LinkPower™ LPS3000 Series
IP Management User's Manual

May, 2022

Corporate Headquarters

Inscape Data Corporation

2012 Hartog Drive

San Jose, CA 95131

U.S.A.

Website: http://www.inscapedata.com

Main: 408 392-9800

Fax: 408 392-9812

Certification

Inscape Data Corporation certifies that this product met its published specifications at time of shipment from the factory.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B 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.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate the equipment.

Industry Canada Statement

This Class A digital apparatus complies with Canadian ICES-003.

CE Statement

This product complies with the European Low Voltage Directive 73/23/EEC and EMC Directive 89/336/EEC as amended by European Directive 93/68/EEC.

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

Limited Warranty and Disclaimer of Warranty

Hardware. Inscape Data Corporation, or subsidiary selling the Product ("Inscape Data") warrants that commencing from the date of shipment to Customer (and in case of resale by a Inscape Data's reseller, commencing not more than ninety (90) days after original shipment by Inscape Data), and continuing for a period of the longer of (a) ninety (90) days or (b) the period set forth in the warranty card accompanying the Product (if any), the Hardware will be free from defects in material and workmanship under normal use. The date of shipment of a Product by Inscape Data is set forth on the packaging material in which the Product is shipped. This limited warranty extends only to the original user of the Product. Customer's sole and exclusive remedy and the entire liability of Inscape Data and its suppliers under this limited warranty will be, at Inscape Data's or its service center's option, shipment of a replacement within the warranty period and according to the replacement process described in the warranty card (if any), or if no warranty card, as described on the Inscape Data Product Warranty Policy or a refund of the purchase price if the Hardware is returned to the party supplying it to Customer, freight and insurance prepaid. Inscape Data replacement parts used in Hardware replacement may be new or equivalent to new. Inscape Data's obligations hereunder are conditioned upon the return of affected Hardware in accordance with Inscape Data's or its service center's then-current Return Material Authorization (RMA) procedures.

Software. The limited warranty in the United States Federal Communications Commission Notice sets forth Inscape Data's warranty obligations with respect to the Software.

Restrictions. The above Hardware warranty and limited warranty in the End User License Agreement ("Software warranty") do not apply if the Software, Hardware Product or any other equipment upon which the Software is authorized by Inscape Data or its suppliers or licensors to be used (a) has been altered, except by Inscape Data or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Inscape Data, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does not apply to (e) any temporary Software modules; (f) any Software not posted on Inscape Data's Software Center (on InscapeData.com URL where Inscape Data makes the Software publicly available to customers); (g) any Software that Inscape Data expressly provides on an "AS IS" basis on Inscape Data's Software Center; or (h) any Software for which Inscape Data does not receive a license fee.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY INSCAPE DATA, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THESE WARRANTIES GIVE CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER

RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. THIS DISCLAIMER AND EXCLUSION SHALL APPLY EVEN IF THE EXPRESS WARRANTY SET FORTH ABOVE FAILS OF ITS ESSENTIAL PURPOSE.

INSCAPE DATA CORPORATION

3-Year Limited Hardware Warranty Terms

The followings are special terms applicable to your hardware warranty. Your formal Warranty Statement, including the warranty applicable to Inscape Data software, appears in the End User License Agreement that accompanies your Inscape Data product.

Duration of Hardware Warranty: Three (3) Year

Replacement, Repair or Refund Procedure for Hardware: Inscape Data or its authorized service center will use commercially reasonable efforts to ship a replacement part after receipt of the RMA request and the RMA item. Actual delivery times may vary depending on Customer location. Inscape Data reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number: Please go to Inscape Data's website and complete the RMA request, http://www.inscapedata.com/rma.htm.

Inscape Data Corporation
1620 Oakland Road, STE D101, CA 95131 USA

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY.

DOWNLOADING, INSTALLING OR USING INSCAPE DATA OR INSCAPE DATA-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

INSCAPE DATA CORPORATION OR ITS SUBSIDIARY LICENSING THE SOFTWARE INSTEAD OF INSCAPE DATA CORPORATION ("INSCAPE DATA") IS WILLING TO LICENSE ITS SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT PLUS ANY ADDITIONAL LIMITATIONS ON THE LICENSE SET FORTH IN A SUPPLEMENTAL LICENSE AGREEMENT ACCOMPANYING THE PRODUCT (COLLECTIVELY THE "AGREEMENT"). TO THE EXTENT OF ANY CONFLICT BETWEEN THE TERMS OF THIS END USER LICENSE AGREEMENT AND ANY SUPPLEMENTAL LICENSE AGREEMENT, THE SUPPLEMENTAL LICENSE AGREEMENT SHALL APPLY. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THE AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN INSCAPE DATA IS UNWILLING TO LICENSE THE SOFTWARE TO YOU AND (A) YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE, AND (B) YOU MAY RETURN THE SOFTWARE (INCLUDING ANY UNOPENED CD PACKAGE AND ANY WRITTEN MATERIALS) FOR A FULL REFUND, OR, IF THE SOFTWARE AND WRITTEN MATERIALS ARE SUPPLIED AS PART OF ANOTHER PRODUCT, YOU MAY RETURN THE ENTIRE PRODUCT FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM INSCAPE DATA OR AN AUTHORIZED INSCAPE DATA RESELLER, AND APPLIES ONLY IF YOU ARE THE ORIGINAL END USER PURCHASER.

THE FOLLOWING TERMS OF THE AGREEMENT GOVERN CUSTOMER'S ACCESS AND USE OF EACH INSCAPE DATA OR INSCAPE DATA-SUPPLIED SOFTWARE ("SOFTWARE"), EXCEPT TO THE EXTENT: (A) THERE IS A SEPARATE SIGNED CONTRACT BETWEEN CUSTOMER AND INSCAPE DATA GOVERNING CUSTOMER'S USE OF THE SOFTWARE, OR (B) THE SOFTWARE INCLUDES A SEPARATE "CLICK-ACCEPT" LICENSE AGREEMENT OR THIRD PARTY LICENSE AGREEMENT AS PART OF THE INSTALLATION AND/OR DOWNLOAD PROCESS GOVERNING CUSTOMER'S USE OF THE SOFTWARE. TO THE EXTENT OF A CONFLICT BETWEEN THE PROVISIONS OF THE FOREGOING DOCUMENTS, THE ORDER OF PRECEDENCE SHALL BE (1)THE SIGNED CONTRACT, (2) THE CLICK-ACCEPT AGREEMENT OR THIRD PARTY LICENSE AGREEMENT, AND (3) THE AGREEMENT.

License. Conditioned upon compliance with the terms and conditions of the Agreement, Inscape Data grants to Customer a nonexclusive and nontransferable license to use for Customer's internal business purposes the Software

and the Documentation for which Customer has paid the required license fees. "Documentation" means written information (whether contained in user or technical manuals, training materials, specifications or otherwise) pertaining to the Software and made available by Inscape Data with the Software in any manner (including on CD-ROM, or on-line). In order to use the Software, Customer may be required to input a registration number or product authorization key and register Customer's copy of the Software online at Inscape Data's website to obtain the necessary license key or license file.

End User License Agreement

Customer's license to use the Software shall be limited to, and Customer shall not use the Software in excess of, a single hardware chassis or card or such other limitations as are set forth in the applicable Supplemental License Agreement or in the applicable purchase order which has been accepted by Inscape Data and for which Customer has paid to Inscape Data the required license fee (the "Purchase Order"). Unless otherwise expressly provided in the Documentation or any applicable Supplemental License Agreement, Customer shall use the Software solely as embedded in, for execution on, or (where the applicable Documentation permits installation on non-Inscape Data equipment) for communication with Inscape Data equipment owned or leased by Customer and used for Customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

For evaluation or beta copies for which Inscape Data does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations. This is a license, not a transfer of title, to the Software and Documentation, and Inscape Data retains ownership of all copies of the Software and Documentation. Customer acknowledges that the Software and Documentation contain trade secrets of Inscape Data or its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under the Agreement, Customer shall have no right, and Customer specifically agrees not to:

(i) transfer, assign or sublicense its license rights to any other person or entity (other than in compliance with any Inscape Data relicensing/transfer policy then in force), or use the Software on unauthorized or secondhand Inscape Data equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

(ii) make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

(iii) reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;

(iv) publish any results of benchmark tests run on the Software;

(v) use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of Inscape Data; or

(vi) disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of Inscape Data. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by applicable law, and at Customer's written request, Inscape Data shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently

created program, on payment of Inscape Data's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Inscape Data makes such information available.

Software, Upgrades and Additional Copies. For purposes of the Agreement, "Software" shall include (and the terms and conditions of the Agreement shall apply to) computer programs, including firmware, as provided to Customer by Inscape Data or an authorized Inscape Data reseller, and any upgrades, updates, bug fixes or modified versions thereto (collectively, "Upgrades") or backup copies of any of the foregoing. NOTWITHSTANDING ANY OTHER PROVISION OF THE AGREEMENT: (1) CUSTOMER HAS NO LICENSE OR RIGHT TO MAKE OR USE ANY ADDITIONAL COPIES OR UPGRADES UNLESS CUSTOMER, AT THE TIME OF MAKING OR ACQUIRING SUCH COPY OR UPGRADE, ALREADY HOLDS A VALID LICENSE TO THE ORIGINAL SOFTWARE AND HAS PAID THE APPLICABLE FEE FOR THE UPGRADE OR ADDITIONAL COPIES; (2) USE OF UPGRADES IS LIMITED TO INSCAPE DATA EQUIPMENT FOR WHICH CUSTOMER IS THE ORIGINAL END USER PURCHASER OR LESSEE OR OTHERWISE HOLDS A VALID LICENSE TO USE THE SOFTWARE WHICH IS BEING UPGRADED; AND (3) THE MAKING AND USE OF ADDITIONAL COPIES IS LIMITED TO NECESSARY BACKUP PURPOSES ONLY.

Proprietary Notices. Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in the Agreement, Customer shall not make any copies or duplicates of any Software without the prior written permission of Inscape Data.

Term and Termination. The Agreement and the license granted herein shall remain effective until terminated. Customer may terminate the Agreement and the license at any time by destroying all copies of Software and any Documentation. Customer's rights under the Agreement will terminate immediately without notice from Inscape Data if Customer fails to comply with any provision of the Agreement. Upon termination, Customer shall destroy all copies of Software and Documentation in its possession or control. All confidentiality obligations of Customer and all limitations of liability and disclaimers and restrictions of warranty shall survive termination of this Agreement. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" and "General Terms Applicable to the Limited Warranty Statement and End User License Agreement" shall survive termination of the Agreement.

Customer Records. Customer grants to Inscape Data and its independent accountants the right to examine Customer's books, records and accounts during Customer's normal business hours to verify compliance with this Agreement. In the event such audit discloses non-compliance with this Agreement, Customer shall promptly pay to Inscape Data the appropriate license fees, plus the reasonable cost of conducting the audit.

Export, Re-Export, Transfer and Use Controls. The Software, Documentation and technology or direct products thereof (hereafter referred to as Software and Technology), supplied by Inscape Data under the Agreement are subject to export controls under the laws and regulations of the United States (U.S.) and any other applicable countries' laws and regulations. Customer shall comply with such laws and regulations governing export, re-export, transfer and use of Inscape Data Software and Technology and will obtain all required U.S. and local authorizations, permits, or licenses.

Inscape Data and Customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses.

End User License Agreement

U.S. Government End User Purchasers. The Software and Documentation qualify as "commercial items," as that term is defined at Federal Acquisition Regulation ("FAR") (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in FAR 12.212. Consistent with FAR 12.212 and DoD FAR Supp. 227.7202-1 through 227.7202-4, and notwithstanding any other FAR or other contractual clause to the contrary in any agreement into which the Agreement may be incorporated, Customer may provide to Government end user or, if the Agreement is direct, Government end user will acquire, the Software and Documentation with only those rights set forth in the Agreement. Use of either the Software or Documentation or both constitutes agreement by the Government that the Software and Documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Limited Warranty

Subject to the limitations and conditions set forth herein, Inscape Data warrants that commencing from the date of shipment to Customer (but in case of resale by an authorized Inscape Data reseller, commencing not more than ninety (90) days after original shipment by Inscape Data), and continuing for a period of the longer of (a) ninety (90) days or (b) the warranty period (if any) expressly set forth as applicable specifically to software in the warranty card accompanying the product of which the Software is a part (the "Product") (if any): (a) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (b) the Software substantially conforms to the Documentation. The date of shipment of a Product by Inscape Data is set forth on the packaging material in which the Product is shipped. Except for the foregoing, the Software is provided "AS IS". This limited warranty extends only to the Customer who is the original licensee. Customer's sole and exclusive remedy and the entire liability of Inscape Data and its suppliers under this limited warranty will be (i) replacement of defective media and/or (ii) at Inscape Data's option, repair, replacement, or refund of the purchase price of the Software, in both cases subject to the condition that any error or defect constituting a breach of this limited warranty is reported to Inscape Data or the party supplying the Software to Customer, if different than Inscape Data, within the warranty period. Inscape Data or the party supplying the Software to Customer may, at its option, require return of the Software and/or Documentation as a condition to the remedy. In no event does Inscape Data warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions. In addition, due to the continual development of new techniques for intruding upon and attacking networks, Inscape Data does not warrant that the Software or any equipment, system or network on which the Software is used will be free of vulnerability to intrusion or attack.

Restrictions. This warranty does not apply if the Software, Product or any other equipment upon which the Software is authorized to be used (a) has been altered, except by Inscape Data or its authorized representative, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Inscape Data, (c) has been subjected to abnormal physical or electrical stress, abnormal environmental conditions, misuse, negligence, or accident; or (d) is licensed for beta, evaluation, testing or demonstration purposes. The Software warranty also does

not apply to (e) any temporary Software modules; or (f) any Software for which Inscape Data does not receive a license fee.

DISCLAIMER OF WARRANTY

EXCEPT AS SPECIFIED IN THIS WARRANTY SECTION, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY, NON-INTERFERENCE, ACCURACY OF INFORMATIONAL CONTENT, OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW AND ARE EXPRESSLY DISCLAIMED BY INSCAPE DATA, ITS SUPPLIERS AND LICENSORS. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE EXPRESS WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY. THIS WARRANTY GIVES CUSTOMER SPECIFIC LEGAL RIGHTS, AND CUSTOMER MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

General Terms Applicable to the Limited Warranty Statement, End User License Agreement, and Supplemental License Agreement

Disclaimer of Liabilities - Limitation of Liability. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, CANADA, JAPAN OR THE CARIBBEAN, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO INSCAPE DATA FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, NOTWITHSTANDING ANYTHING ELSE IN THE AGREEMENT TO THE CONTRARY, ALL LIABILITY OF INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS COLLECTIVELY, TO CUSTOMER, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), BREACH OF WARRANTY OR OTHERWISE, SHALL NOT EXCEED THE PRICE PAID BY CUSTOMER TO INSCAPE DATA FOR THE SOFTWARE THAT GAVE RISE TO THE CLAIM OR IF THE SOFTWARE IS PART OF ANOTHER PRODUCT, THE PRICE PAID FOR SUCH OTHER PRODUCT. THIS LIMITATION OF LIABILITY FOR SOFTWARE IS CUMULATIVE AND NOT PER INCIDENT (I.E. THE EXISTENCE OF TWO OR MORE CLAIMS WILL NOT ENLARGE THIS LIMIT). NOTHING IN THE AGREEMENT SHALL LIMIT (I) THE LIABILITY OF INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS TO CUSTOMER FOR PERSONAL INJURY OR DEATH CAUSED BY THEIR NEGLIGENCE, (II) INSCAPE DATA'S LIABILITY FOR FRAUDULENT MISREPRESENTATION, OR (III) ANY LIABILITY OF INSCAPE DATA WHICH CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

End User License Agreement

Disclaimer of Liabilities - Waiver of Consequential Damages and Other Losses. IF YOU ACQUIRED THE SOFTWARE IN THE UNITED STATES, LATIN AMERICA, THE CARIBBEAN OR CANADA, REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL INSCAPE DATA OR ITS SUPPLIERS

BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF INSCAPE DATA OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

IF YOU ACQUIRED THE SOFTWARE IN JAPAN, EXCEPT FOR LIABILITY ARISING OUT OF OR IN CONNECTION WITH DEATH OR PERSONAL INJURY, FRAUDULENT MISREPRESENTATION, AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE OR OTHERWISE, IN NO EVENT WILL INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE OR OTHERWISE AND EVEN IF INSCAPE DATA OR ITS SUPPLIERS OR LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IF YOU ACQUIRED THE SOFTWARE IN EUROPE, THE MIDDLE EAST, AFRICA, ASIA OR OCEANIA, IN NO EVENT WILL INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, BE LIABLE FOR ANY LOST REVENUE, LOST PROFIT, OR LOST OR DAMAGED DATA, BUSINESS INTERRUPTION, LOSS OF CAPITAL, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES, HOWSOEVER ARISING, INCLUDING, WITHOUT LIMITATION, IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR WHETHER ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF, IN EACH CASE, INSCAPE DATA, ITS AFFILIATES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS AND LICENSORS, HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT FULLY APPLY TO YOU. THE FOREGOING WAIVER SHALL NOT APPLY TO ANY LIABILITY ARISING OUT OF OR IN CONNECTION WITH: (I) DEATH OR PERSONAL INJURY, (II) FRAUDULENT MISREPRESENTATION, OR (III) INSCAPE DATA'S LIABILITY IN CONNECTION WITH ANY TERMS THAT CANNOT BE EXCLUDED UNDER APPLICABLE LAW.

For all countries referred to above, Customer agrees that the limitations of liability and disclaimers set forth herein will apply regardless of whether Customer has accepted the Software or any other product or service delivered by Inscape Data. Customer acknowledges and agrees that Inscape Data has set its prices and entered into the Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the parties.

Controlling Law, Jurisdiction. If you acquired the Software in the United States, Latin America, or the Caribbean, the Agreement and Hardware and Software warranties ("Warranties") are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Canada, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the Province of Ontario, Canada, notwithstanding any conflicts of law

provisions; and the courts of the Province of Ontario shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Europe, the Middle East, Africa, Asia or Oceania (excluding Australia), unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of England, notwithstanding any conflicts of law provisions; and the English courts shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. In addition, if the Agreement is controlled by the laws of England, no person who is not a party to the Agreement shall be entitled to enforce or take the benefit of any of its terms under the Contracts (Rights of Third Parties) Act 1999. If you acquired the Software in Japan, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of Japan, notwithstanding any conflicts of law provisions; and the Tokyo District Court of Japan shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in Australia, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of New South Wales, Australia, notwithstanding any conflicts of law provisions; and the State and federal courts of New South Wales shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties. If you acquired the Software in any other country, unless expressly prohibited by local law, the Agreement and Warranties are controlled by and construed under the laws of the State of California, United States of America, notwithstanding any conflicts of law provisions; and the state and federal courts of California shall have exclusive jurisdiction over any claim arising under the Agreement or Warranties.

For all countries referred to above, the parties specifically disclaim the application of the UN Convention on Contracts for the International Sale of Goods. Notwithstanding the foregoing, either party may seek interim injunctive relief in any court of appropriate jurisdiction with respect to any alleged breach of such party's intellectual property or proprietary rights. If any portion hereof is found to be void or unenforceable, the remaining provisions of the Agreement and Warranties shall remain in full force and effect. Except as expressly provided herein, the Agreement constitutes the entire agreement between the parties with respect to the license of the Software and Documentation and supersedes any conflicting or additional terms contained in any Purchase Order or elsewhere, all of which terms are excluded. The Agreement has been written in the English language, and the parties agree that the English version will govern.

