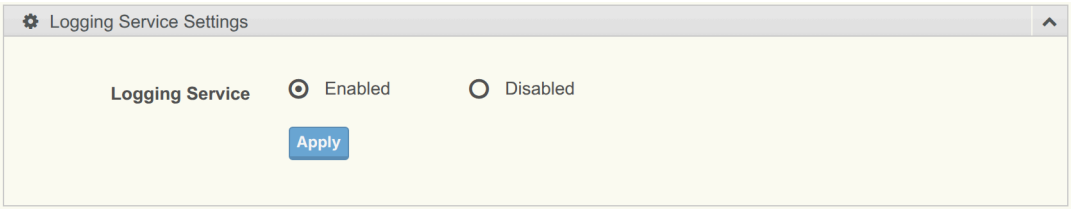


Figure 3.256 Diagnostics > System Log > Logging Service

The following table describes the items in the previous figure.

Item	Description
Logging Service	Click Enabled or Disabled to set the Logging Service status.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Logging Information** settings.



Figure 3.257 Diagnostics > System Log > Logging Information

3.11.4.2 Local Logging

The Local Logging page allows you to designate a local target when the severity criteria is reached.

To access this page, click **Diagnostics > System Log > Local Logging**.



Figure 3.258 Diagnostics > System Log > Local Logging

The following table describes the items in the previous figure.

Item	Description
Target	Enter the local logging target.

Item	Description
Severity	Click the drop-down menu to select the severity level for local log messages. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity ■ alert: Indicates action must be taken immediately ■ crit: 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
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Local Logging Setting Status** settings. Click **Delete** to remove the desired entry.

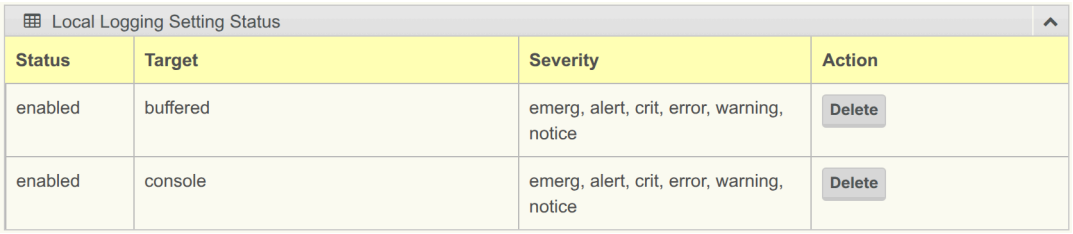


Figure 3.259 Diagnostics > System Log > Local Logging Setting Status

3.11.4.3 System Log Server

The System Log Server page allows you to configure the log server.

To access this page, click **Diagnostics > System Log > System Log Server**.

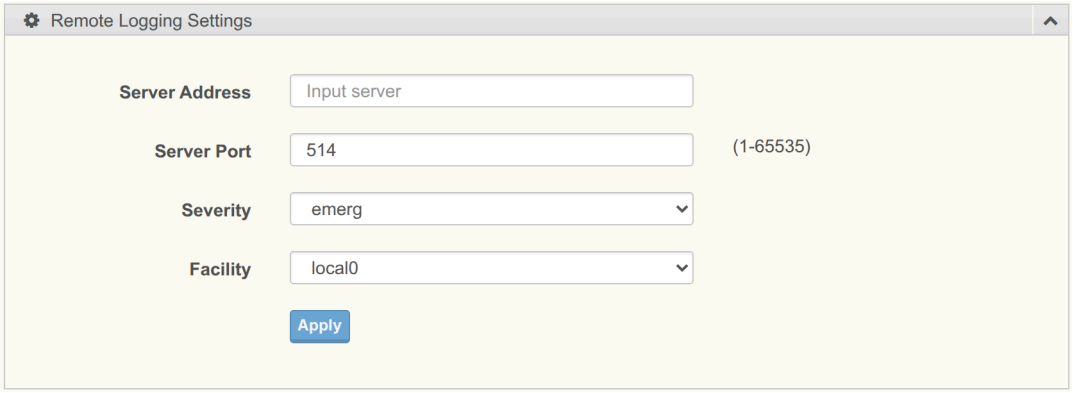


Figure 3.260 Diagnostics > System Log > System Log Server

The following table describes the items in the previous figure.

Item	Description
Server Address	Enter the IP address of the log server.
Server Port	Enter the Udp port number of the log server.

Item	Description
Severity	Click the drop-down menu to select the severity level for local log messages. The default is emerg. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity ■ alert: Indicates action must be taken immediately ■ crit: 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
Facility	Click the drop-down menu to select facility to which the message refers.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Remote Logging Setting Status** settings.

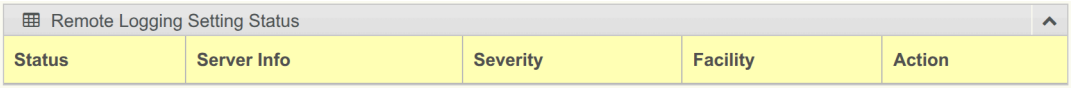


Figure 3.261 Diagnostics > System Log > Remote Logging Setting Status

3.11.5 DDM

The DDM page allows you to setup the diagnostic alarm status.

To access this page, click **Diagnostics > DDM**.



Figure 3.262 Diagnostics > DDM

The following table describes the items in the previous figure.

Item	Description
Diagnostic Alarm	Click the drop-down menu to designate the announcement method: Disabled, SysLog, E-mail, or SNMP.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Diagnostic Alarm Information** settings.

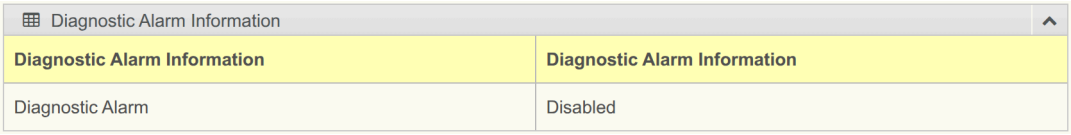


Figure 3.263 Diagnostics > Diagnostic Alarm Information

The following figure displays the **DMI INFO** settings.