Safety Summary

The following general safety precautions must be observed during all phases of operation of this instrument. Failure to comply with these precautions or with specific warnings elsewhere in this manual violates safety standards of design, manufacture, and intended use of the instrument. Inscape Data Corporation assumes no liability for the customer's failure to

comply with these requirements.

Before Applying Power

Verify that the product is set to match the available line voltage and all safety precautions are taken.

Over Temperature Warning

To prevent the switch from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of (70°C). To prevent product cooling restriction, allow at least 3 inches (7.6 cm) of clearance around the product after installation.

Ground the Instrument

To minimize shock hazard, the instrument chassis and cabinet must be connected to an electrical ground. The instrument must be connected to the ac power supply mains through a three-conductor power cable, with the third wire firmly connected to an electrical ground (safety ground) at the power outlet. For instruments designed to be hard-wired to the ac power lines (supply mains), connect the protective earth terminal to a protective conductor before any other connection is made. Any interruption of the protective (grounding) conductor or disconnection of the protective earth terminal will cause a potential shock hazard that could result in personal injury.

When installing the unit, always make the ground connection first and disconnect it last.

Jewelry Removal Warning

Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Do not Operate in Explosive Atmosphere

Do not operate the product in the presence of flammable gases or fumes.

Chassis Power Connection

Before connecting or disconnecting ground or power wires to the chassis, ensure that power is removed from the device. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the device, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

Work During Lightning Activity

Do not work on the system or connect or disconnect cables during periods of lightning activity.

Comply with Local and National Electrical Codes

Installation of the equipment must comply with local and national electrical codes

Do Not Exceed Input and Output Ratings

Do not operate the product to exceed the power input and output ratings.

TABLE OF CONTENTS

1. Introduction

1.1 Overview

Thank you for purchasing Inscape Data's Managed PoE Switch. You can conveniently manage, monitor, configure all software functions via embedded Web-based (HTML) interface without using the console port. By using a standard browser, you can manage switch at any remote site in the network. ***Please note, all managed PoE switches, i.e., LPS3400, 3802, and 3800 use the same common web interface, so all managed PoE switches share the this User's Manual.***

1.2 Web Management Login

Open a web browser, e.g., Google Chrome, Microsoft Edge, or Firefox on your PC, enter the switch's IP address, such as http://xxx.xxx.xxx.xxx, then open the URL to access the web management software.

Note: Default IP address of switch is 192.168.2.1. So please enter http://192.168.2.1 in the browser.

When the login window appears, please enter the default username "admin" with password "system". Then click OK to login.

Figure1-1 Login Window

Default User Name: admin
Default Password: system

1.3 Web-based User Interface

After entering the username and password, the main screen appears as the following Figure1-2.

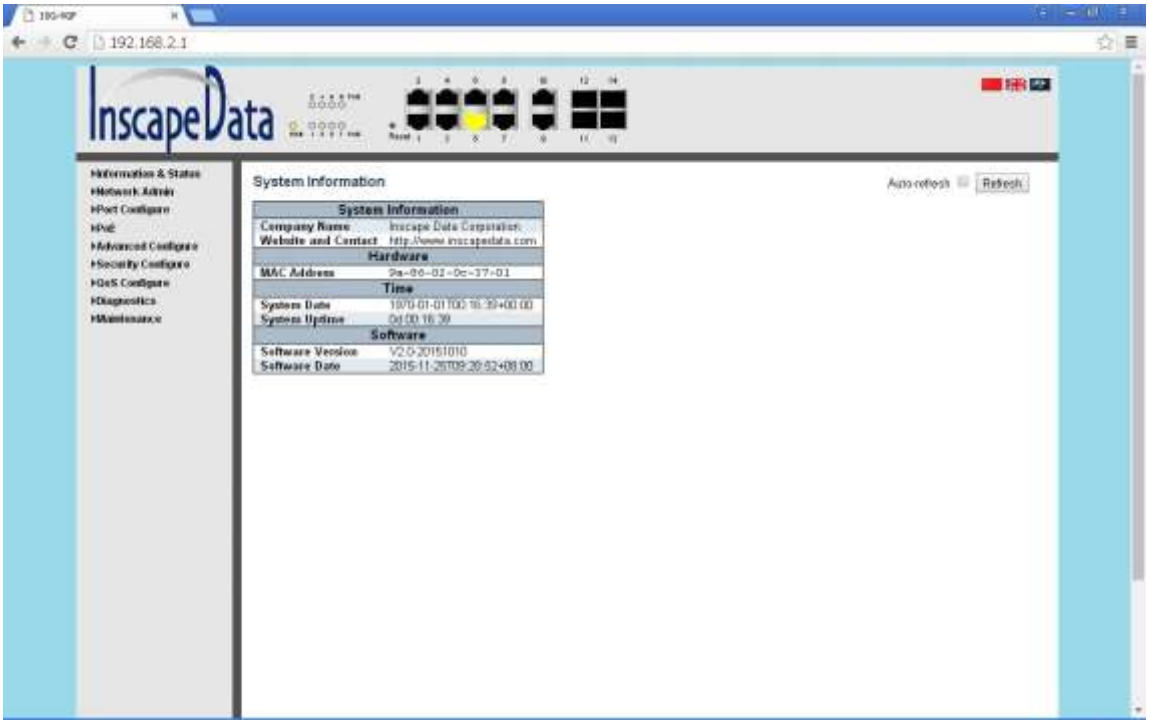


Figure1-2 Web management Main Page interface

This Main Page interface includes 3 parts as the following:

Part	Description
Part 1	Company LOGO; Panel display; Port indicators, including PoE and Link working status; Language selection button; Help document
Part 2	The Main Menu, lets you access all the commands and statistics
Part 3	Main Screen, showing configuration details

The Web agent displays an image of the Managed Switch's ports. Different colors mean different states, they are illustrated as follows:

: 100Mbps linked ; : 1000Mbps linked ; : No link

1.4 Main Menu

Using the onboard Web agent, you can define system parameters, manage and control the Managed Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the Managed Switch by selecting the functions those listed in the Main Menu. The following is short description:

Information & Status - Users can check switch information and working status under this menu.

Network Admin - Users can check and configure related features of network under this menu.

Port Configure - Users can check and configure specification of ports under this menu.

PoE - Users can check and configure related features of Power-over-Ethernet (PoE) under this menu.

Advanced Configure - Users can check and configure L2 advanced features under this menu.

Security Configure - Users can check and configure security features of the switch under this

2. Network Management

2.1 IP Configuration

Note: Default IP address of switch is 192.168.2.1, and the default subnet mask is 255.255.255.0 (24)

Click "Network Admin" > "IP", screen will show as:

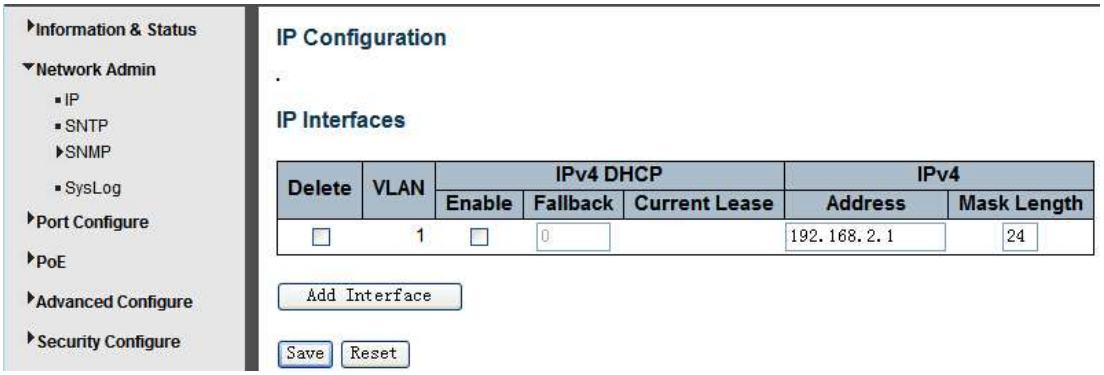


Figure 2-1 IP Configuration Screen

The following shows description details about IP configuration:

Name	Description
Port Name	Display system's port name
VLAN	VLAN for for access and management of switch
IPv4 DHCP	- If enable, it means that VLAN port start IPv4 DHCP client, to dynamically get IPv4 addresses of the switch. Otherwise, it will use switch's static IP configuration. - Fallback(Seconds), means the waiting time for switch to get dynamic IP address via DHCP. The value of "0" here means never over the time. - Current Lease, means the IP address get from DHCP
IPv4	- Address: static IPv4 address entered by user. - Mask Length: static IPv4 subnet mask entered by user.

Click "Add Interface"to create a new management for VLAN and IP address. Click "Save"to save settings.

Note: The switch only created VLAN1 by default. If user needs to use other VLAN for switch management, please first add VLAN in the VLAN module, and add the relevant port to the VLAN.

2.2 SNTP Configuration

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. You can specify SNTP Servers and set GMT Time zone. The SNTP Configuration screens will appear after you click "Network Admin" > "NTP".

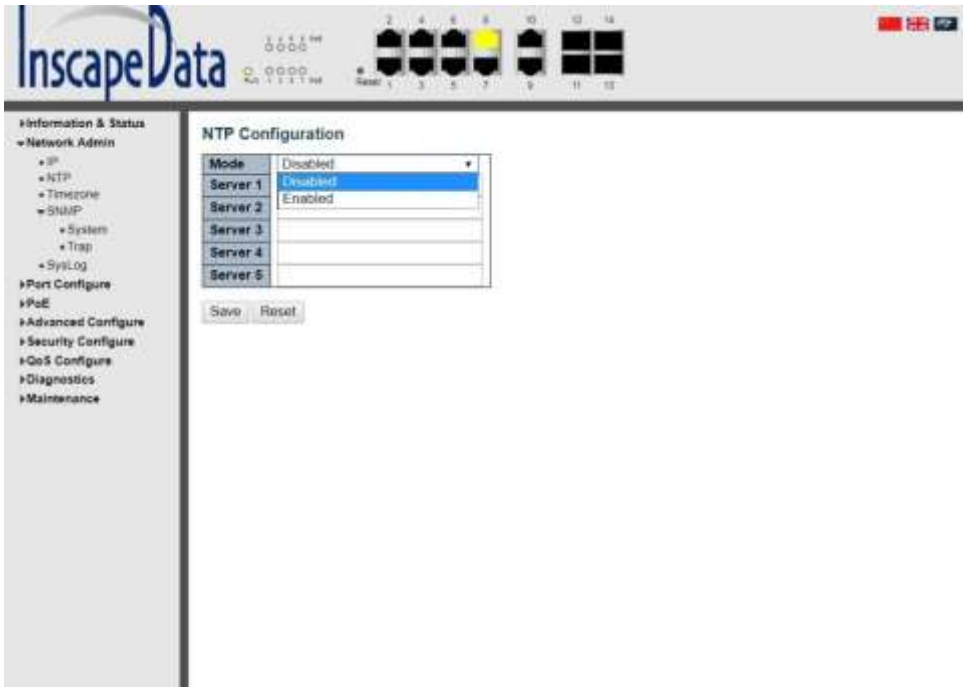


Figure 2-2 SNTP Setting Screen

Configuration object and description is:

Object	Description
Mode	Click drop-down menu to select "Enabled" or "Disabled" SNTP. Enabled: Enable SNTP mode operation. When enabling SNTP mode operation, the agent forwards and transfers SNTP messages between the clients and the server when they are not on the same subnet domain. Disabled: Disable SNTP mode operation.
SNTP Sever	After input SNTP server IP address, SNTP information will be get from that server.

After configuration was set, please click "Save" to save the setting.

2.3 SNMP Configuration

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP)protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

This switch support SNMPv1, v2c. Different versions of SNMP provide different security level for management stations and network devices.

In SNMP's v1 and v2c, it uses the "Community String" for user authentication. That string is similar to password function. SNMP application of remote user and SNMP of the Switch must use the same community string. SNMP packets of any unauthorized sites will be ignored (discarded).

"Community String" by default for switch's SNMPv1 and v2c access management is:

1. public – allow authentication management station to read MIB objects.
2. private – allow authentication management station to read, write and edit MIB objects.

Trap

Used by the agent to asynchronously inform the NMS of some event. These events may be very serious, such as reboot (someone accidentally turned off switch), or just general information, such as port status change. In these cases, switch creates trap information and sends then to receiver or network admin. Typical trap includes authentication failure, networking changes and cold/hot start trap.

MIB

A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules. Switch uses standard MIB-II information management module. So, MIB object value can be read by any SNMP web-managed software.

2.3.1 SNMP System Configuration

You can enable or disable the SNMP System Configuration. Its screen will appear after you click "Network Admin" > "SNMP" > "System"

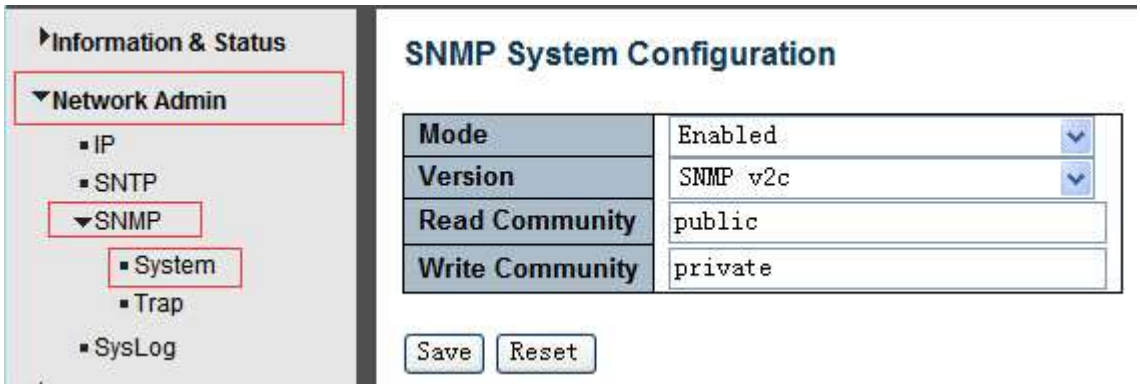


Figure 2-3 SNMP System Setting Screen

Configuration object and description is:

Object	Description
Mode	Enabled or Disable SNMP function
Version	Click drop-down menu to select SNMP v2c or SNMP v1 version
Read Community	Public: allow authentication management station to read MIB objects
Write Community	Private: allow authentication management station to read and write MIB objects.

2.3.2 SNMP Trap Configuration

User can enable or disable SNMP Trap function and set configuration. Click "Network Admin" > "SNMP" > "Trap", then this screen will show as:

2.4 System Log Configuration

User can configure switch's system log, via the following screen after click "Network Admin" > "Syslog"

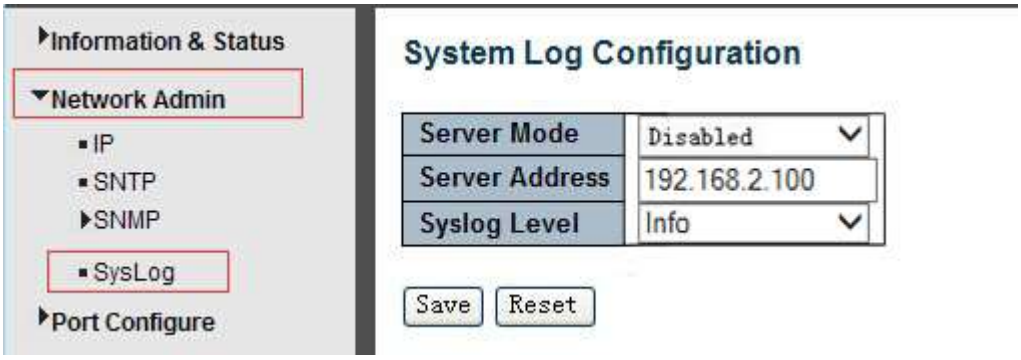


Figure 2-4 System Log Configuration Screen

Configuration object and description is:

Object	Description
Server Mode	Enabled or Disable SNMP System Log function. If "Enable"is selected, switch will send System Log to defined server.
Server Address	Defined server IP address
Syslog Level	To define leverl of System Log, including: **Info**: Information, warnings and errors. **Warning**: warnings and errors. **Error**: errors.

3. Port Configure

3.1 Port Configuration

This page is for configuring port specifications of the switch. After click "Port Configure" > "Ports", this screen will appear as:

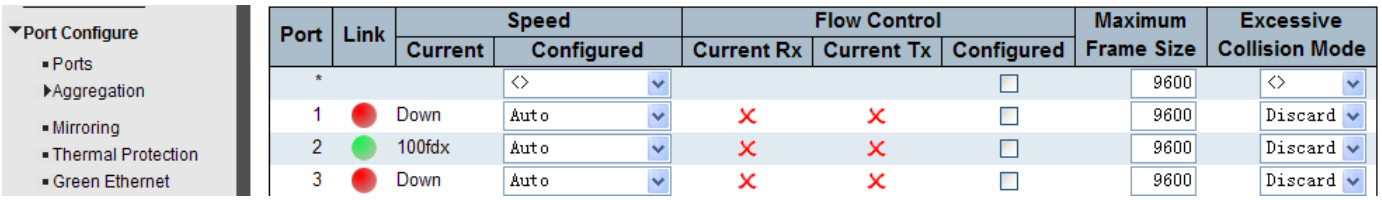


Figure 3-1 Port Configure Screen

Configuration object and description is:

Object	Description
Link	Red color means Link Down, green color means Link Up

Speed	Select the port speed and full / half duplex mode. "Disabled" means that port is disabled. "Auto" meaning in full-duplex (FDX) or half-duplex mode (HDX) (1000mbps always in full-duplex mode) auto negotiate among 10,100,1000Mbps devices. "Auto" setting allows the port to automatically determine the fastest settings for the device connected, and to apply these settings. "1000-X_AMS" means that port is Ethernet/Optical combo port, and optical port is prioritized. Other options are 10M HDX, 10M FDX, 100M HDX, 100M FDX, 1000M FDX, 1000-X.
Flow Control	It is a flow control mechanism for a variety of port configurations. Full-duplex ports use 802.3x flow control, half-duplex ports use backpressure flow control. It is disabled by default. Check to enable flow control.
Maximum Frame Size	It is used to set the maximum frame size for Ethernet. The default setting is 9600, which is to support Jumbo frames.

Click "Save" to store and active settings.

3.2 Link Aggregation

Users can set up multiple links among multiple switches. Link Aggregation, is a method that tie some physical ports together as one logic port, to enlarge bandwidth. This switch supports up to 13 groups Link Aggregation, 2 to 8 port as one group.

Note: If any port in the link aggregation group is disconnected, data packet that sent to disconnected port will share load with other connected port in this aggregation group.

3.2.1 Static Aggregation

In this page, user can configure static aggregation of switch's ports. After click the menu "Port Configure" > "Aggregation" > "Static", the following window will appear for making static aggregation settings.