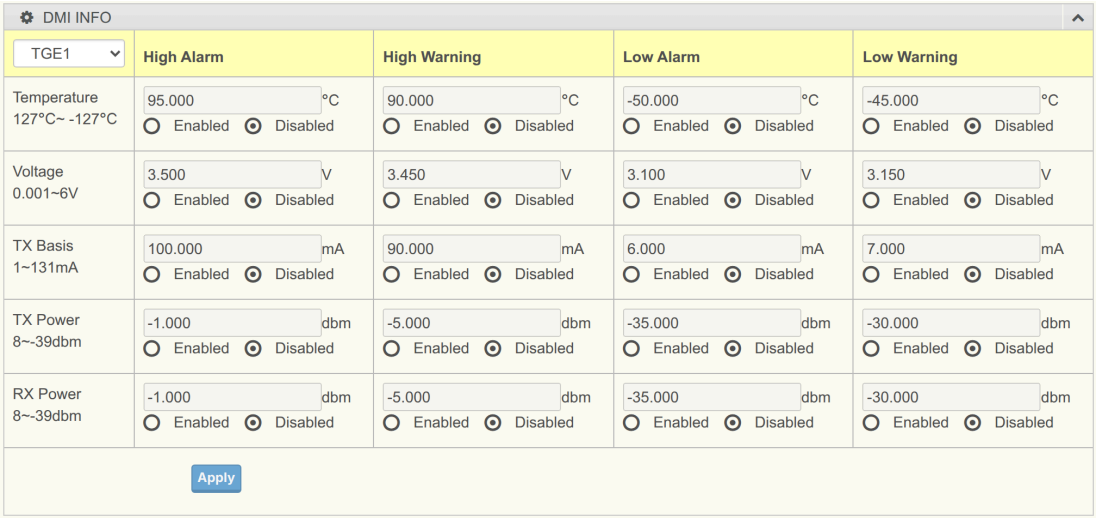


Figure 3.264 Diagnostics > DMI INFO

The following table describes the items in the previous figure.

Item	Description
Enabled	Click the radio button of each measured value (Temperature, Voltage, TX Bias, TX Power and RX Power) to enable or disable the alarm for that value on the designated port.
High Alarm	Click **Enabled** or **Disabled** to raise an alarm when the measured value rises above its high threshold.
High Warning	Click **Enabled** or **Disabled** to raise a warning when the measured value rises above its high threshold.
Low Alarm	Click **Enabled** or **Disabled** to raise an alarm when the measured value falls below its low threshold.
Low Warning	Click **Enabled** or **Disabled** to raise a warning when the measured value falls below its low threshold.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Vendor Info** settings. Click **Refresh** to reload the vendor information.

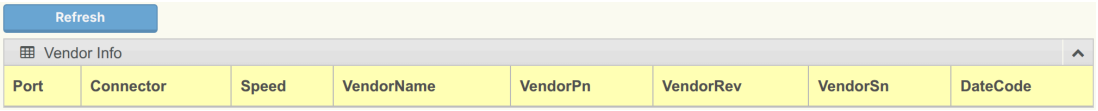


Figure 3.265 Diagnostics > Vendor Info

3.11.6 LED Indication

To access this page, click **Diagnostics > LED Indication**.

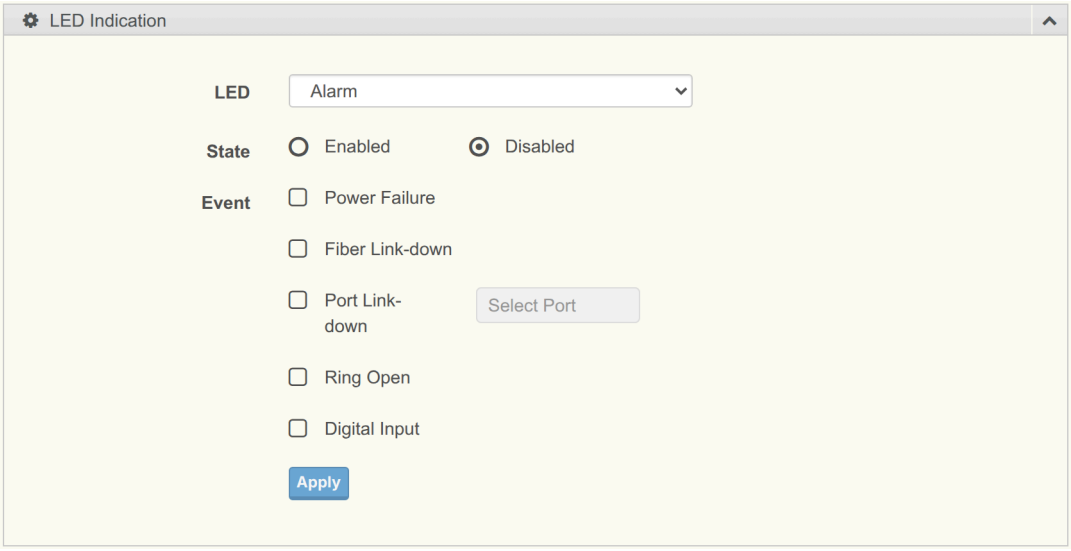


Figure 3.266 Diagnostics > LED Indication

The following table describes the items in the previous figure.

Item	Description
LED	Click the drop-down menu to select LED indicator.
State	Select **Enable** or **Disable** to enable LED alarm.
Event	Click the check box of each event that lights the designated LED: ■ Power Failure ■ Fiber Link-down ■ Port Link-down ■ Ring Open ■ Digital Input
Apply	Click **Apply** to save the values and update the screen.
Edit	Click **Edit** beside an entry in the Event Information table to modify it.
Refresh	Click **Refresh** to update the screen.

The following figure displays the **LED Information** settings.

To access this page, click **Diagnostics > LED Indication**.

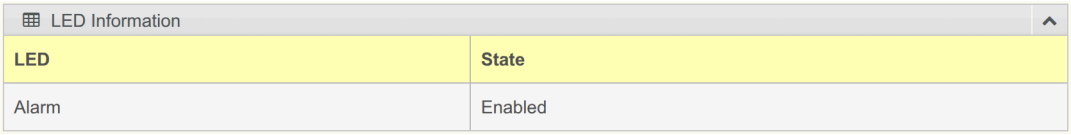


Figure 3.267 Diagnostics > LED Information

The following figure displays the **Event Information** settings.

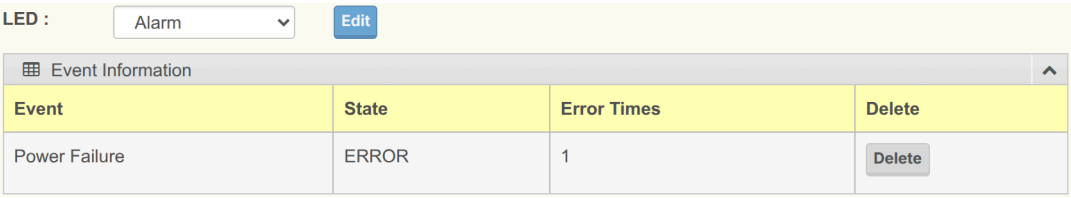


Figure 3.268 Diagnostics > Event Information

The following figure displays the **Event Detail** settings.

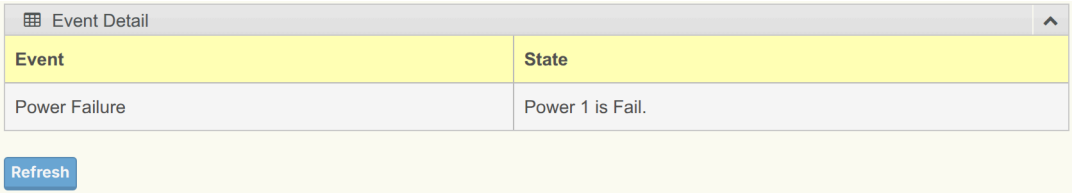


Figure 3.269 Diagnostics > Event Detail

3.11.7 Self Monitoring

The Self Monitoring menu allows the switch to watch its own resources and to react when they run short: CPU load, system health and per-port utilization.

3.11.7.1 Global Settings

The Global Settings page allows you to define how often the self monitoring functions sample the state of the switch.

To access this page, click **Diagnostics > Self Monitoring > Global Settings**.

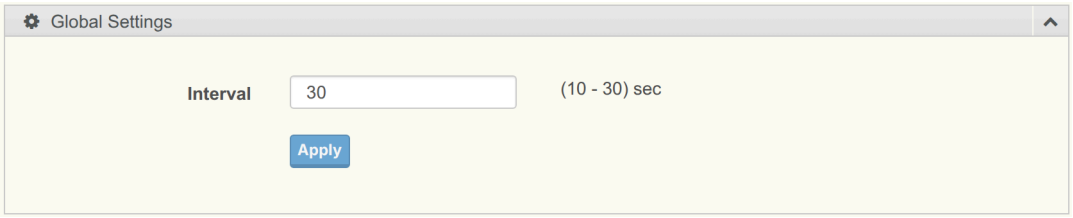


Figure 3.270 Diagnostics > Self Monitoring > Global Settings

The following table describes the items in the previous figure.

Item	Description
Interval	Enter a value to specify the interval between two samples, in seconds.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Global Information** settings.

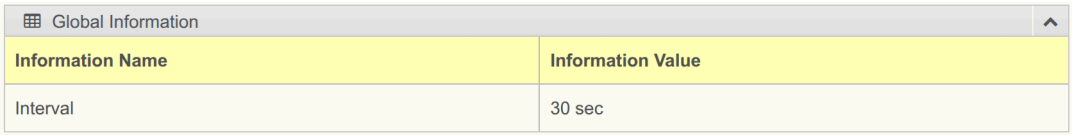


Figure 3.271 Diagnostics > Self Monitoring > Global Information

3.11.7.2 CPU Degrade Settings

The CPU Degrade Settings page allows you to enable protection of the CPU. When the function is enabled and the CPU load stays high, the switch lowers the rate at which control traffic is passed to the CPU so that management access is retained.

To access this page, click **Diagnostics > Self Monitoring > CPU Degrade Settings**.

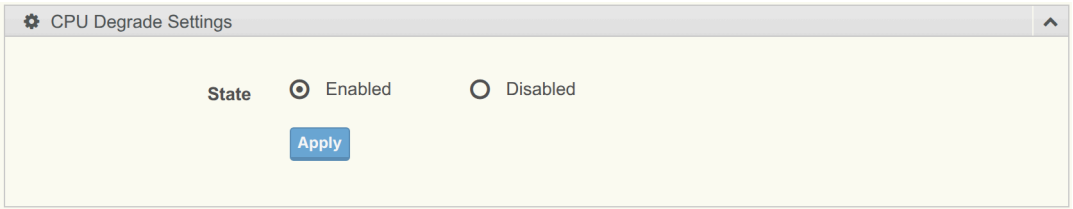


Figure 3.272 Diagnostics > Self Monitoring > CPU Degrade Settings

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the CPU degrade function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **CPU Degrade Information** settings.

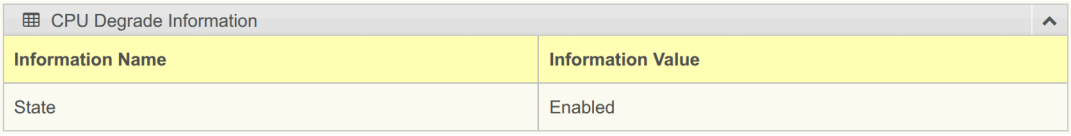


Figure 3.273 Diagnostics > Self Monitoring > CPU Degrade Information

3.11.7.3 System Settings

The System Settings page allows you to enable the monitoring of system resources, such as CPU and memory usage, and the logging of an event when a resource is exhausted.

To access this page, click **Diagnostics > Self Monitoring > System Settings**.

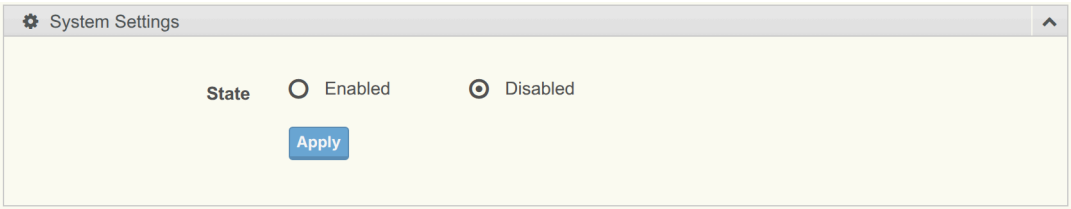


Figure 3.274 Diagnostics > Self Monitoring > System Settings

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the system monitoring function.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **System Information** settings.

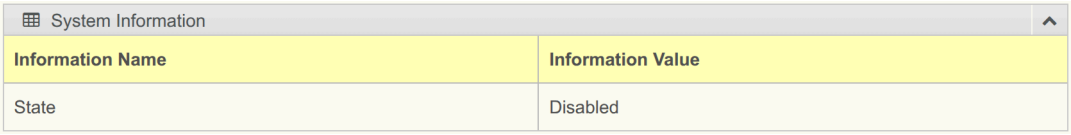


Figure 3.275 Diagnostics > Self Monitoring > System Information

3.11.7.4 Port Settings

The Port Settings page allows you to define a utilization threshold for each port. An event is logged when the utilization of the port exceeds the threshold.

To access this page, click **Diagnostics > Self Monitoring > Port Settings**.