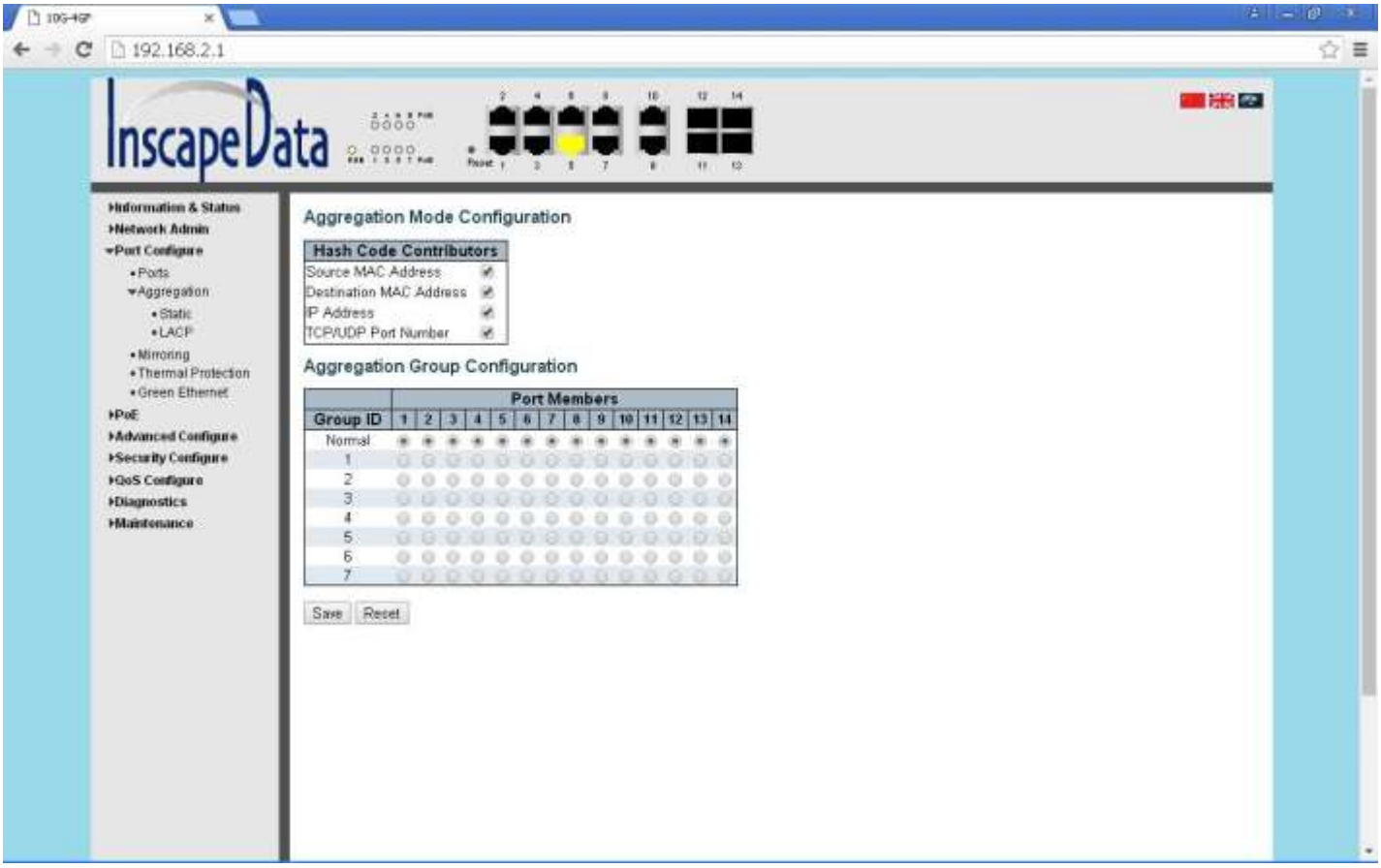


Figure 3-2 Port Static Aggregation Configuration Screen

Configuration object and description is:

Object	Description
Aggregation Mode Configuration	This parameter is flow hash algorithm among LAG(Link Aggregated Group) ports.
Group ID	Static aggregation group ID
Port Members	This switch supports up to 13 groups Link Aggregation, 2 to 8 port as one group.

Click "Save" to store and active settings.

Note: It allows a maximum of 8 ports to be aggregated as 1 static trunk group at the same time.

3.2.2 LACP Aggregation

Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems that require high-speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode. For more detailed information, refer to the IEEE 802.3ad standard.

Users can create dynamic aggregation group for switches. After click "Port Configure" > "Aggregation" > "LACP", users can set LACP configuration in the following screen.

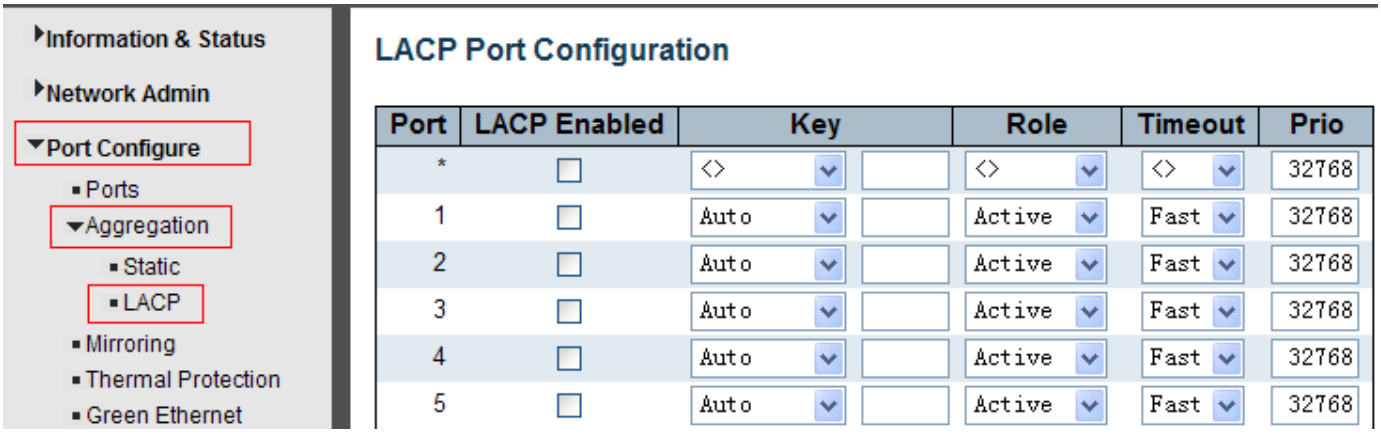


Figure 3-3 LACP Configuration Screen

Configuration object and description is:

Object	Description
LACP	Enable or disable LACP function of that port.
Key	The Key value incurred by the port, range 1-65535 . The Auto setting will set the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot.
Role	The Role shows the LACP activity status. The Active will transmit LACP packets each second, while Passive will wait for a LACP packet from a partner (speak if spoken to).
Timeout	The Timeout controls the period between BPDU transmissions. Fast will transmit LACP packets each second, while Slow will wait for 30 seconds before sending a LACP packet.
Prio	The Prio controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device then this parameter will control which ports will be active and which ports will be in a backup role. Lower number means greater priority.

Click "Save" to store and active settings.

3.3 Port Mirroring

Configure port Mirroring on this page. This function provides monitoring of network traffic that forwards a copy of each incoming or outgoing packet from one port of a network switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

To configure Mirror settings, please click "Port Configure" > "Mirroring". Then, the following screen will appear as:

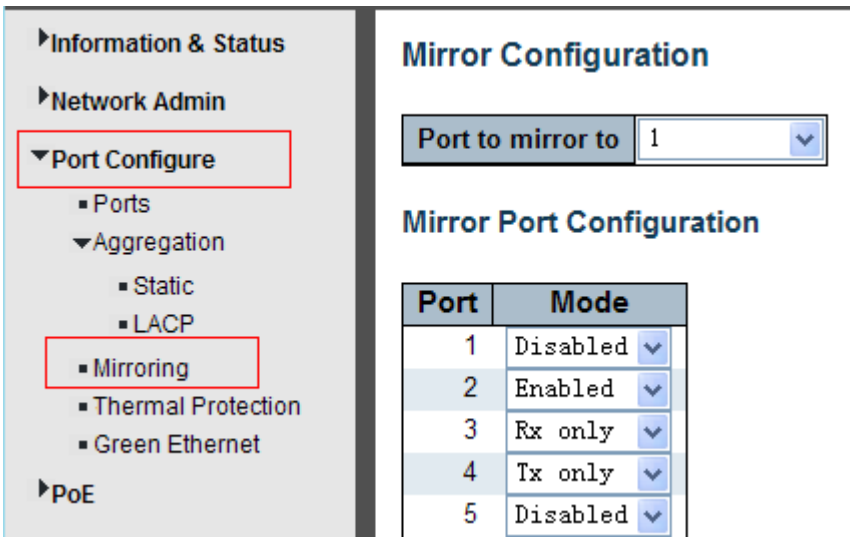


Figure 3-4 Mirror Configuration Screen

Configuration object and description is:

Object	Description
Port mirror to	Frames from ports that have either source (rx) or destination (tx) mirroring enabled are mirrored on this port. Disabled disables mirroring.
Mode	Select source port mirror mode. Rx only Frames received on this port are mirrored on the mirror port. Frames transmitted are not mirrored. Tx only Frames transmitted on this port are mirrored on the mirror port. Frames received are not mirrored. Disabled Neither frames transmitted nor frames received are mirrored. Enabled Frames received and frames transmitted are mirrored on the mirror port. Note: For a given port, a frame is only transmitted once. It is therefore not possible to mirror mirror port Tx frames. Because of this, mode for the selected mirror port is limited to Disabled or Rx only.

Click "Save" to store and active settings.

Note: You can not set fast speed port(s) mirror to a low speed port. For example, there is problem if you

try to mirror 100Mbps port(s) to a 10 Mbps port. So destination port should has equal or higher speed comparing to source port. Besides, source port and destination port should not be same one.

3.4 Thermal Protection Configuration

Thermal protection is for detecting and protecting working switch. When switch detected port temperature is higher that defined temperature, system will disable the port, to protect switch itself.

After click "Port Configure" > "Thermal Protection", the following screen will appear as:

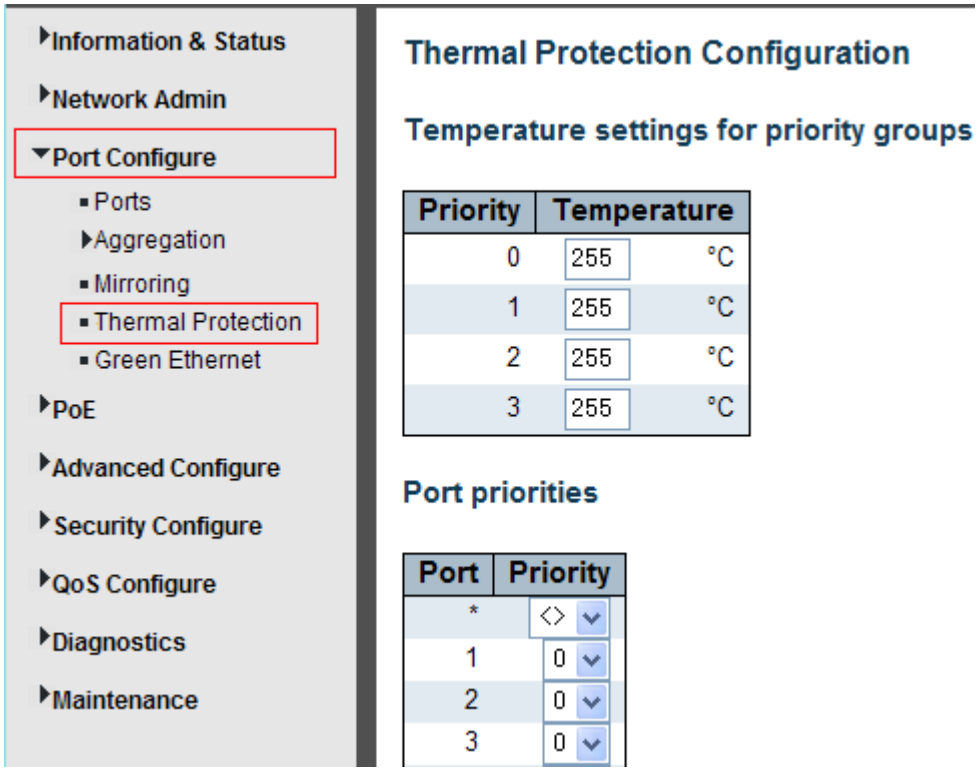


Figure 3-5 Thermal Protection Configuration Screen

Configuration object and description is:

Object	Description
Temperature settings for priority groups	This switch support 4 Thermal Protection priority groups, and each of them can have a defined temperature for protection.
Port priorities	Define which priority group that port belong to.

Click "Save" to store and active settings.

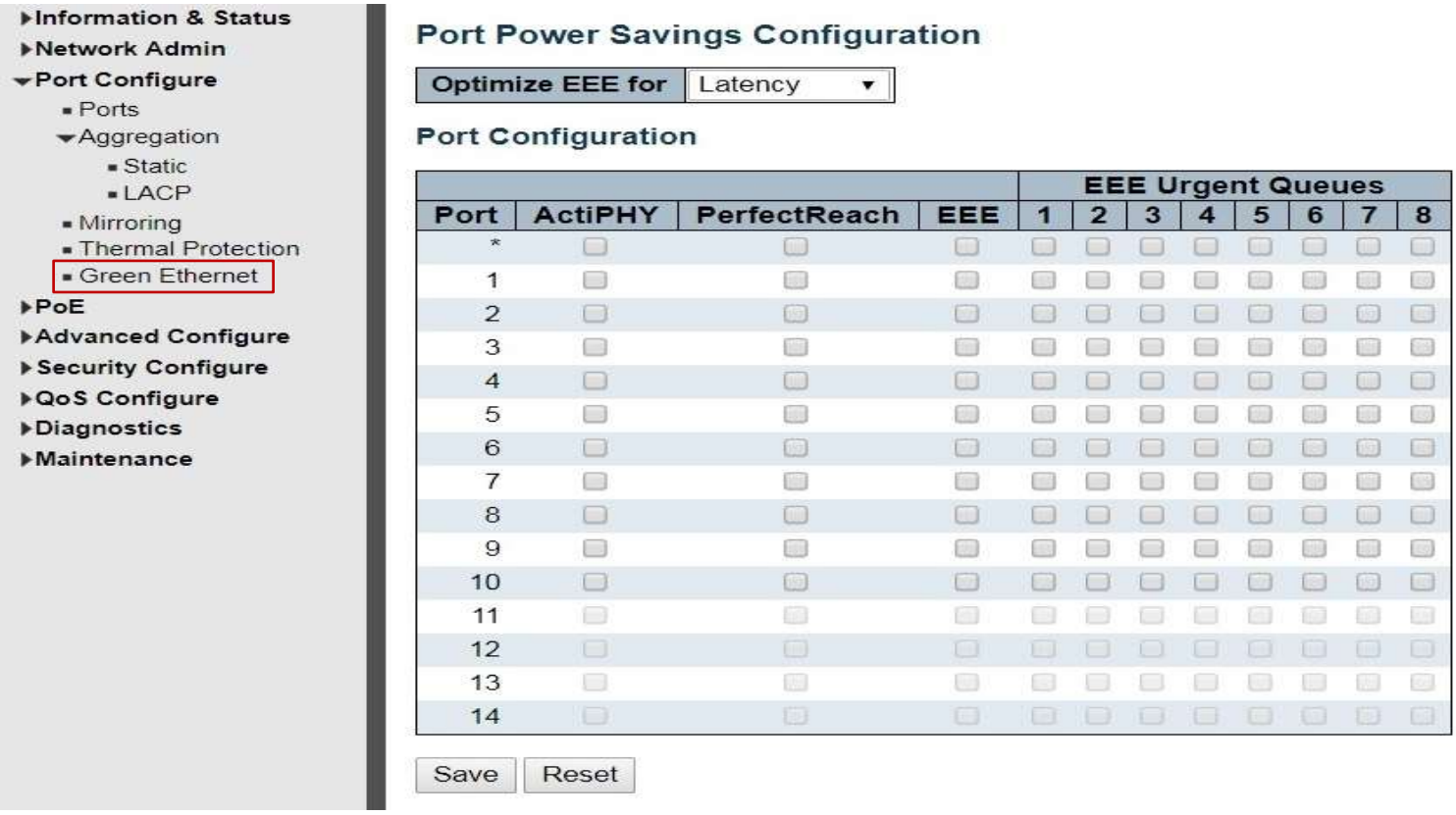
Note: By default, all ports of switch belong to Priority Group 0, with protected temperature 225 degree C.

3.4 Green Ethernet

Green Ethernet is a common name for a set of features that is designed to be environmentally friendly and reduce the power consumption of a device. Unlike Energy Efficient Ethernet (EEE), Green Ethernet energy-detection is enabled on all ports whereas only devices with gigabyte ports are enabled with EEE.

The Green Ethernet feature can reduce overall power usage in the following ways:

After click "Port Configure">"Green Ethernet", the followed screen will appear as:



Click "Save" to store and active settings.

Green Ethernet configuration object and description is:

Object	Description
Optimize EEE for Port	The switch can be set to optimize EEE for either best power saving or least traffic latency. The switch port number of the logical port.
ActiPHY	Link down power savings enabled. ActiPHY works by lowering the power for a port when there is no link. The port is power up for short moment in order to determine if cable is inserted.
PerfectReach	Cable length power savings enabled. PerfectReach works by determining the cable length and lowering the power for ports with short cables.
EEE	Controls whether EEE is enabled for this switch port. For maximizing power savings, the circuit isn't started at once transmit data is ready for a port, but is instead queued until a burst of data is ready to be transmitted. This will give some traffic latency. If desired it is possible to minimize the latency for specific frames, by mapping the frames to a specific queue (done with QOS), and then mark the queue as an urgent queue. When an urgent queue gets data to be transmitted, the circuits will be powered up at once and the latency will be reduced to the wakeup time.
EEE Urgent Queues	Queues set will activate transmission of frames as soon as data is available. Otherwise the queue will postpone transmission until a burst of frames can be transmitted.

4. PoE Configuration

Power-over-Ethernet (PoE), means Ethernet network power supply via 100BASE-TX, 1000BASE-T. Its maximum power distance is 100 meters. By PoE power system, based on Ethernet wires, e.g., UTP Cat5 or higher Cable, it can transmit power to IP cameras, VoIP phones, wireless AP, as well as transmit data concurrently. So there is no need to concern about the power wire building, reducing the cost of networking building.

PoE power supply system has unified standard, IEEE 802.3af and 802.3at. So devices from different manufacturers have no problem in general usage, as long as they are complied with these standards.

PD, it is defined as powered device in the PoE Power Supply System , primarily including IP camera, wireless AP, network VoIP phone, and other IP-based terminal equipment.

The whole process of PoE:
1. Detection: At beginning, PSE device output a very small voltage, to detect and judge if its linked PD is IEEE802.3af / IEEE802.3at compliant device. Only if detected that PD is a standard compliant device, then it will go to next step.
2. PD Classification: After detected PDs, PSE will classify them and recognize what is the power that PD required.
3. Power up: When above 2 steps finished, PSE start feeding required power for PD, with 44~57VDC output voltage.
4. Power supply: PSE provides stable 44~57V DC to PDs, and auto feeding power as requirement of PDs. Maximum power of single PoE port for IEEE 802.3af devices: 15.4W; Maximum power of single PoE port for IEEE 802.3at devices: 25.5W.
5. Disconnection: If PD is disconnected or user disable PoE from management software, PSE will quickly(300-400ms) stop powering PD.