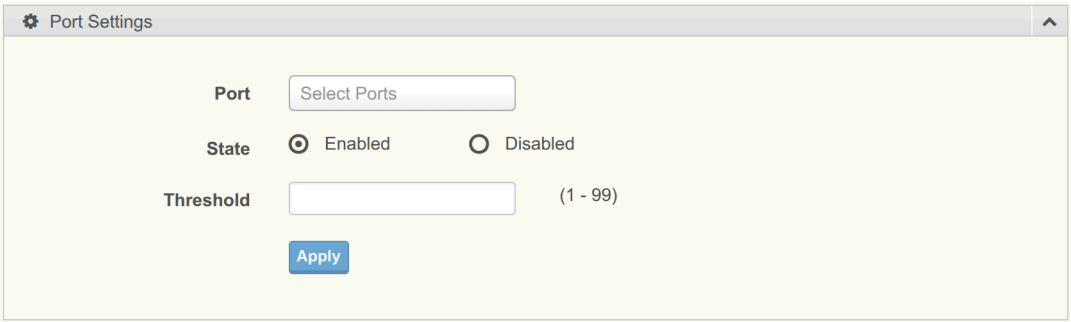


Figure 3.276 Diagnostics > Self Monitoring > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select the port to be monitored.
State	Select **Enabled** or **Disabled** to setup the monitoring of the designated port.
Threshold	Enter a value to specify the utilization at which the event is raised, as a percentage of the port bandwidth.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Port Information** settings.

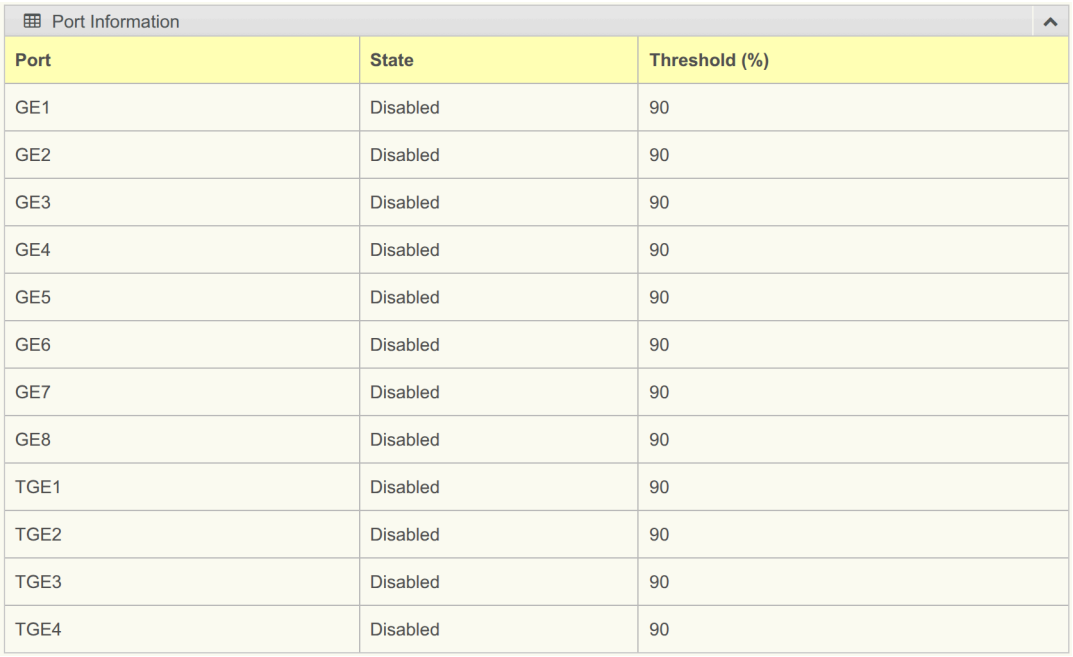


Figure 3.277 Diagnostics > Self Monitoring > Port Information

3.12 Tools

3.12.1 Backup Manager

The Backup Manager page allows you to configure a remote TFTP sever or host file system in order to backup the firmware image or configuration file.

To access this page, click **Tools > Backup Manager**.

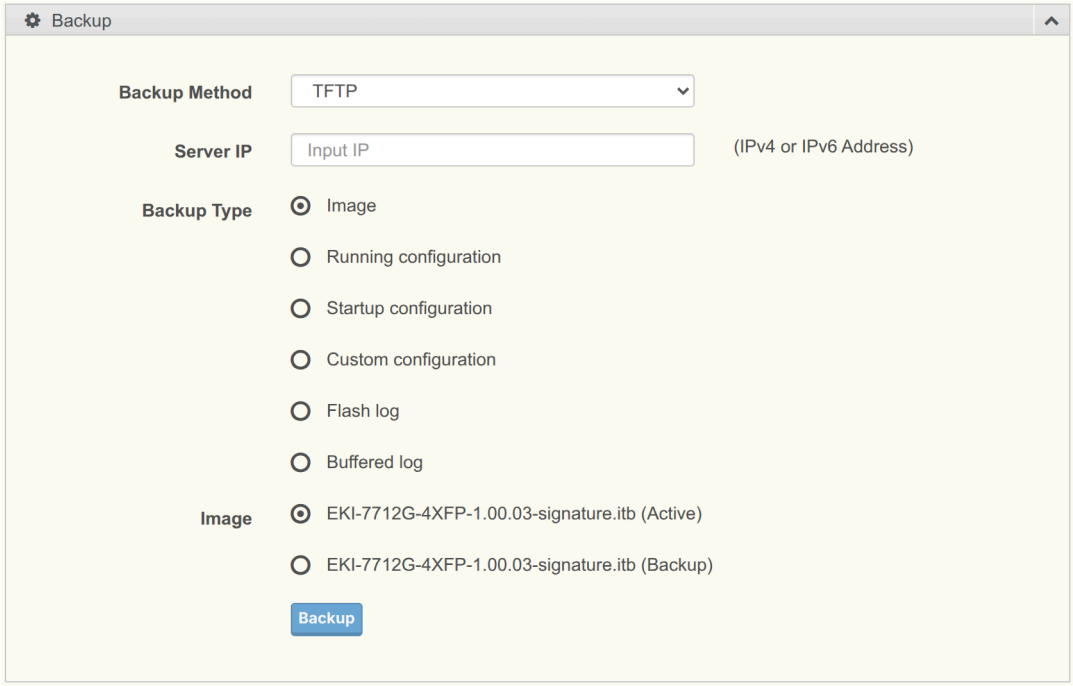


Figure 3.278 Tools > Backup Manager

The following table describes the items in the previous figure.

Item	Description
Backup Method	Click the drop-down menu to select the backup method: TFTP or HTTP.
Server IP	Enter the IP address of the backup server.
Backup Type	Click a type to define the backup method: image: running configuration, startup configuration, custom configuration, flash log, or buffered log.
Image	Click the format for the image type: Active or Backup.
Backup	Click **Backup** to backup the settings.

3.12.2 Upgrade Manager

The Upgrade Manager page allows you to configure a remote TFTP sever or host file system in order to upload firmware upgrade images or configuration files.

To access this page, click **Tools > Upgrade Manager**.