In any moment of PSE powering PD process, PSE will stop working and then restart from step1 if abnormal situation happens, such as PD Short circuit, power consumption is higher than feeding power, and so on.

4.1 PoE Setting

After click "PoE"> "PoE Setting", user can make PoE settings in the following screen:

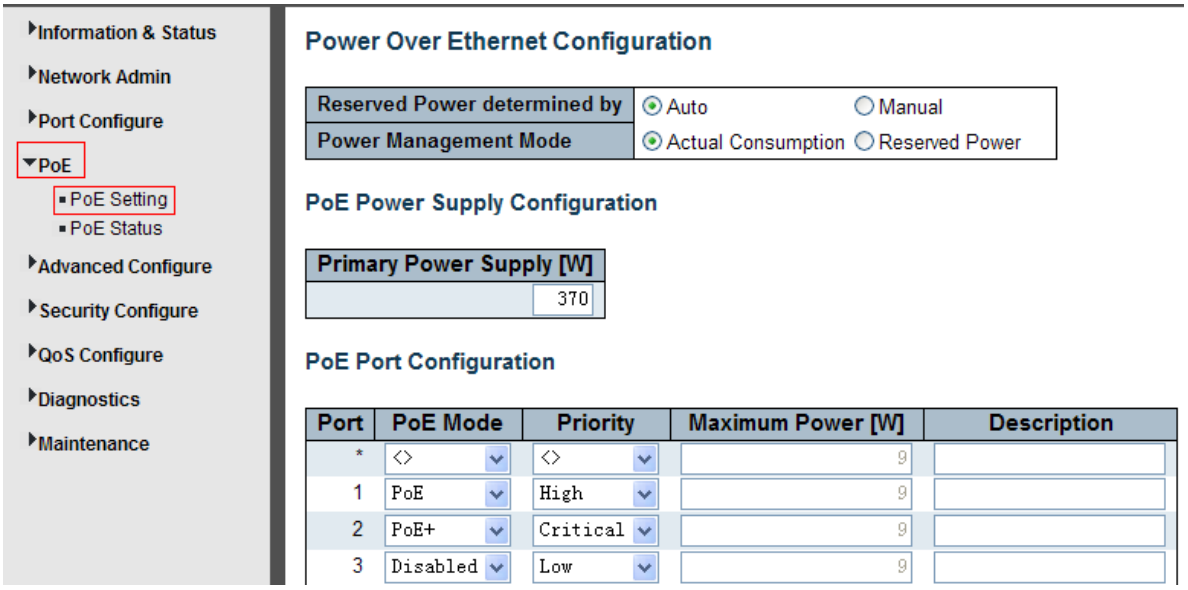


Figure 4-1 PoE Setting Screen

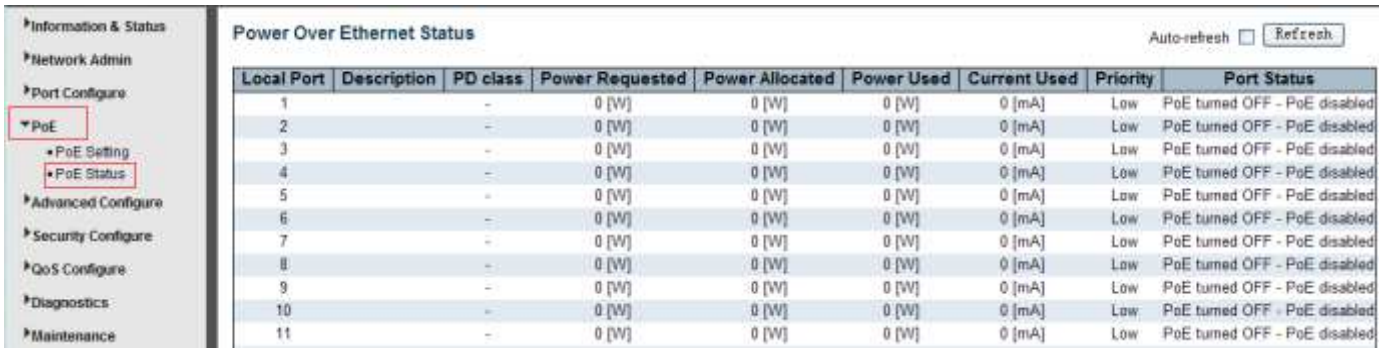
Configuration object and description is:

Object	Description
Reserved Power determined by	This switch supports 2 modes for reserved power determination. Auto: Switch automatically assigned maximum power of switch port according to detected PD class. About PD Class, please refer to the 802.3af / 802.3at definition. Manual: Maximum reserved power of the port is customize by the user.
Power Management Mode	This switch supports 2 modes for Power Management. 1. Actual Consumption: In this mode, when the actual power consumption of all the ports exceeds the switch's power budget, the lowest priority port will be shut down. If all ports have the same priority, then the maximum port number would be shut down. 2. Reserved Power: In this mode, when the reserved power consumption of all the ports exceeds the switch's power budget, the port that connect to new PD will not be enabled.
Primary Power Supply [W]	Users can set the maximum primary power of the whole switch. Default setting is 370W.
PoE Mode	This switch support 802.3af(PoE) and 802.3at(PoE+) mode. Default setting is 802.3at.
Priority	Define the priority of the PoE port. Priority from low to high is Low, High, Critical.
Maximum Power(W)	It is for define port's maximum Power when user set Manual as reserved power determination mode.

Click "Save" to store and active settings.

4.2 PoE Status

In this page, user can check and look PoE status of all ports, after click "PoE"> "PoE Status".



Local Port	Description	PD class	Power Requested	Power Allocated	Power Used	Current Used	Priority	Port Status
1		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
2		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
3		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
4		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
5		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
6		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
7		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
8		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
9		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
10		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled
11		-	0 [W]	0 [W]	0 [W]	0 [mA]	Low	PoE turned OFF - PoE disabled

Figure 4-2 PoE Status Screen

5. Advanced Configure

5.1 MAC Address Table

This page allows you to configure Mac address table settings. After Click "Advanced Configure" > "Mac Table" , the following screen will appear.

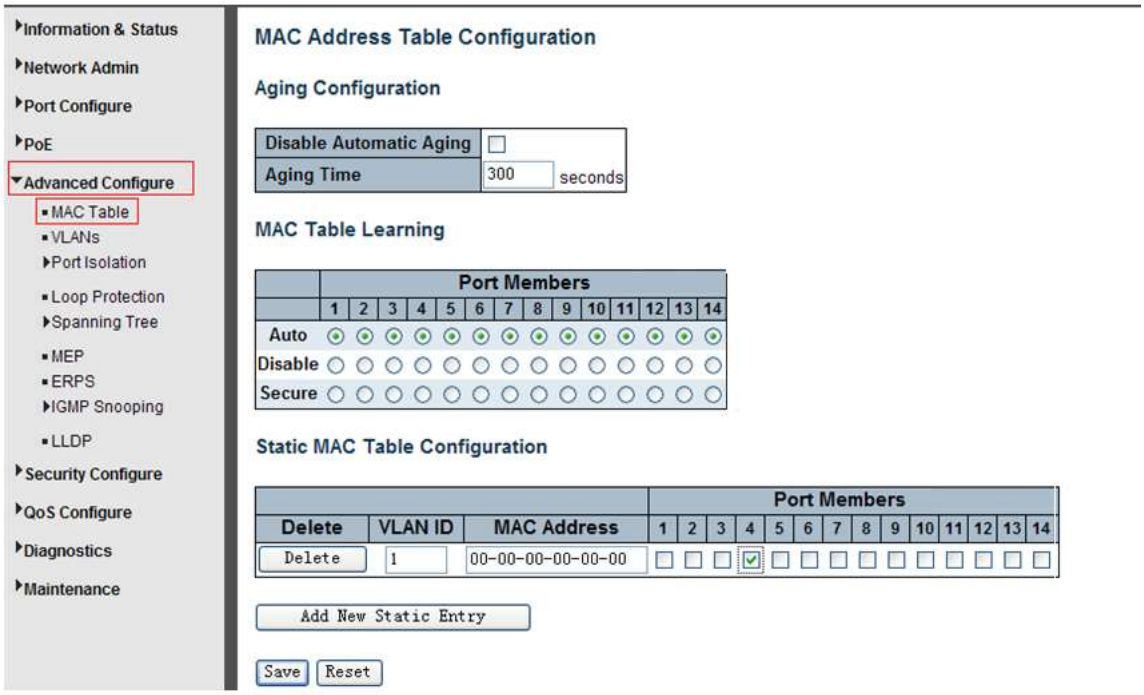


Figure 5-6 MAC Address Table Configuration Screen

Configuration object and description is:

Object	Description
Disable Automatic Aging	If the box is checked, then the automatic aging function is disabled.
Aging Time	The time after which a learned entry is discarded . Range: 10-1000000 seconds; Default: 300 seconds.
MAC Table Learning	This switch supports 3 types for MAC Table Learning 1. Auto: port will auto learn Mac address. 2. Disable: port will NOT learn MAC address. 3. Secure: port only forward data of configured static MAC address.
Static MAC Table Configuration	The static entries in the MAC table are shown in this table. Click "Add New Static Entry" to create a new record.

Click "Save" to store and active settings.

5.2 VLAN

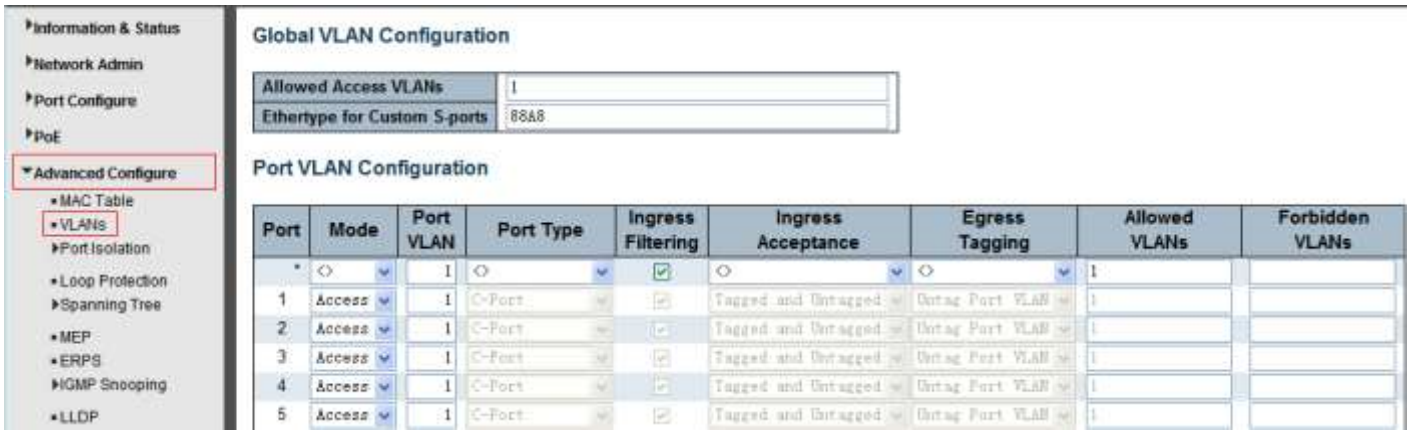
Adding virtual LAN (VLAN) support to a Layer 2 switch offers some of the benefits of both bridging and routing. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast. Like a router, it partitions the network into logical segments, which provides better administration,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

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

Each VLAN in a network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on a VLAN. An end station might omit the tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet can either reject it or insert a tag using its default VLAN ID. A given port can handle traffic for more than one VLAN, but it can support only one default VLAN ID.
The Private Edge VLAN feature lets you set protection between ports located on the switch. This means that a protected port cannot forward traffic to another protected port on the same switch. The feature does not provide protection between ports located on different switches.

VLAN (Virtual Local Area Network) logically divide one LAN(Local Area Network) into a plurality of subsets, and each subset will form their own broadcast area network. In short, VLAN is a communication technology that logically divide one physical LAN into multiple broadcast area network (multiple VLAN). Hosts within a VLAN can communicate directly. But VLAN groups can not directly communicate with each other. So it will limit the broadcast packets within a VLAN. Since it can not directly access between VLAN groups, thus it improves network security.

Click "Advanced Configure"> "VLANs" to see 802.1Q VLAN configuration screen as the following:



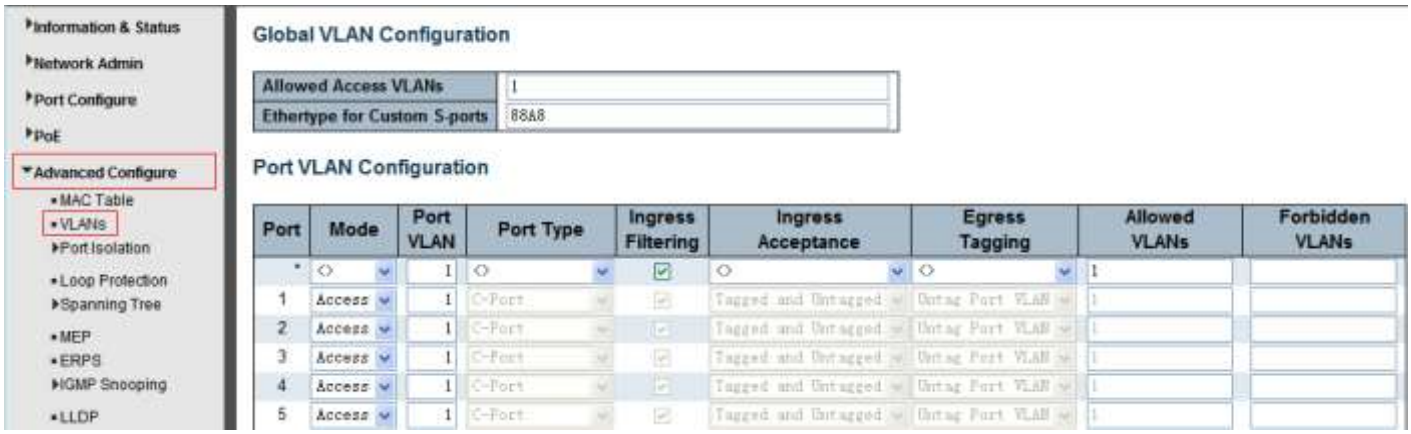


Figure 5-1 802.1Q VLAN Configuration Screen

VLAN configuration object and description:

Object	Description
Allowed VLANs	Here displays created VLAN ID. It is 1 by default. If you want to create new VLAN, just need to add VLAN ID here.
Ethertype for Custom S-ports	This field specifies the ethertype/TPID (specified in hexadecimal) used for Custom S-ports. The setting is in force for all ports whose Port Type is set to S-Custom-Port.
Mode	The port mode (default is Access) determines the fundamental behavior of the port in question. A port can be in one of three modes as described below. Whenever a particular mode is selected, the remaining fields in that row will be either grayed out or made changeable depending on the mode in question. Grayed out fields show the value that the port will get when the mode is applied. **Access:** Access ports are normally used to connect to end stations. Access ports have the the following characteristics: • Member of exactly one VLAN, the Port VLAN (a.k.a. Access VLAN), which by default is 1 • Accepts untagged and C-tagged frames • Discards all frames that are not classified to the Access VLAN • On egress all frames classified to the Access VLAN are transmitted untagged. Other (dynamically added VLANs) are transmitted tagged **Trunk:** Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics: • By default, a trunk port is member of all VLANs (1-4094) • The VLANs that a trunk port is member of may be limited by the use of Allowed VLANs • Frames classified to a VLAN that the port is not a member of are discarded • By default, all frames but frames classified to the Port VLAN (a.k.a. Native VLAN) get tagged on egress. Frames classified to the Port VLAN do not get C-tagged on egress • Egress tagging can be changed to tag all frames, in which case only tagged

	frames are accepted on ingress **Hybrid:** Hybrid ports resemble trunk ports in many ways, but adds additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have these abilities: • Can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware • Ingress filtering can be controlled • Ingress acceptance of frames and configuration of egress tagging can be configured independently
Port VLAN	Determines the port's VLAN ID (a.k.a. PVID). Allowed VLANs are in the range 1 through 4094, default being 1. On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0). On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging configuration is set to untag Port VLAN. The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.
Port Type	Ports in hybrid mode allow for changing the port type, that is, whether a frame's VLAN tag is used to classify the frame on ingress to a particular VLAN, and if so, which TPID it reacts on. Likewise, on egress, the Port Type determines the TPID of the tag, if a tag is required. **Unaware:** On ingress, all frames, whether carrying a VLAN tag or not, get classified to the Port VLAN, and possible tags are not removed on egress. **C-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with a C-tag. **S-Port:** On ingress, frames with a VLAN tag with TPID = 0x8100 or 0x88A8 get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with an S-tag. **S-Custom-Port:** On ingress, frames with a VLAN tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S ports get classified to the VLAN ID embedded in the tag. If a frame is untagged or priority tagged, the frame gets classified to the Port VLAN. If frames must be tagged on egress, they will be tagged with the custom S-tag.
Ingress Filter	Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled. If ingress filtering is enabled (checkbox is checked), frames classified to a VLAN that the port is not a member of get discarded. If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.。

Ingress Acceptance	Hybrid ports allow for changing the type of frames that are accepted on ingress. **Tagged and Untagged** Both tagged and untagged frames are accepted. **Tagged Only** Only tagged frames are accepted on ingress. Untagged frames are discarded. **Untagged Only** Only untagged frames are accepted on ingress. Tagged frames are discarded.
Egress Tagging	Ports in Trunk and Hybrid mode may control the tagging of frames on egress. **Untag Port VLAN** Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag. **Tag All** All frames, whether classified to the Port VLAN or not, are transmitted with a tag. **Untag All** All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.
Allowed VLANs	Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be member of one VLAN, the Access VLAN. The field's syntax is identical to the syntax used in the Enabled VLANs field. By default, a Trunk or Hybrid port will become member of all VLANs, and is therefore set to **1-4094**. The field may be left empty, which means that the port will not become member of any VLANs.
Forbidden VLANs	A port may be configured to never be member of one or more VLANs. This is particularly useful when dynamic VLAN protocols like MVRP and GVRP must be prevented from dynamically adding ports to VLANs. The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Enabled VLANs field. By default, the field is left blank, which means that the port may become a member of all possible VLANs.

Click "Save" to store and active settings.

5.2 Port Isolation

Port isolation is for limiting data between ports. It is similar to VLAN, but more stricter.

5.2.1 Port Group

This switch support port groups. Members of port group can forward date.

Note: port can belong to to multiple port groups. Data can be forwarded among any port that belong to one port group.

After Click "Advanced Configure" > "Port Isolation" > "Port Group", then the following screen will appear for making port group configuration.