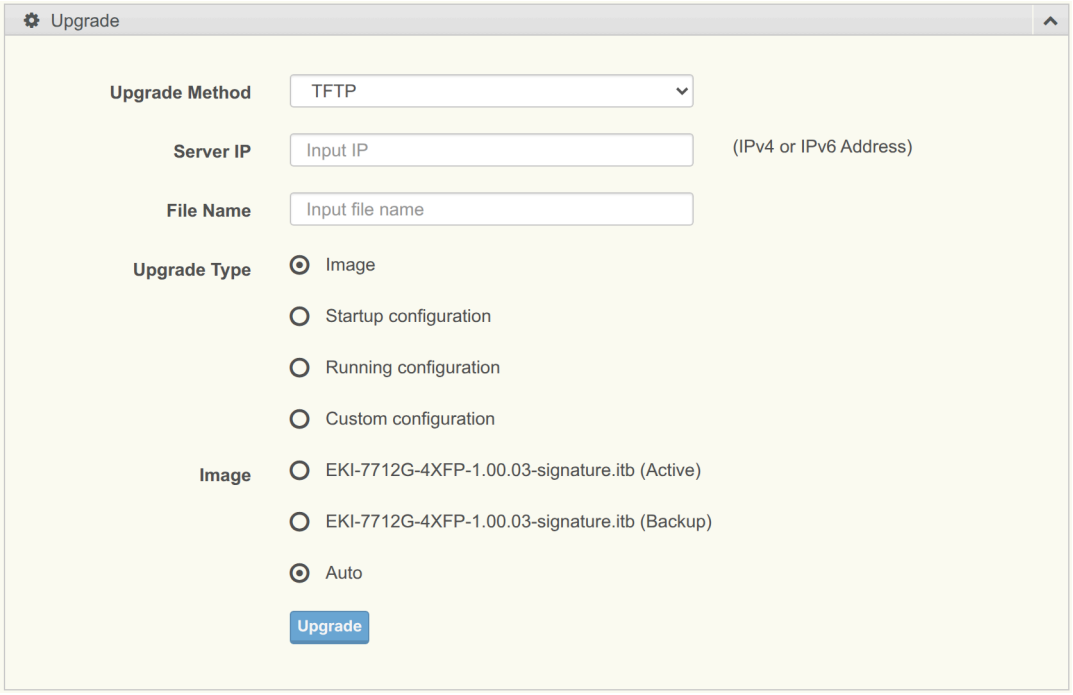


Figure 3.279 Tools > Upgrade Manager

The following table describes the items in the previous figure.

Item	Description
Upgrade Method	Click the drop-down menu to select the upgrade method: TFTP or HTTP.
Server IP	Enter the IP address of the upgrade server.
File Name	Enter the file name of the new firmware version.
Upgrade Type	Click a type to define the upgrade method: image, startup configuration, running configuration, or custom configuration.
Image	Click the format for the image type: Active, Backup, or auto.
Browse file	Click **Browse file** to select the file from the management station. The field is only available when the upgrade method is HTTP.
Upgrade	Click **Upgrade** to upgrade to the current version.

3.12.3 Dual Image

The Dual Image page allows you to setup an active and backup partitions for firmware image redundancy.

To access this page, click **Tools > Dual Image**.

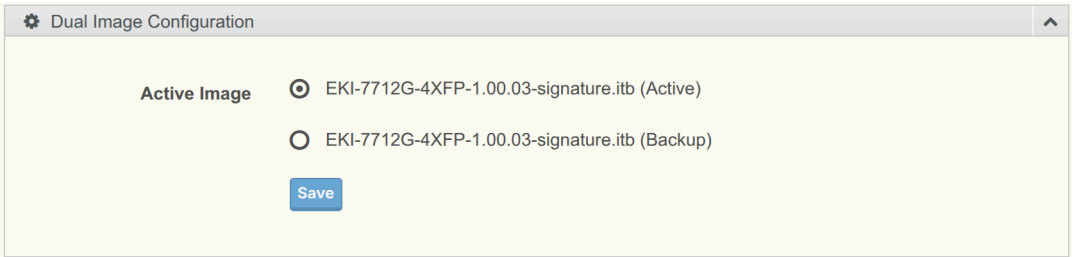


Figure 3.280 Tools > Dual Image

The following table describes the items in the previous figure.

Item	Description
Active Image	Click the format for the image type: Active or Backup.
Save	Click **Save** to save and keep the new settings.

The following figure displays the **Images Information 0** settings.

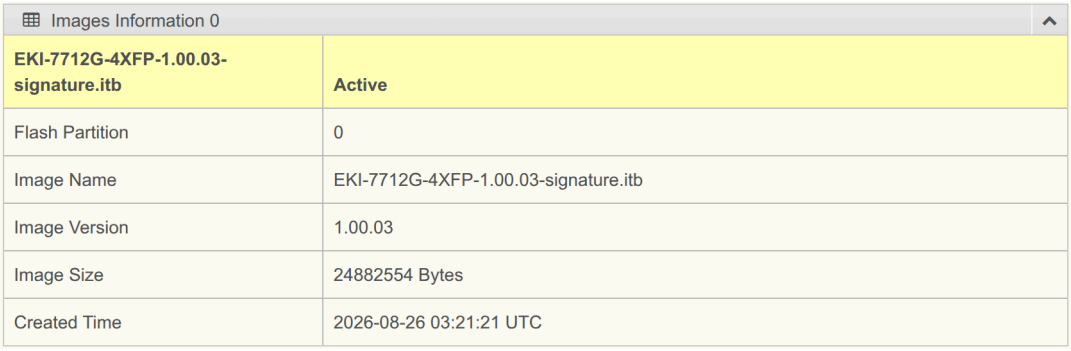


Figure 3.281 Tools > Images Information 0

The following figure displays the **Images Information 1** settings.

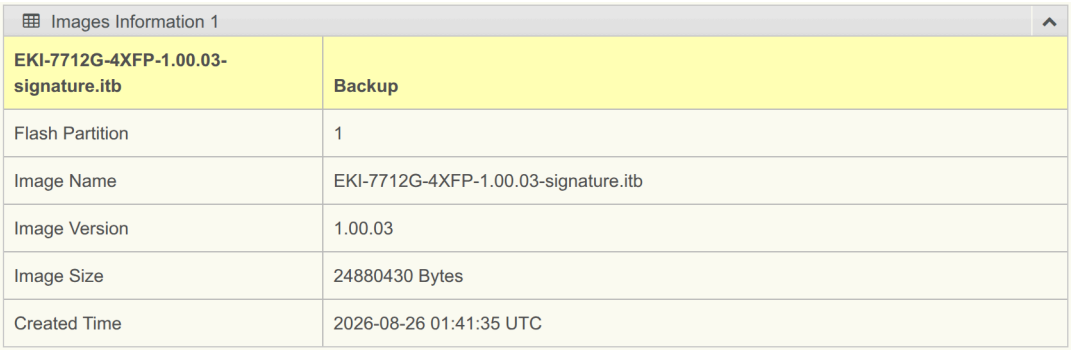


Figure 3.282 Tools > Images Information 1

3.12.4 Save Configuration

Click **Save Configuration to FLASH** 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.

To access this page, click **Tools > Save Configuration**.

3.12.5 User Account

3.12.5.1 User Account

The User Account page allows you to setup a user and the related parameters.

To access this page, click **Tools > User Account > User Account**.

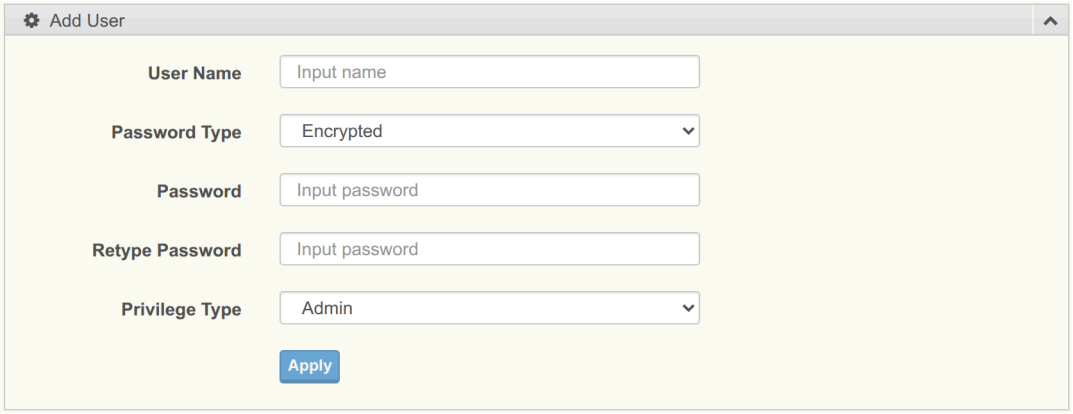


Figure 3.283 Tools > User Account > User Account

The following table describes the items in the previous figure.

Item	Description
User Name	Enter the name of the new user entry.
Password Type	Click the drop-down menu to define the type of password: **Encrypted**.
Password	Enter the character set for the define password type.
Retype Password	Retype the password entry to confirm the profile password.
Privilege Type	Click the drop-down menu to designate privilege authority for the user entry: **Admin**, **Operator** or **User**.
Apply	Click **Apply** to create a new user account.

Click **Delete** beside an entry to remove that account.

The following figure displays the **Local Users** settings.



Figure 3.284 Tools > User Account > Local Users

3.12.5.2 Password Change

The Password Change page allows you to change the password of an existing user account. The lower table lists the local users, the way their password is stored, and their privilege level.

To access this page, click **Tools > User Account > Password Change**.

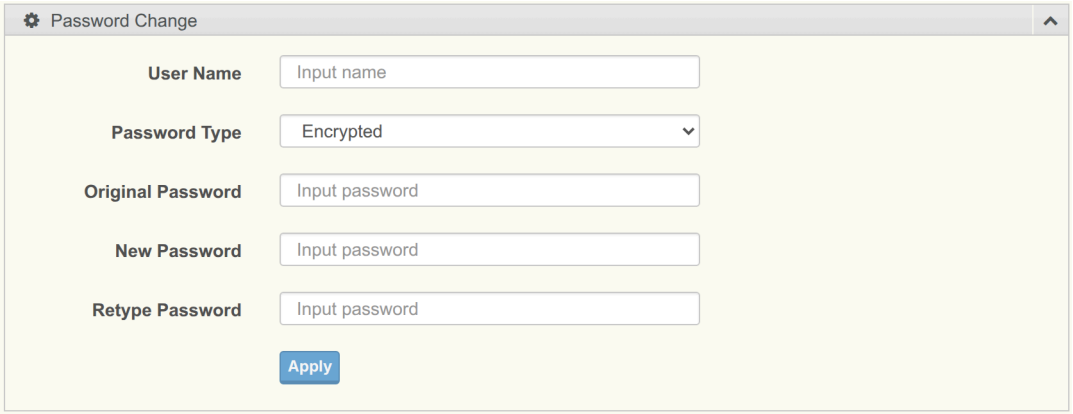


Figure 3.285 Tools > User Account > Password Change

The following table describes the items in the previous figure.

Item	Description
User Name	Click the drop-down menu to select the account whose password is changed.
Password Type	Click the drop-down menu to select how the new password is stored: ■ Encrypted: Store the password in encrypted form.
Original Password	Enter the current password of the account.
New Password	Enter the new password of the account.
Retype Password	Enter the new password again to confirm it.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Local Users** settings.



Figure 3.286 Tools > User Account > Local Users

3.12.5.3 Password Rule

The Password Rule page allows you to enforce a minimum complexity for the passwords of local accounts. A password that does not meet the rule is rejected when it is set.

To access this page, click **Tools > User Account > Password Rule**.

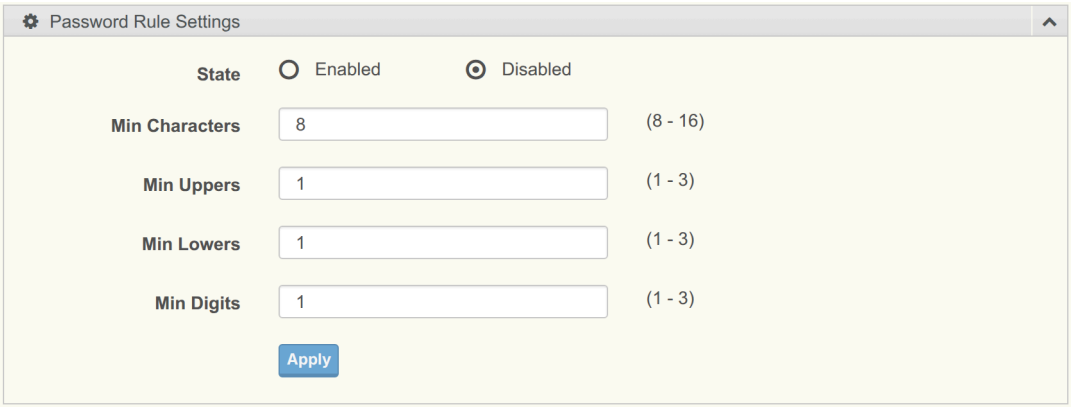


Figure 3.287 Tools > User Account > Password Rule

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the password rule function.
Min Characters	Enter a value to specify the minimum length of the password.
Min Uppers	Enter a value to specify the minimum number of upper case letters, ranging from 1 to 3.
Min Lowers	Enter a value to specify the minimum number of lower case letters, ranging from 1 to 3.
Min Digits	Enter a value to specify the minimum number of digits, ranging from 1 to 3.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **Password Rule Status** settings.