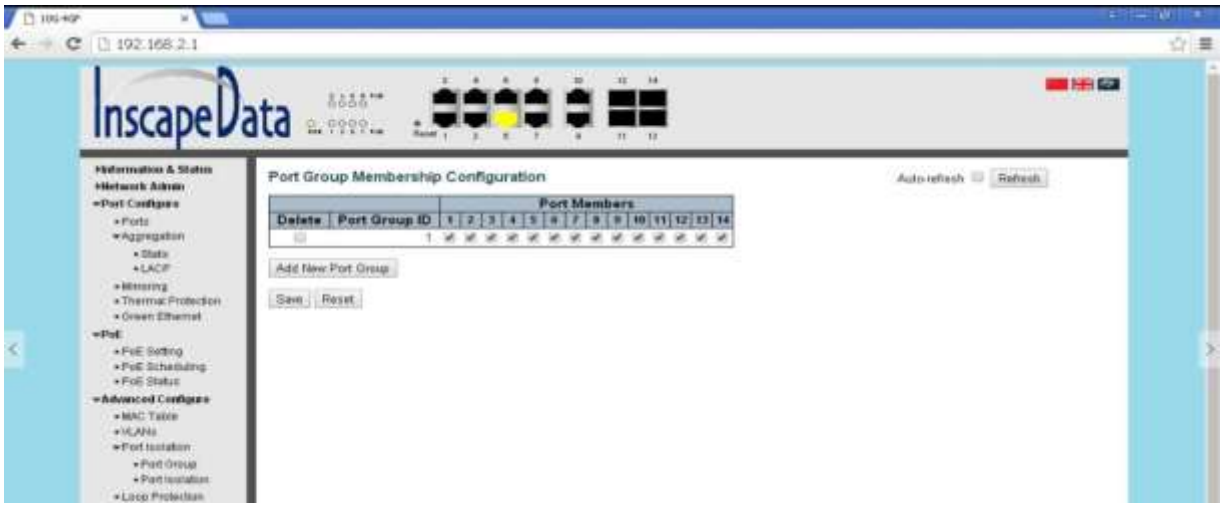


Figure 5-2 Port Group Configuration Screen

Configuration object and description is:

Object	Description
Port Members	Check the corresponding box to set them as one port group.

Click "Add New Port Group" to create a new port group, "Delete" to remove corresponding port group, and "Save" to store and active settings.

5.2.2 Port Isolation

After Click "Advanced Configure" > "Port Isolation" > "Port Isolation", then the following screen will appear for making port isolation configuration.

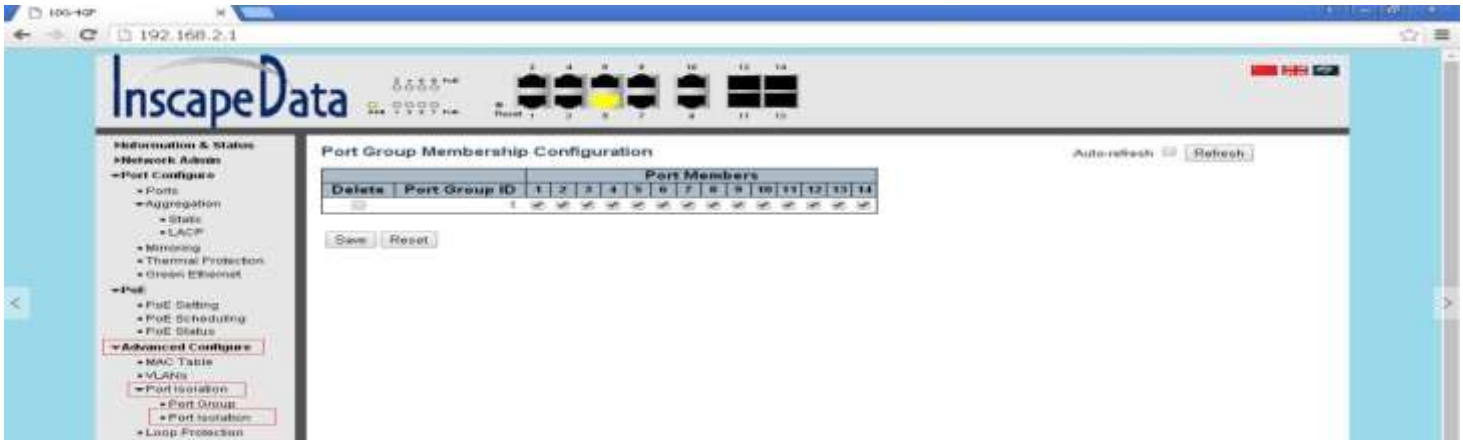


Figure 5-3 Port Isolation Configuration Screen

Configuration object and description is:

Object	Description
Port Number	Check box to set corresponding port as port isolation, so that they can not forward data flow.

Click "Save" to store and active settings.

5.3 STP

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

5.3.1 STP Bridge Settings

This page allows you to configure port STP settings. After Click "Advanced Configure" > "Spanning Tree" > "Bridge Settings" ,the following screen will appear.

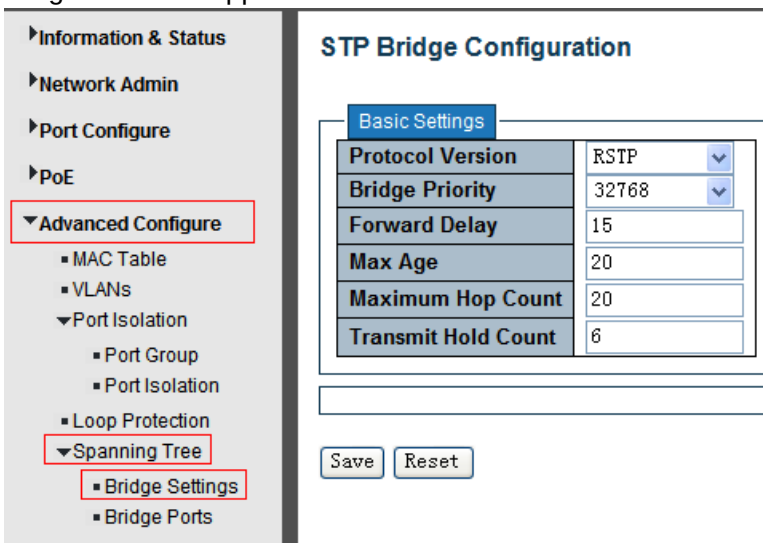


Figure 5-4 Spanning Tree Configuration Screen

Configuration object and description is:

Object	Description
Protocol Version	Click drop-down menu to select STP protocol version, including: STP - Spanning Tree Protocol (IEEE802.1D); RSTP - Rapid Spanning Tree Protocol (IEEE802.1w)
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a *Bridge Identifier*.
Forward Delay (4-30)	Forward Delay setting range is from 4 to 30 seconds. Default value is 15 seconds.
Max Age (6-40)	The maximum age of the information transmitted by the Bridge when it is the Root

	Bridge. Valid values are in the range 6 to 40 seconds. Default value is 20 .
Maximum Hop Count (6-40)	This defines the initial value of remaining Hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDU information. Valid values are in the range 6 to 40 hops.
Transmit Hold Count (1-10)	The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second. Default value is 6 .

Click "Save" to store and active settings.

5.3.2 STP Bridge Port

After Click "Advanced Configure" > "Spanning Tree" > "Bridge Ports" , the following screen will appear.

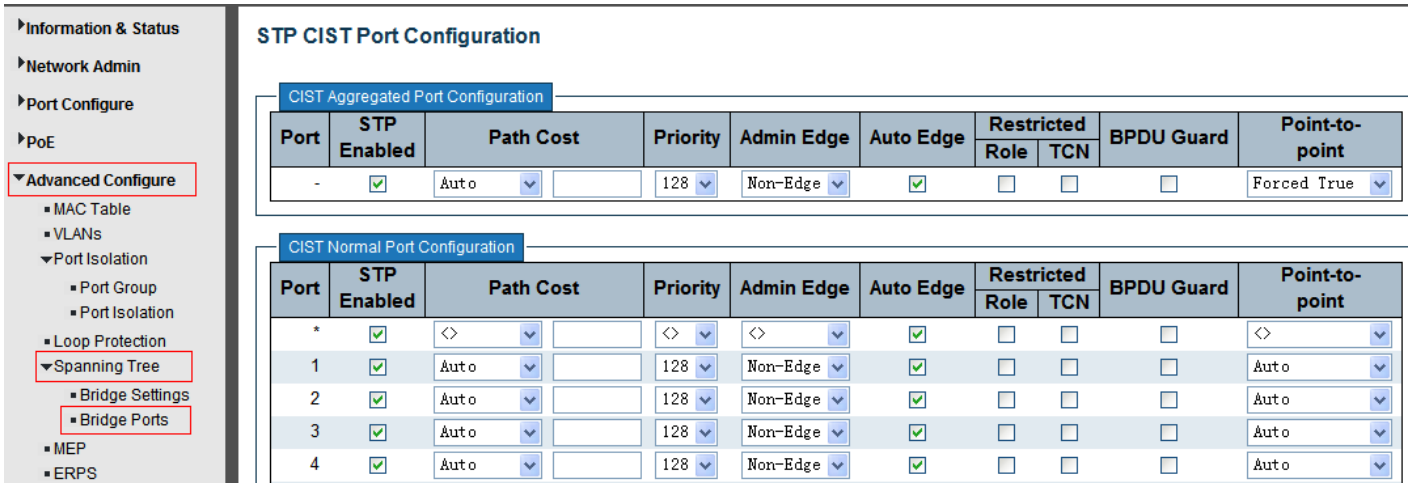


Figure 5-5 STP Configuration Screen

Configuration object and description is:

Object	Description
STP Enabled	Check to enable STP function.
Path Cost(0=Auto)	Controls the path cost incurred by the port. The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values. Using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favour of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Controls the port priority. This can be used to control priority of ports having identical port cost. (See above).
Auto Edge	Check box to set corresponding port as Auto Edge.
Restricted Role	Check box to set corresponding port as Restricted Role

Restricted TCN	Check box to set corresponding port as Restricted TCN
BPDU Guide	Check box to enable BPDU Guide. So when port receives BPDU reception, it will turn to Disable(Shut Down) status.
Point-to-point	Controls whether the port connects to a point-to-point LAN rather than a shared medium. This can be automatically determined, or forced either true or false. Transition to the forwarding state is faster for point-to-point LANs than for shared media. (This applies to physical ports only. Aggregations are always forced Point2Point.

Click "Save" to store and active settings.

5.4 MAC Address Table

This page allows you to configure Mac address table settings. After Click "Advanced Configure" > "Mac Table", the following screen will appear.

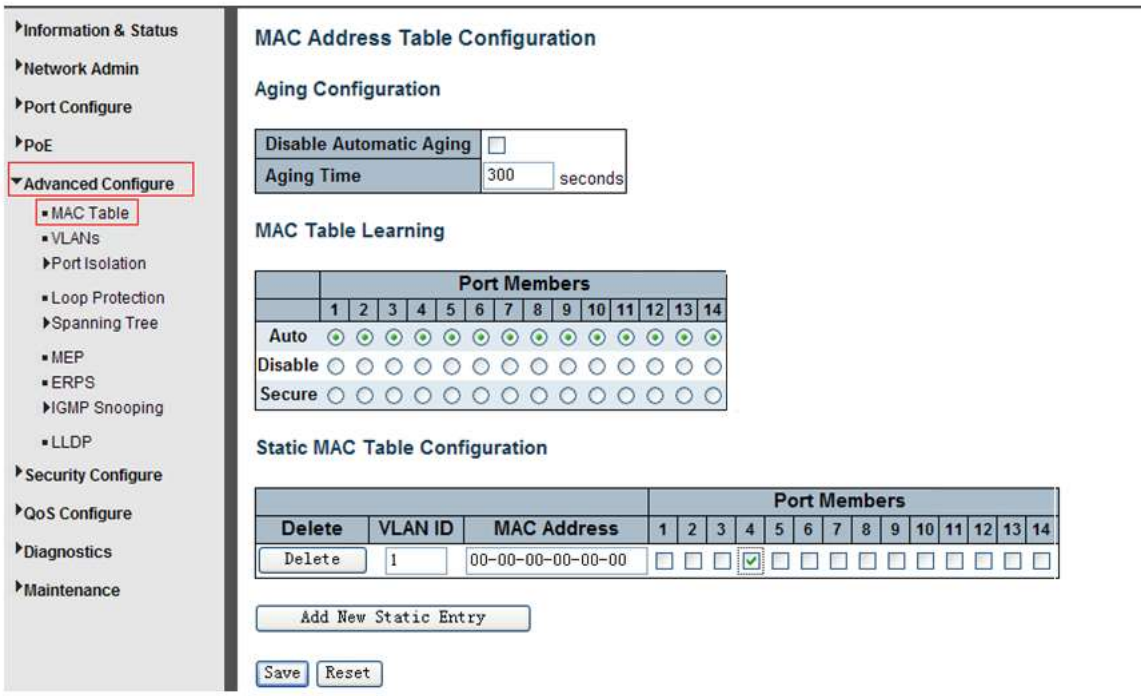


Figure 5-6 MAC Address Table Configuration Screen

Configuration object and description is:

Object	Description
Disable Automatic Aging	If the box is checked, then the automatic aging function is disabled.
Aging Time	The time after which a learned entry is discarded . Range: 10-1000000 seconds; Default: 300 seconds.

MAC Table Learning	This switch supports 3 types for MAC Table Learning 1. Auto: port will auto learn Mac address. 2. Disable: port will NOT learn MAC address. 3. Secure: port only forward data of configured static MAC address.
Static MAC Table Configuration	The static entries in the MAC table are shown in this table. Click "Add New Static Entry" to create a new record.

Click "Save" to store and active settings.

5.5 IGMP Snooping

Internet Group Management Protocol (IGMP) lets host and routers share information about multicast groups memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for feature processing. The overall purpose of IGMP Snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.

5.5.1 Basic Configuration

After Click "Advanced Configure" > "IGMP Snooping" > "Basic Configuration", the following screen will appear.

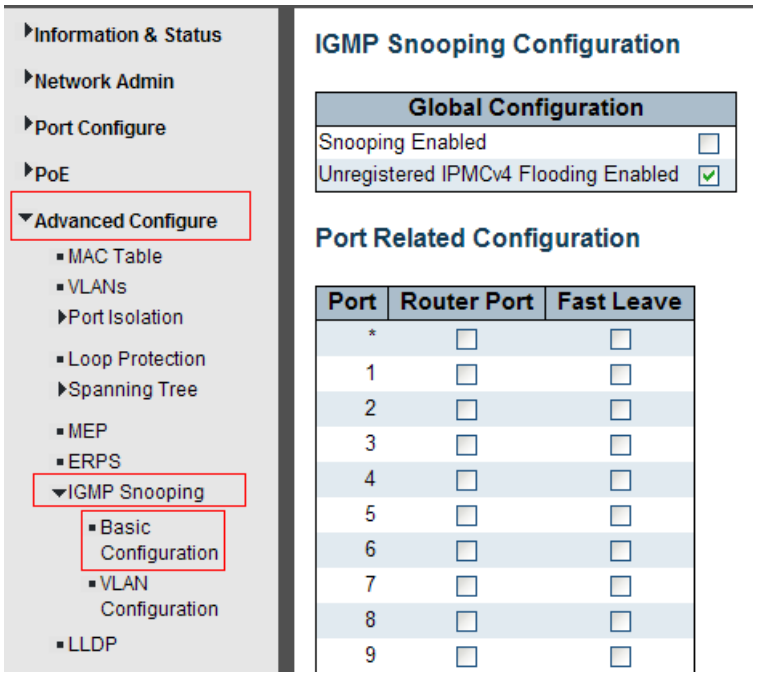


Figure 5-7 IGMP Snooping Basic Configuration

Configuration object and description is:

Object	Description
Snooping Enabled	Enable or disable the IGMP snooping. The default value is "Disabled". Enable: check the box; Disable: do not check the box.
Unregistered IPMCv4 Flooding Enabled	Check the box to enable unregistered IPMCv4 Flooding

Router Port	Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Fast leave performs deleting MAC forward entry immediately upon receiving message for group de-registration

Click "Save" to store and active settings.

5.5.2 IGMP Snooping VLAN Configuration

After Click "Advanced Configure" > "IGMP Snooping" > "VLAN Configuration", the following screen will appear.

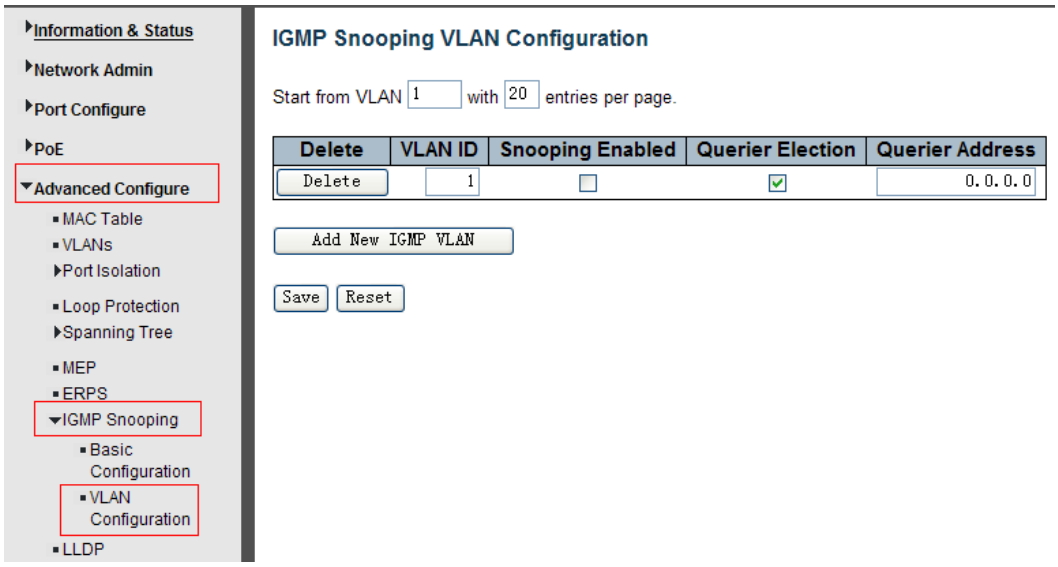


Figure 5-7 IGMP Snooping VLAN Configuration

Configuration object and description is:

Object	Description
Snooping Enabled	Enable the per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.
Querier Election	Enable to join IGMP Querier election in the VLAN. Disable to act as an IGMP Non-Querier.
Querier Address	Define the IPv4 address as source address used in IP header for IGMP Querier election. When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, system uses the first available IPv4 management address. Otherwise, system uses a pre-defined value. By default, this value will be 192.0.2.1.

Click "Save" to store and active settings.

5.6 ERPS

ERPS(Ethernet Ring Protection Switching), it integrates OAM function and APS protocol. If the ring network was interrupted accidentally, the fault recovery times could be less than 50ms to quickly bring the network back to normal operation. ITU-T G.8032 is the first industry standard for ERPS.

Note: Before enable ERPS, STP of ring port should be disabled.

After Click "Advanced Configure" > "ERPS ", the following screen will appear.

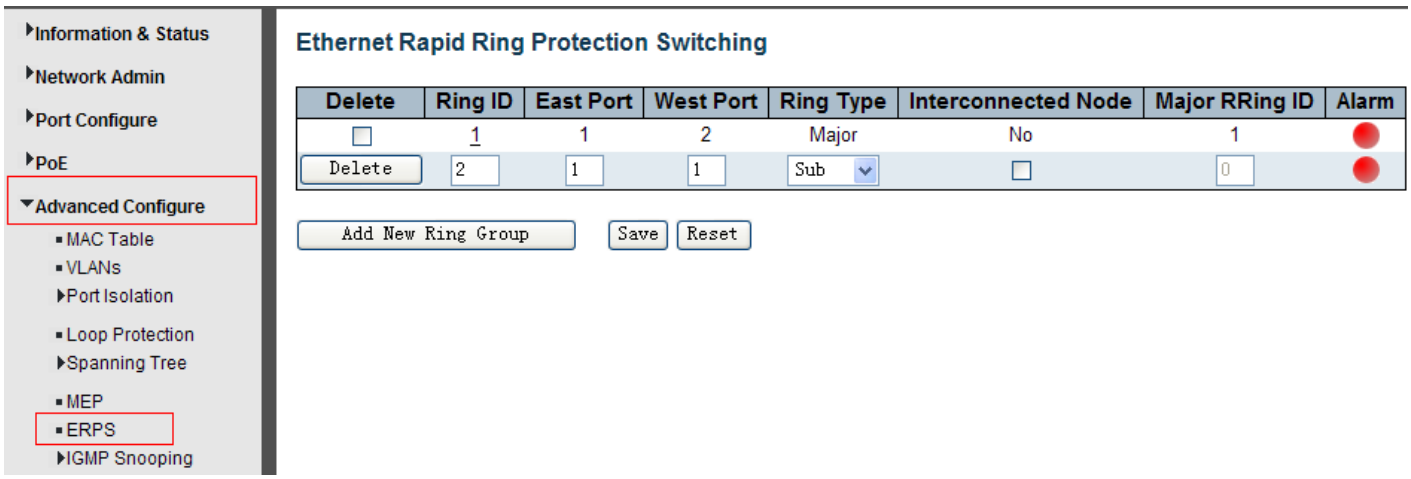


Figure 5-8 EPRS Configuration

Configuration object and description is:

Object	Description
Ring ID	ERPS Ring ID
East Port	Number of the port which participate in this Ring protection.
West Port	Number of the other port which participate in this Ring protection.
Ring Type	Available selection: "Major Ring" or "Sub Ring". Only in case of Multi Ring application, "Sub Ring" is required to configure. Default Ring Type: "Major Ring". Only if there is multi ring application, it is required to set.
Interconnected Node	In Multi Ring application, Interconnected Node is the node that connect 2 or more rings.
Major Ring ID	In Single Ring application, Major Ring ID is same as Ring ID. In Multi Ring application, Sub Ring has to be type as Major Ring ID.
R-APS VLAN(1-4094)	Define VLAN for R - APS VLAN .

Click "Add New Ring Group" to create a new ERPS ring application.

Click "Save" to store and active settings.

After click the number under "Ring ID", it will go to the page for Ring Configuration as the following screen:

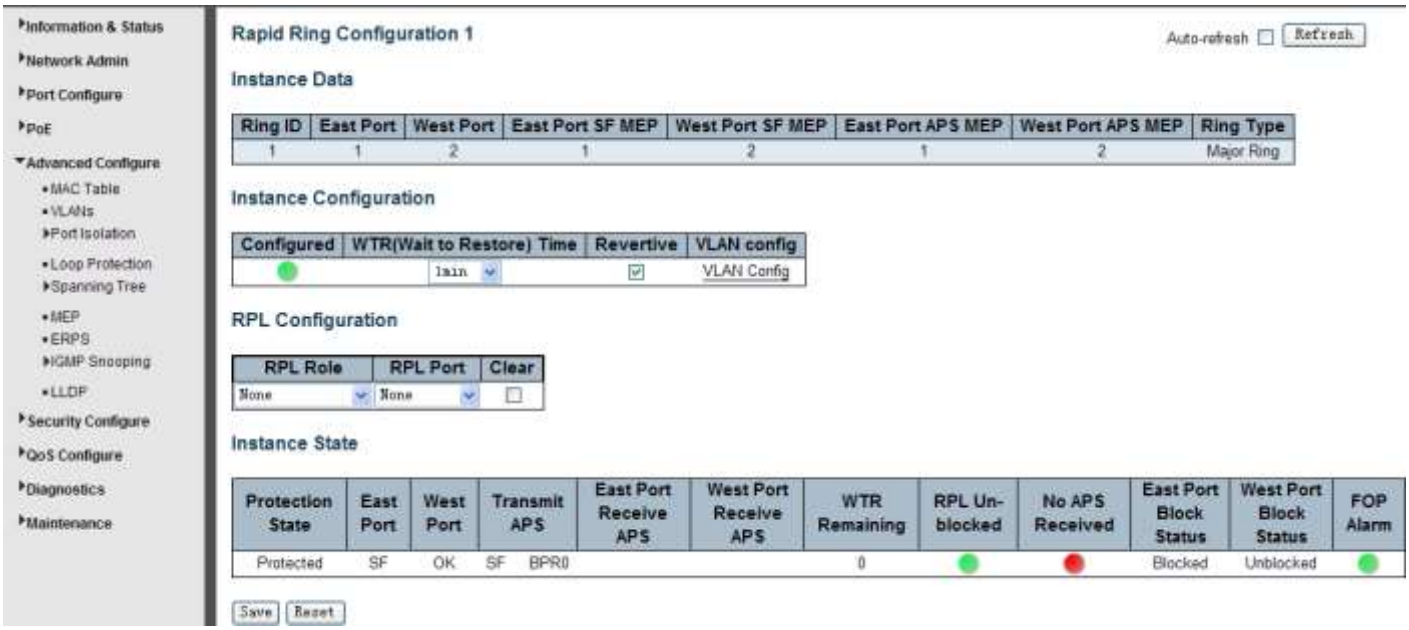


Figure 5-9 EPRS Ring Configuration

Configuration object and description is:

Object	Description
WTR(Wait to Restore) Time(1-12)	Click Click drop-down menu to select WTR time for R-APS. Available selection: 1-12min Default: 1 min
Revertive	Check to enable Revertive status of R-APS.
VLAN config	After clicked " VLAN config ", it will go the page of Rapid Ring VLAN Configuration.
RPL Role	Click drop-down menu to select "None", "RPL Owner", or "RPL Neighbor" role.
RPL Port	Click drop-down menu to select "None", "East Port", or "West Port".

Click "Save" to store and active settings.

After clicked " VLAN config ", it will go the page of Rapid Ring VLAN Configuration as the following screen:

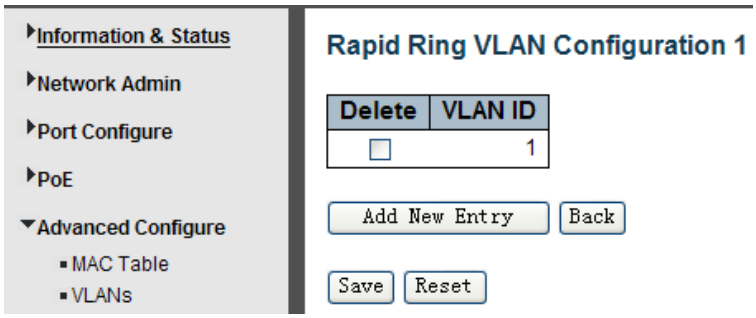


Figure 5-10 Rapid Ring VLAN Configuration

Click "Add New Entry" to create a new entry. Click "Save" to store and active settings.

5.7 LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

After Click "Advanced Configure" > "LLDP", the following screen will appear.

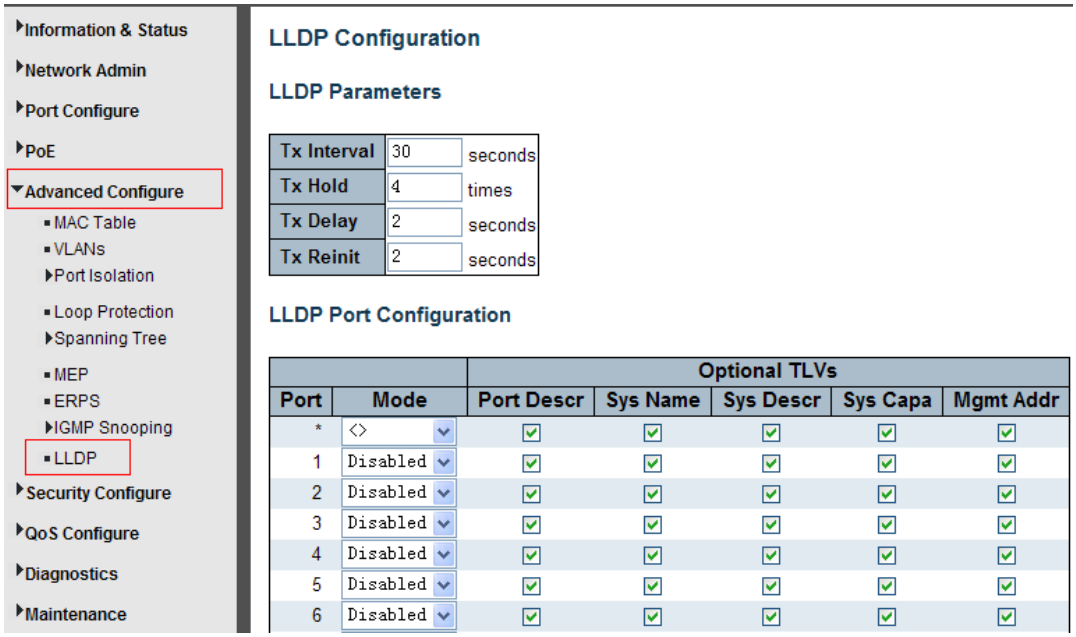


Figure 5-10 LLDP Configuration Screen

Configuration object and description is:

Object	Description
LLDP Parameters	Here allows the user to inspect and configure the current LLDP port settings: ➢ Tx Interval: Transmission Interval Time ➢ Tx Hold: Hold time Multiplier ➢ Tx Delay: Transmit Delay Time ➢ Tx Remit: Transmit Remit Time
Mode	Select LLDP messages transmit and receive modes for LLDP Protocol Data Units. Options are Tx only, Rx only, Enabled, and Disabled.
Optional TLVs	To configure the information included in the TLV field of advertised messages. When the following option is checked, corresponding information will be included in LLDP information transmitted. ➢ Port Descr: Port Description ➢ Sys Name: System Name ➢ Sys Descr: System Description ➢ Sys Capa: System Capability ➢ Mgmt Addr: Management Address

Click "Save" to store and active settings.

5.8 Loop Protection

Loop protection is to avoid broadcast loops. After Click "Advanced Configure" > "Loop Protection", the following screen will appear.

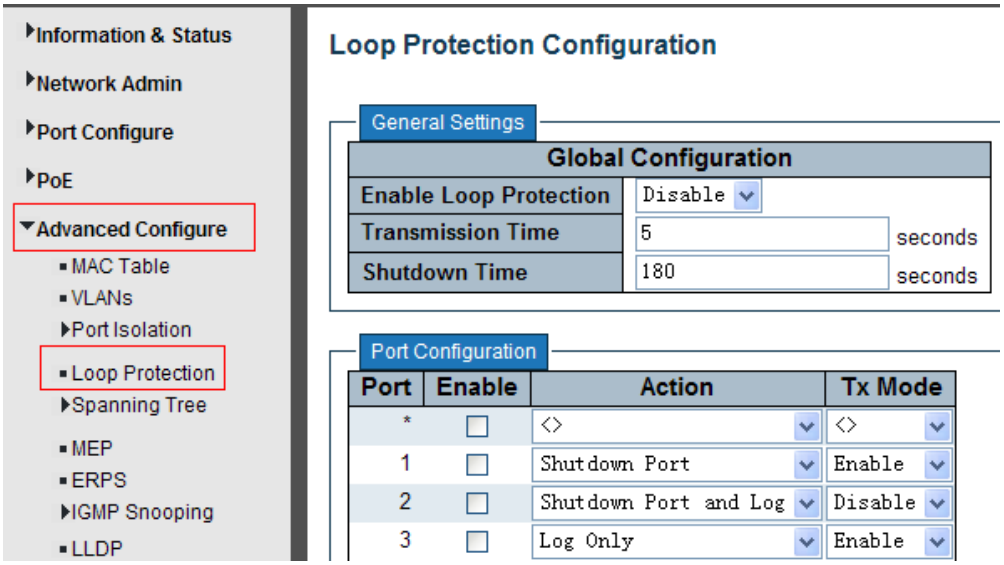


Figure 5-11 Loop Protection Configuration Screen

Configuration object and description is:

Object	Description
Global Configuration	Enable Loop Protection: click drop-down menu to disable or enable Loop Protection; Transmission Time: enter a number to set Loop Protection Interval Time; Shutdown Time: enter a number to set port Shutdown Time.
Enable	Check to enable corresponding port loop protection.
Action	Action take when the port detected loop. There are 3 types of action for users to select, Shutdown port, Shutdown port and Log, Log Only.
Tx Mode	To enable or disable Tx.

Click "Save" to store and active settings.

6. QoS Configuration

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic. This function does not only reserve network bandwidth, but it can also limits other traffic that is "less important".

6.1 QoS Port Classification

After Click "QoS Configure" > "Port Classification", the following screen will appear.

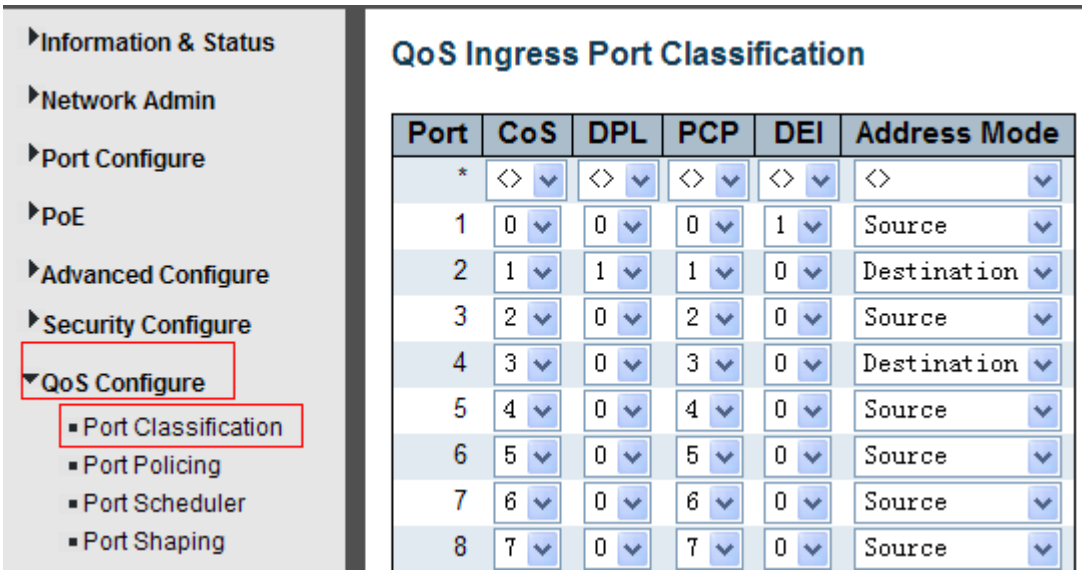


Figure 6-1 Port Classification Configuration Screen

Configuration object and description is:

Object	Description
CoS	Controls the default class of service, ranging from 0 (lowest) to 7 (highest). All frames are classified to a CoS. There is a one to one mapping between CoS, queue and priority. A CoS of 0 (zero) has the lowest priority The classified CoS can be overruled by a QCL entry. Note: If the default CoS has been dynamically changed, then the actual default CoS is shown in parentheses after the configured default CoS.
DPL	Controls the default drop precedence level. All frames are classified to a drop precedence level. The classified DPL can be overruled by a QCL entry.

PCP	Controls the default PCP value. All frames are classified to a PCP value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	Controls the default DEI value. All frames are classified to a DEI value. If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Address Mode	The IP/MAC address mode specifying whether the QCL classification must be based on source (SMAC/SIP) or destination (DMAC/DIP) addresses on this port. The allowed values are: Source: Enable SMAC/SIP matching. Destination: Enable DMAC/DIP matching.

Click "Save" to store and active settings.

6.2 Port Policing

After Click "QoS Configure" > "Port Policing", the following screen will appear.

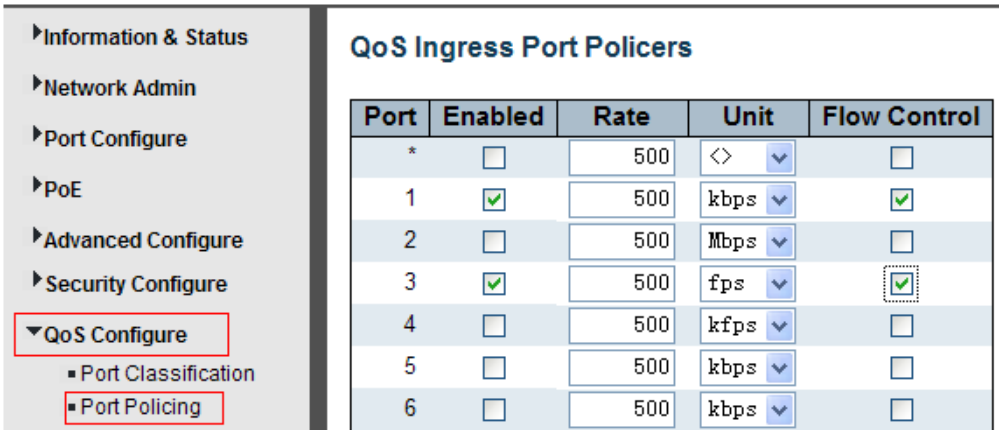


Figure 6-2 Port Policing Configuration Screen

Configuration object and description is:

Object	Description
Enabled	Check the box to enable Port Policing.
Rate	Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
Unit	Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.

Click "Save" to store and active settings.

6.3 Storm Control Configuration

After Click "QoS Configure" > "Storm Control", the following screen will appear.

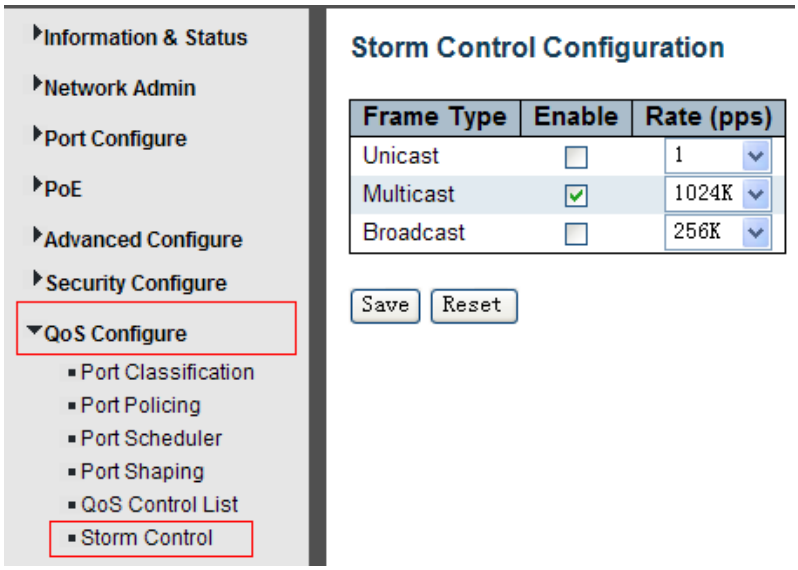


Figure 6-3 Port Policing Configuration Screen

Configuration object and description is:

Object	Description
Frame Type	This switch supports 3 kinds of Frame Type: Unicast, Unknown Multicast, Broadcast.
Enable	Check the box to enable Storm Control.
Rate(pps)	The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.

Click "Save" to store and active settings.

7. Security Configuration

7.1 Password

To change system login password of the switch, please click "Security Configure" > "Password" .