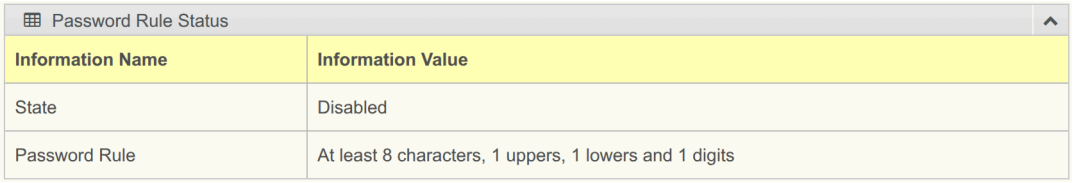


Figure 3.288 Tools > User Account > Password Rule Status

3.12.5.4 Wrong Password

The following figure displays the **Wrong Password** settings.

To access this page, click **Tools > User Account > Wrong Password**.

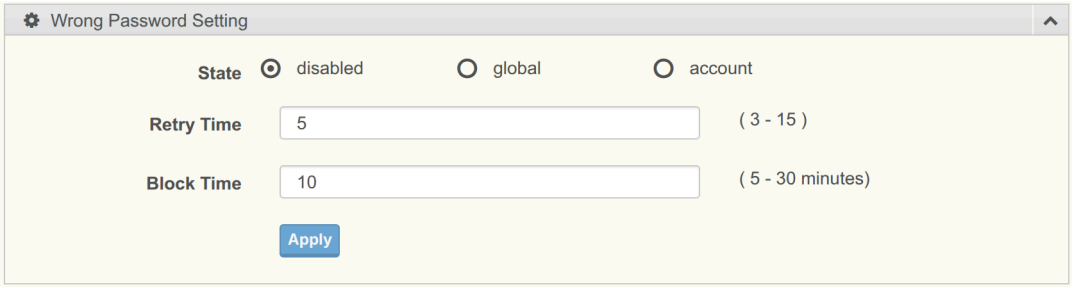


Figure 3.289 Tools > User Account > Wrong Password

To access this page, click **Tools > User Account**.

Item	Description
State	Click the radio button to select the scope of the wrong password detection: ■ disabled: Do not block after repeated failures. ■ global: Block any further login attempt on the switch. ■ account: Block only the account that failed.
Retry Time	Enter a variable to designate the wrong password entry threshold, **State** option must be enabled.
Block Time	Enter a variable to designate the lockout period in minutes after the retry attempts threshold is reached.
Apply	Click **Apply** to create a new user account.

The following figure displays the **Wrong Password Information** settings.

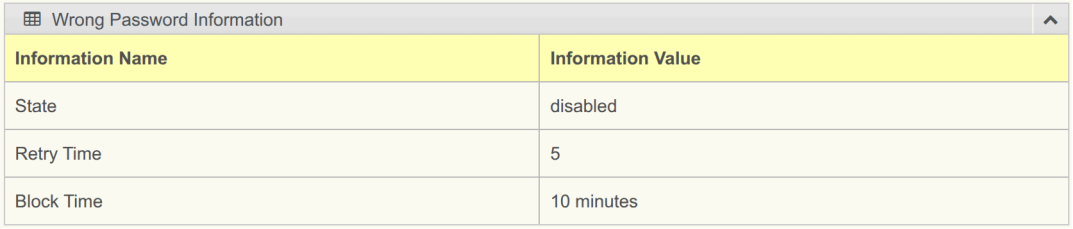


Figure 3.290 Tools > User Account > Wrong Password Information

3.12.5.5 User Name Expired

The User Name Expired page allows you to enable the checking of account expiry. When the function is enabled, an account that has passed its expiry date can no longer be used to log in.

To access this page, click **Tools > User Account > User Name Expired**.

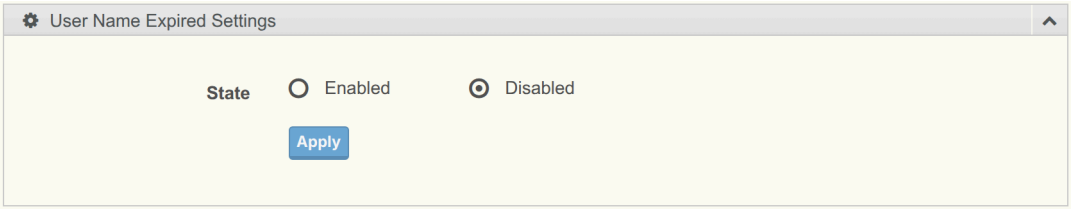


Figure 3.291 Tools > User Account > User Name Expired

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the user name expiry check.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **User Name Expired Information** settings.



Figure 3.292 Tools > User Account > User Name Expired Information

3.12.6 USB

The USB page allows you to back up the configuration of the switch to a USB storage device, and to restore it from that device. In automatic mode the switch performs the transfer on its own whenever a USB device is inserted, which allows a switch to be replaced without a management station.

The USB menu is available on the EKI-87xx series. On a model that does not support the function, this menu is not displayed.

To access this page, click **Tools > USB**.

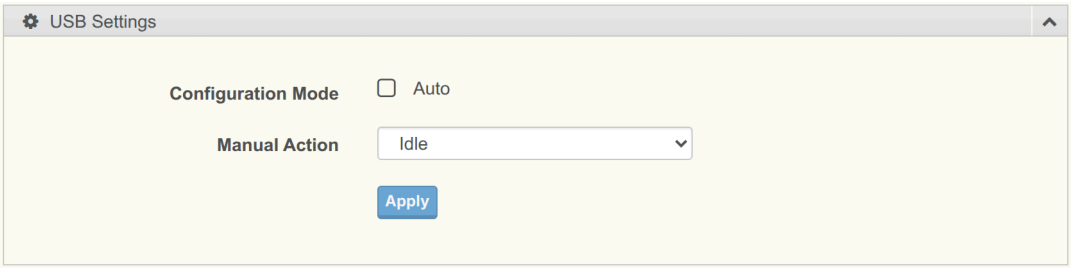


Figure 3.293 Tools > USB

The following table describes the items in the previous figure.

Item	Description
Configuration Mode	Click the check box to enable automatic backup and restore. When the check box is cleared, the transfer is performed only by the Manual Action selection.
Manual Action	Click the drop-down menu to select the transfer performed once **Apply** is clicked. The field is unavailable while automatic mode is enabled.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **USB Information** settings.



Figure 3.294 Tools > USB Information

3.12.7 N-Key

The N-Key page allows you to copy the configuration of the switch to an N-Key, and to load it back. The N-Key is a hardware key that stores the configuration outside the switch, so that a replacement unit can be brought into service without a management station.

The N-Key menu is available on the EKI-95xx series. On a model that does not support the function, this menu is not displayed.

To access this page, click **Tools > N-Key**.