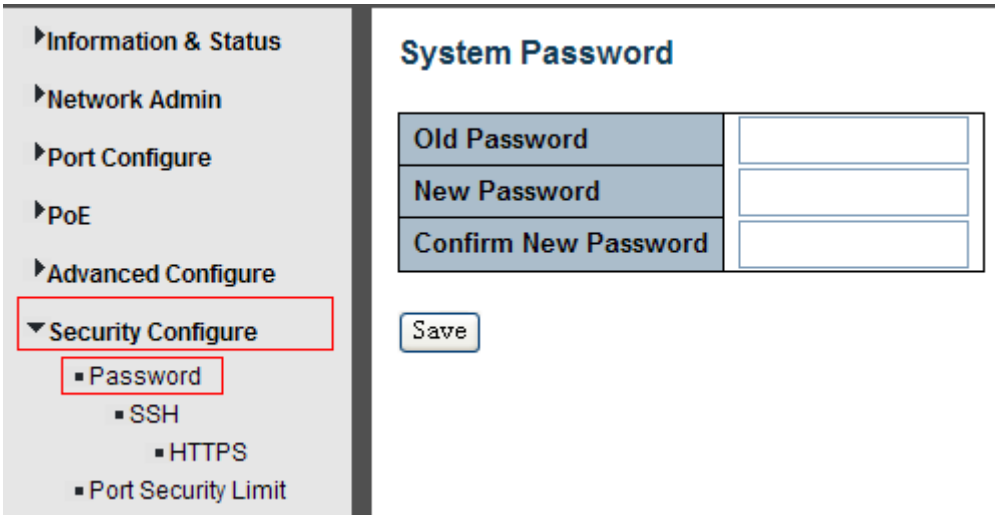


Figure 7-1 System Password Configuration Screen

Click "Save" to store and active settings.

7.2 802.1X

In the 802.1X-world, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP over LANs) frames. EAPOL frames encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets.

RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible, in that it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) doesn't need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.

The IEEE 802.1X standard defines a client-server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port before making available any services offered by the switch or the LAN.

Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL)traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

This switch supports 802.1X port-based authentication. In this page, user can configure 802.1X. After click "Security Configure" > "802.1X", the following screen will appear.

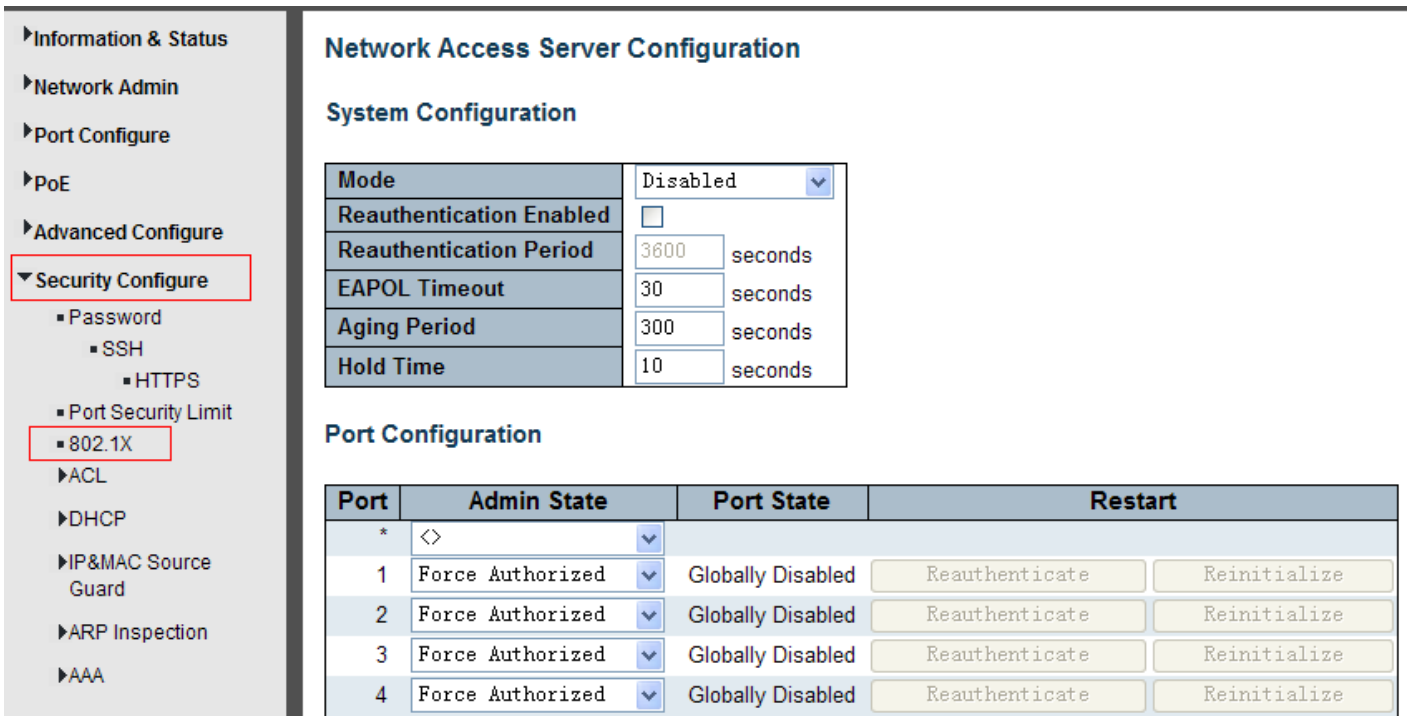


Figure 7-2 802.1X Configuration Screen

Configuration object and description is:

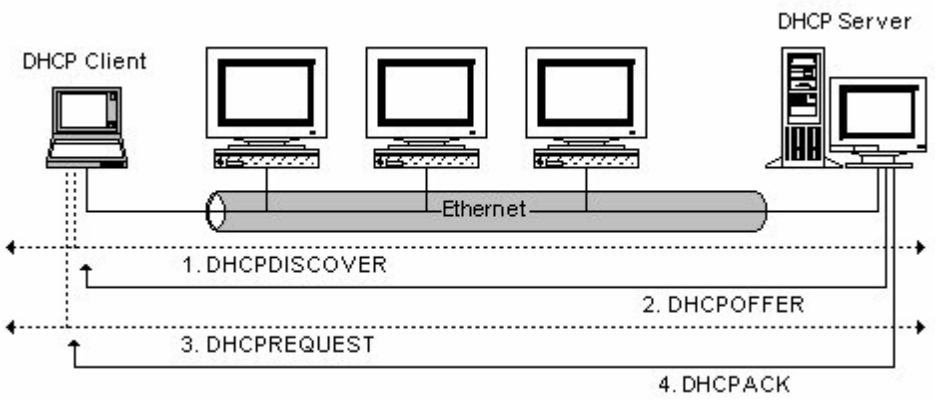
Object	Description
System Configuration	Here, user can enable or disable 802.1X or Reauthentication, as well as set Reauthentication Period / EAPOL Timeout / Aging Period / Hold Time
Port Configuration	Click drop-down menu to select a Admin State. Available options: Force Authorized, Force Unauthorized, 802.1X, Mac-based Auth.

Click "Save" to store and active settings.

7.3 DHCP Snooping

7.3.1 DHCP Overview

DHCP protocol is widely used to dynamically allocate reusable network resources, such as IP address. A typical process of DHCP to obtain IP is as the following:



DHCP Client sent DHCP DISCOVER message to DHCP Server, if Client did not receive respond from server within a period of time, it will resend DHCP DISCOVER message.
After received DHCP DISCOVER message, DHCP Server will assign sources (IP address for example) to client, and then send DHCP OFFER message to DHCP Client.

After received DHCP OFFER message, DHCP Client send DHCP REQUEST to ask for server lease, and notify the other servers that it has accepted this server to assign addresses.

After received DHCP REQUEST, server will verify whether resource can be allocated. If OK, it will send DHCP ACK message; If not OK, it will send DHCP NAK message. After received DHCP ACK message, start using the source which server assigned. If received DHCP NAK, DHCP Client will resend DHCP DISCOVER message.

7.3.2 About DHCP Snooping

The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping. DHCP snooping allows a switch to protect a network from rogue DHCP servers or other devices which send port-related information to a DHCP server. This information can be useful in tracking an IP address back to a physical port.

Command Usage

- Network traffic may be disrupted when malicious DHCP messages are received from an outside source. DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall When DHCP snooping is enabled globally and enabled on a VLAN interface, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped
- Table entries are only learned for trusted interfaces. An entry is added or removed dynamically to the DHCP snooping table when a client receives or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.
- When DHCP snooping is enabled, DHCP messages entering an untrusted interface are filtered based upon dynamic entries learned via DHCP snooping.
- If a DHCP packet from a client passes the filtering criteria, it will only be forwarded to trusted ports in the same VLAN
- If a DHCP packet is from server is received on a trusted port, it will be forwarded to both trusted and untrusted ports in the same VLAN.
- If the DHCP snooping is globally disabled, all dynamic bindings are removed from the binding table.

7.3.3 DHCP Snooping Configure

After click "Security Configure" > "DHCP " > "Snooping Setting", the following screen will appear.

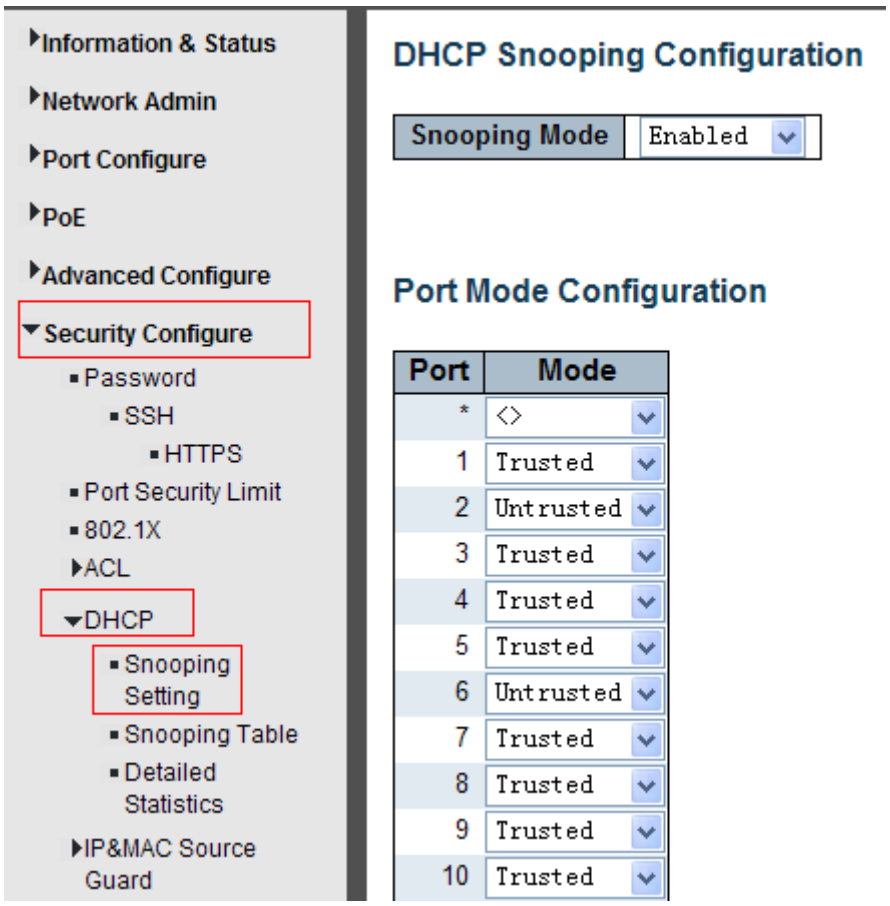


Figure 7-3 DHCP Snooping Configuration Screen

Configuration object and description is:

Object	Description
DHCP Snooping Mode	Click drop-down menu to enable or disable DHCP Snooping
Port Mode	Indicates the DHCP snooping port mode. Possible port modes are: Trusted: Configures the port as trusted source of the DHCP messages. Untrusted: Configures the port as untrusted source of the DHCP messages.

Click "Save" to store and active settings.

7.4 IP&MAC Source Guard

IP&MAC Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

7.4.1 Port Configuration

In this page, user can make IP&MAC Source Guard Port Configuration. After click "Security Configure">"IP & MAC Source Guard" >"Configuration", the following screen will appear.

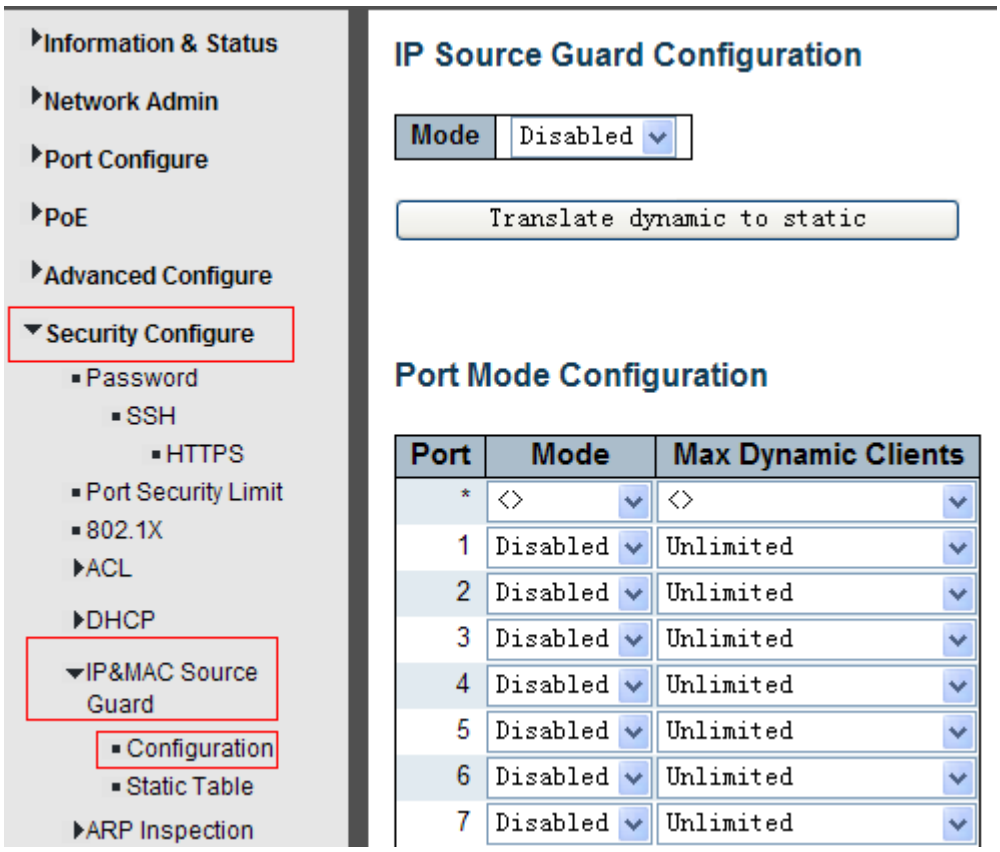


Figure 7-4 IP&MAC Guard- Port Configuration Screen

Configuration object and description is:

Object	Description
Global Mode	Click drop-down menu to enable or disable Global IP&MAC Source Guard function
Port Mode	Click drop-down menu to enable or disable the IP&MAC Source Guard function for corresponding port.
Max Dynamic Clients	Click drop-down menu to select Max Dynamic Clients. Available options: Unlimited, 0, 1, 2.

Click "Save" to store and active settings.

7.4.2 Static Table

In this page, user can manually set Static Table of IP&MAC Guard to fulfill controlling function to port. After click "Security Configure">"IP&MAC Source Guard" >"Static Table", the following screen will appear.

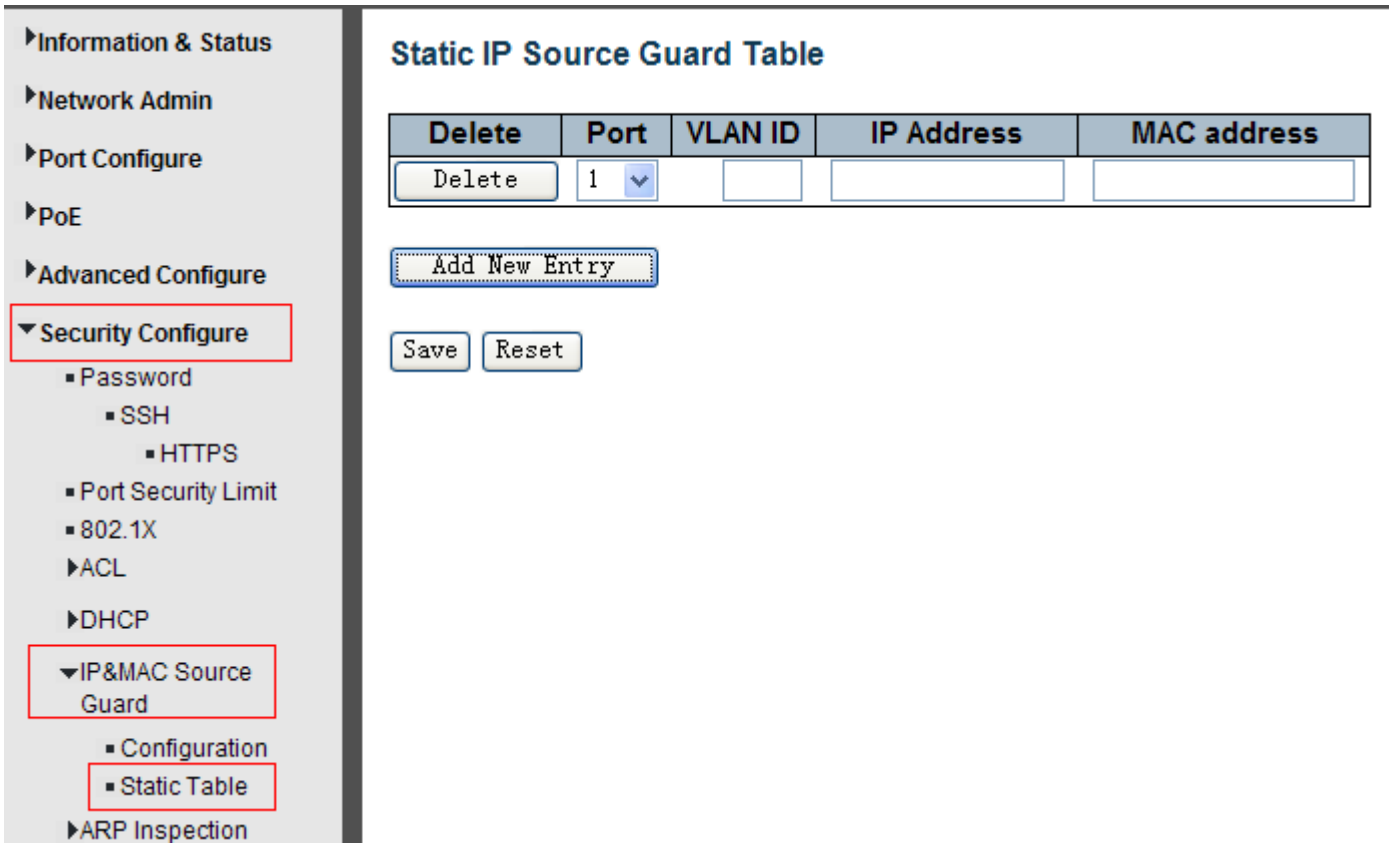


Figure 7-5 Static Table Configuration Screen

Configuration object and description is:

Object	Description
Port	Click drop-down menu to select which port should be fixed.
VLAN	Type VLAN ID that should be fixed to
IP Address	Type IP Address that should be fixed to
MAC Address	Type Mac Address that should be fixed to

Click "Add New Entry" button to create a new record.