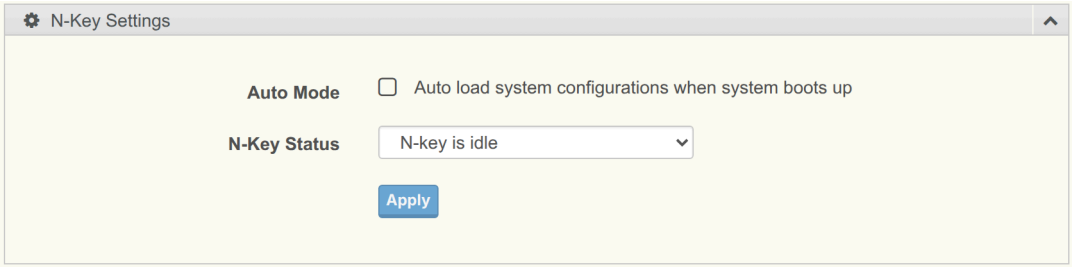


Figure 3.295 Tools > N-Key

The following table describes the items in the previous figure.

Item	Description
Auto Mode	Click the check box **Auto load system configurations when system boots up** to load the configuration stored on the N-Key each time the switch starts. While the check box is selected, the N-Key Status field is unavailable.
N-Key Status	Click the drop-down menu to select the transfer performed once **Apply** is clicked: ■ N-key is idle: Perform no transfer. ■ Backup the current configurations to N-Key: Copy the configuration of the switch to the N-Key. ■ Restore N-Key's configurations to switch: Load the configuration stored on the N-Key into the switch.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **N-Key Information** settings.

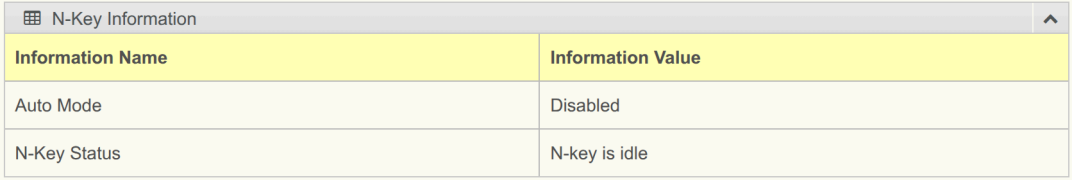


Figure 3.296 Tools > N-Key Information

3.12.8 Reset System

Click **Restore** 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.

Click **Select Excepted Configuration** to keep the configuration you selected when resetting.

Reset settings take effect after a system reboot.

To access this page, click **Tools > Reset System**.

3.12.9 Reboot Device

Click **Reboot** to reboot the switch. Any configuration changes you have made since the last time you issued a save will be lost.

To access this page, click **Tools > Reboot Device**.

3.12.10 System Use Notice

The System Use Notice page allows you to display a notice on the login screen, for example an authorized use statement required by the site security policy.

To access this page, click **Tools > System Use Notice**.

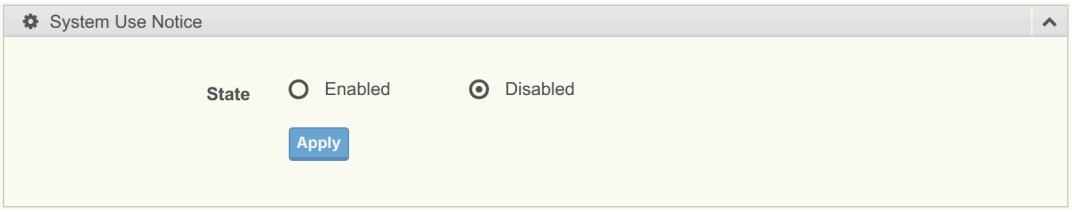


Figure 3.297 Tools > System Use Notice

The following table describes the items in the previous figure.

Item	Description
State	Select **Enabled** or **Disabled** to setup the display of the notice.
Apply	Click **Apply** to save the values and update the screen.

The following figure displays the **System Use Notice** settings.

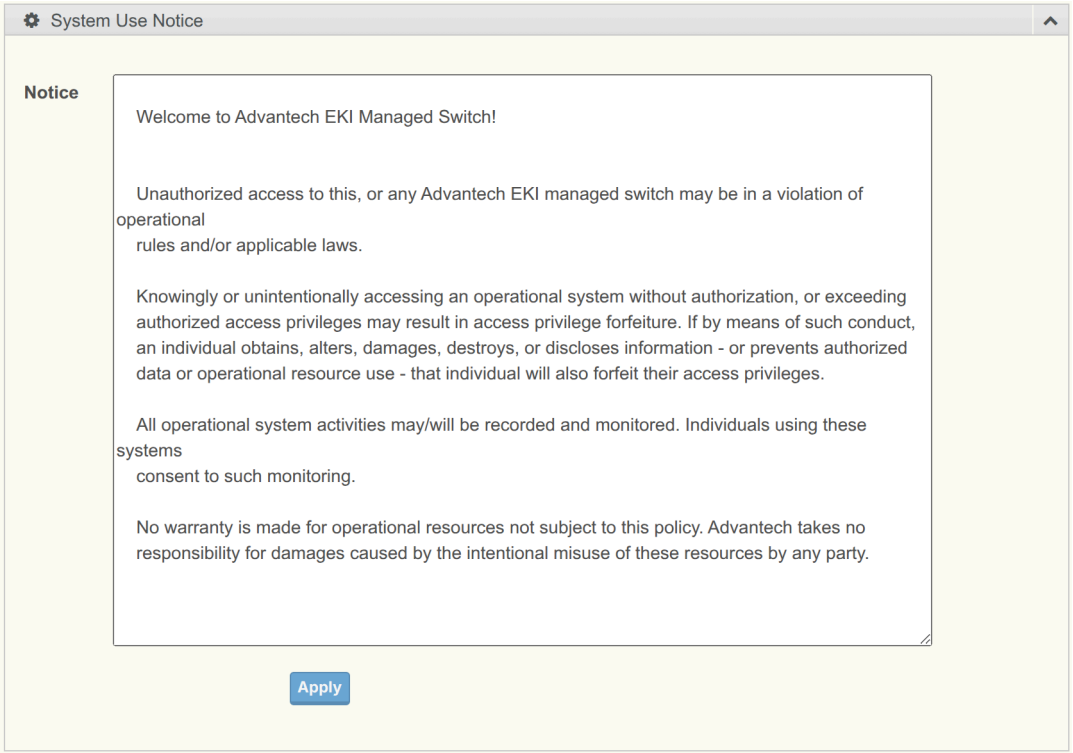


Figure 3.298 Tools > System Use Notice

The following table describes the items in the previous figure.

Item	Description
Notice	Enter the text displayed on the login screen.
Apply	Click **Apply** to save the values and update the screen.

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com
Please verify specifications before quoting. This guide is intended for reference purposes only.
All product specifications are subject to change without notice.
No part of this publication may be reproduced in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission of the publisher.
All brand and product names are trademarks or registered trademarks of their respective companies.
© Advantech Co., Ltd. 2026