Click "Save" to store and active settings.

7.5 ARP Inspection

Dynamic ARP Inspection (DAI) is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT. A Dynamic ARP prevents the untrust ARP packets based on the DHCP Snooping Database. This page provides ARP Inspection related configuration.

7.5.1 Port Configuration

User can make port configuration in this page. After click "Security Configure">"ARP Inspection" >"Port Configuration", the following screen will appear.

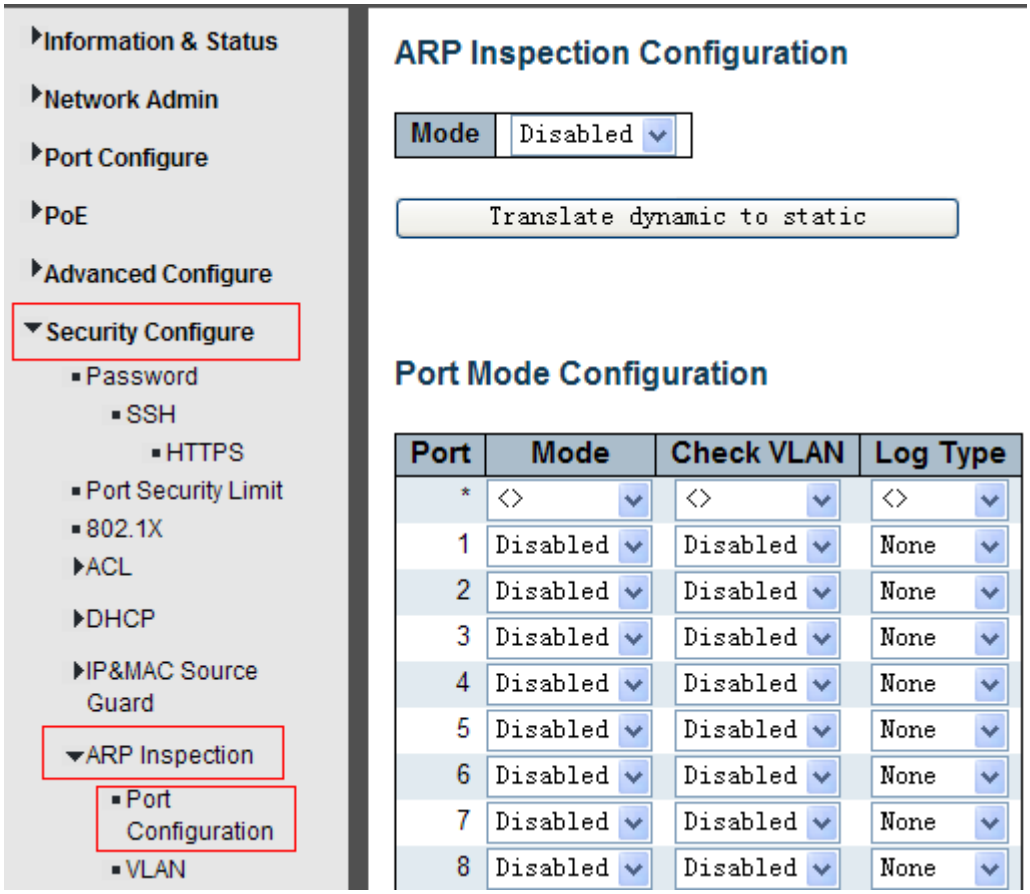


Figure 7-6 ARP Inspection Port Configuration Screen

Configuration object and description is:

Object	Description
Global Mode	Click drop-down menu to enable or disable Global ARP Inspection
Port Mode	Click drop-down menu to enable or disable port-based ARP Inspection
Check VLAN	If you want to inspect the VLAN configuration, you have to enable the setting of "Check VLAN". The default setting of "Check VLAN" is disabled. When the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. And the setting of "Check VLAN" is enabled, the log type of ARP Inspection will refer to the VLAN setting. Possible setting of "Check VLAN" are: Enabled: Enable check VLAN operation. Disabled: Disable check VLAN operation.
Log Type	Only the Global Mode and Port Mode on a given port are enabled, and the setting of "Check VLAN" is disabled, the log type of ARP Inspection will refer to the port setting. There are four log types and possible types: None: Log nothing. Deny: Log denied entries. Permit: Log permitted entries. ALL: Log all entries.

Click "Save" to store and active settings.

7.5.2 VLAN Configuration

After click "Security Configure">"ARP Inspection" >"VLAN Configuration", the following screen will appear.

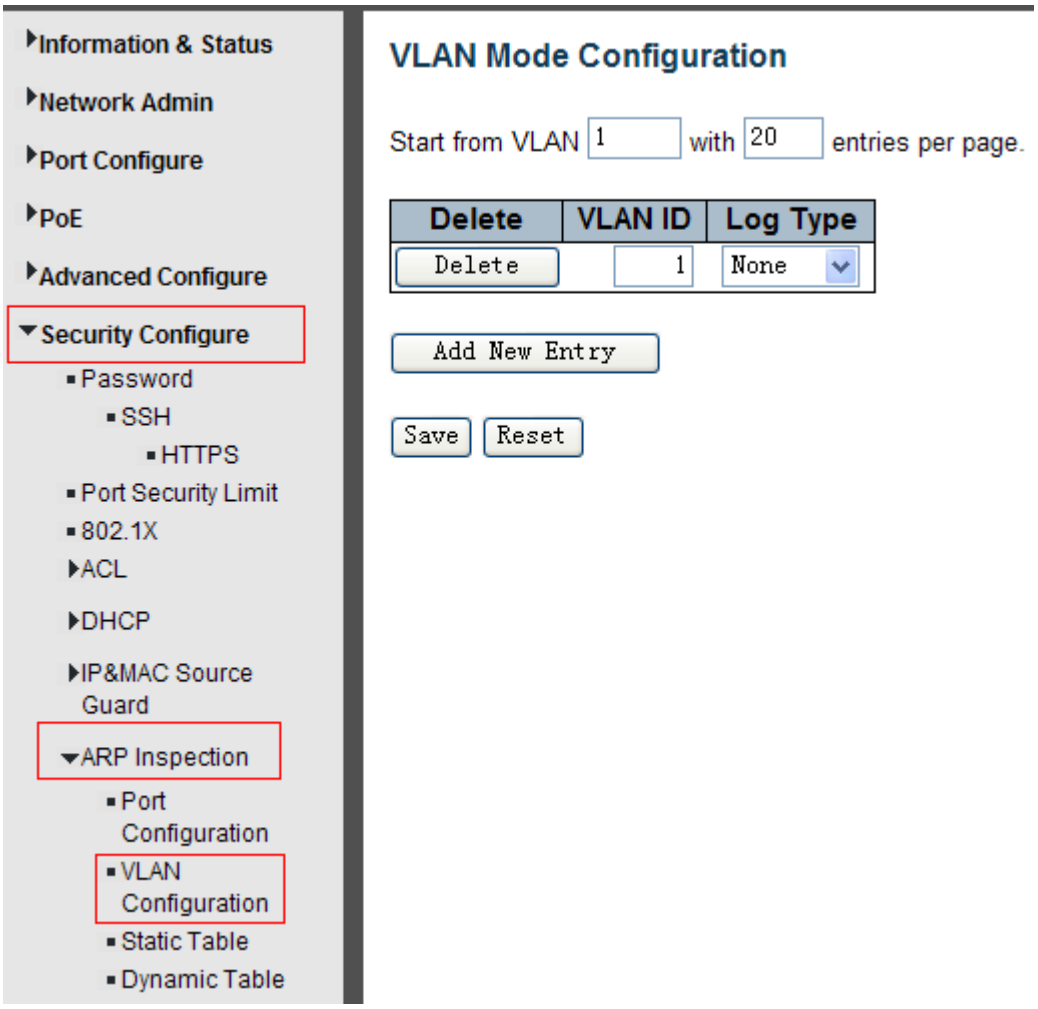


Figure 7-8 ARP Inspection VLAN Configuration Screen

Configuration object and description is:

Object	Description
VLAN ID	Indicates the ID of this particular VLAN
Log Type	Click drop-down menu to enable or disable port-based ARP Inspection. Specify ARP Inspection is enabled on which VLANs. First, you have to enable the port setting on Port mode configuration web page. Only when both Global Mode and Port Mode on a given port are enabled, ARP Inspection is enabled on this given port. Second, you can specify which VLAN will be inspected on VLAN mode configuration web page. The log type also can be configured on per VLAN setting. Possible types are: None: Log nothing. Deny: Log denied entries. Permit: Log permitted entries. ALL: Log all entries.

Click "Add New Entry" button to create a new record of VLAN configuration. Click "Save" to store and active settings.

7.5.3 Static Table

User can manually configure ARP Inspection Static Table to control port. After click "Security Configure">"ARP Inspection" >"Static Table", the following screen will appear.

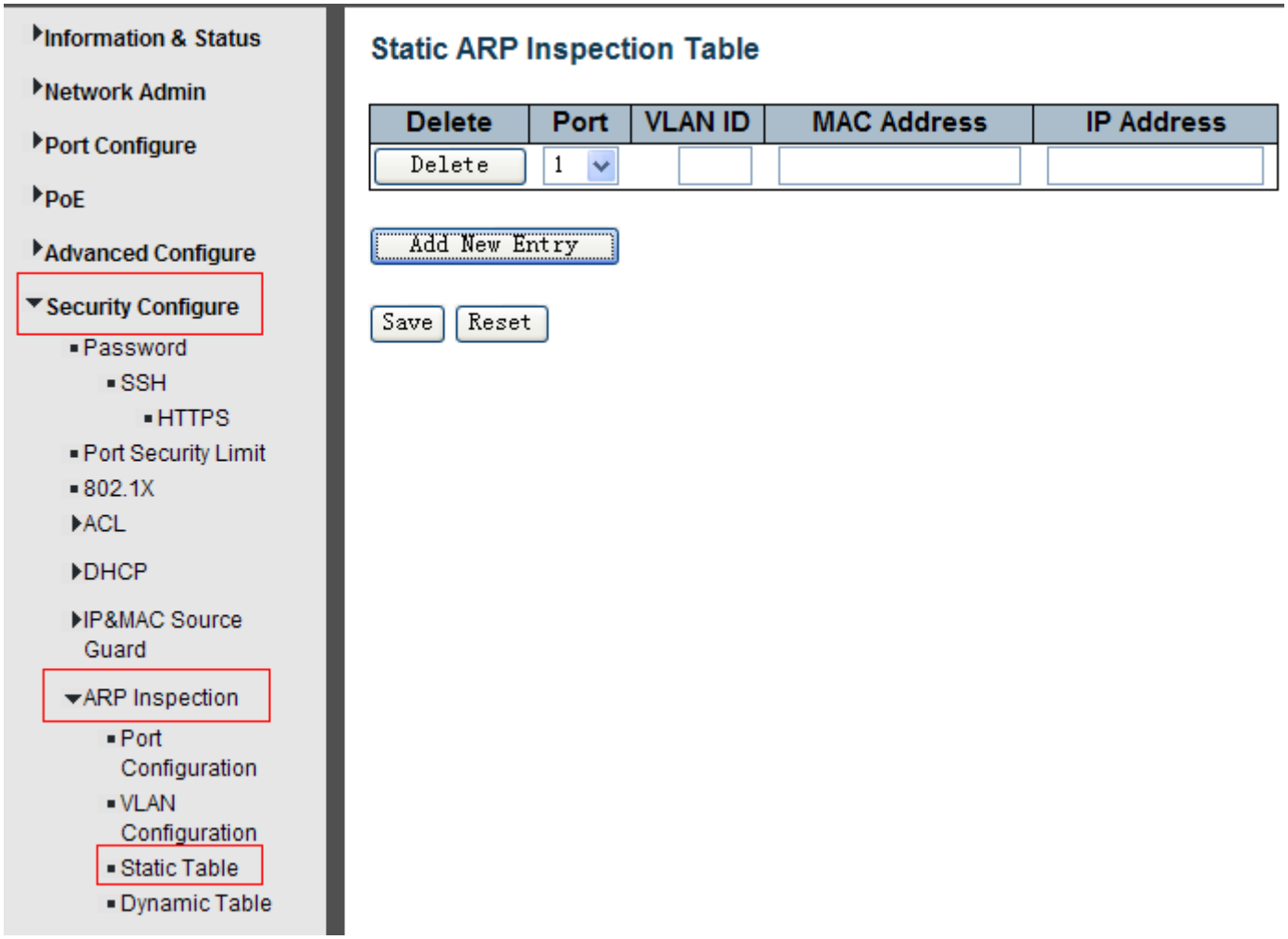


Figure 7-9 Static Table Configuration Screen

Configuration object and description is:

Object	Description
Port	Click drop-down menu to select which port should be fixed.
VLAN	Type VLAN ID that should be fixed to
IP Address	Type IP Address that should be fixed to
MAC Address	Type Mac Address that should be fixed to

Click "Add New Entry" button to create a new record. Click "Save" to store and active settings.

7.6 ACL

ACL is an acronym for **Access Control List**. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

7.6.1 ACL Ports Configure

After click "Security Configure">"ACL" >"Ports", the following screen will appear.

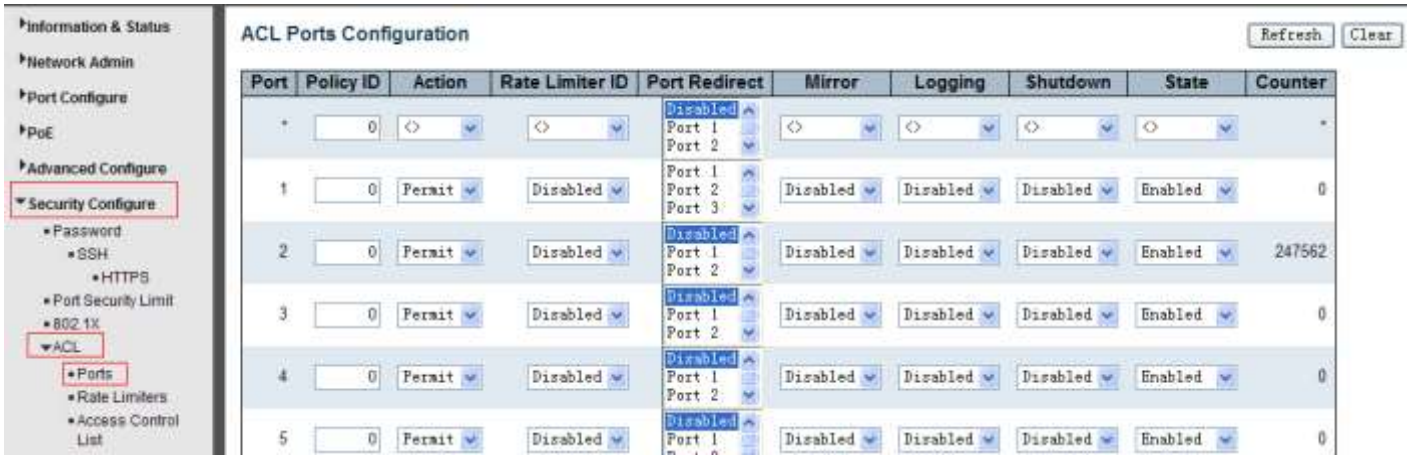


Figure 7-10 ACL Ports Configuration Screen

Configuration object and description is:

Object	Description
Action	There are 2 available options: Permit: that specific port allows data going through. Deny: that specific port forbid data going through.
Rate Limiter ID	Port's fixed Rate Limiter ID, please go to Rate Limiter Configuration for more details.
Port Redirect	Select which port frames are redirected on. The allowed values are Disabled or a specific port number and it can't be set when action is permitted. The default value is "Disabled".
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Enabled or Disabled Log
Shut Down	Specify the port shut down operation of this port. The allowed values are: Enabled: If a frame is received on the port, the port will be disabled. Disabled: Port shut down is disabled. The default value is "Disabled". Note: The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

State	Specify the port state of this port. The allowed values are: Enabled: To reopen ports by changing the volatile port configuration of the ACL user module. Disabled: To close ports by changing the volatile port configuration of the ACL user module. The default value is "Enabled".
Counter	Counts the number of frames that match this rule.

Click "Save" to store and active settings.

7.6.2 Rate Limiter Configuration

User can make ACL Rate limiter configuration in this page. After click "Security Configure">"ACL" >"Rate Limiter", the following screen will appear.

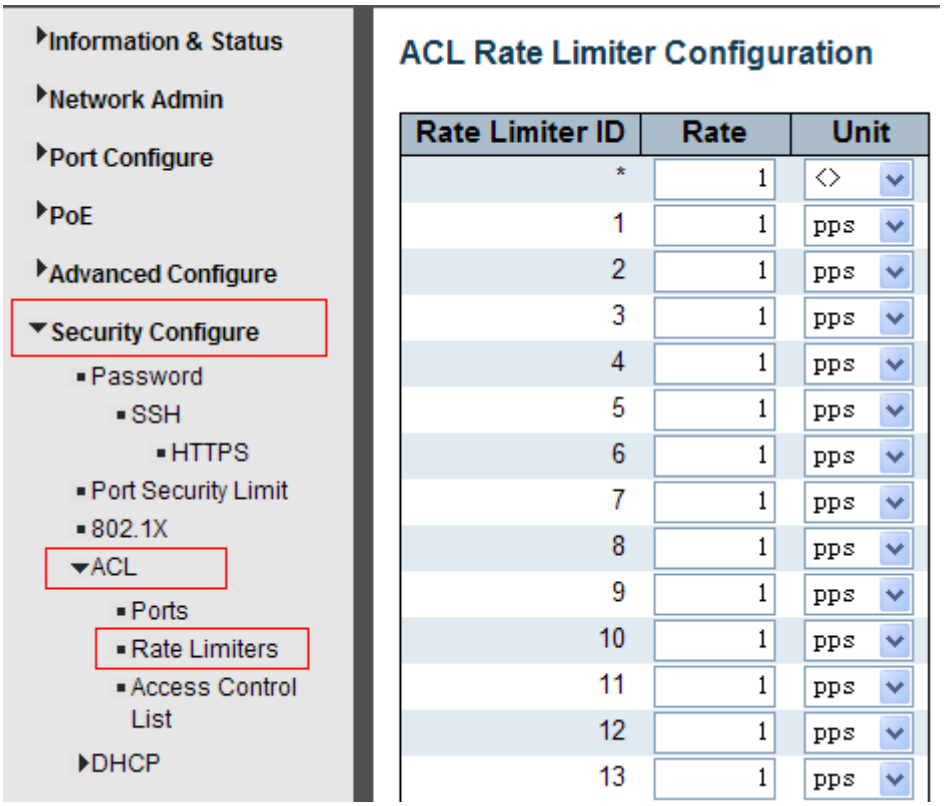


Figure 7-11 ACL Rate Limiters Configuration Screen

Click "Save" to store and active settings.

7.6.3 Access Control List Configuration

User can make Access Control List Configuration in this page . After click "Security Configure" > "ACL" >"Access Control List", the following screen will appear.

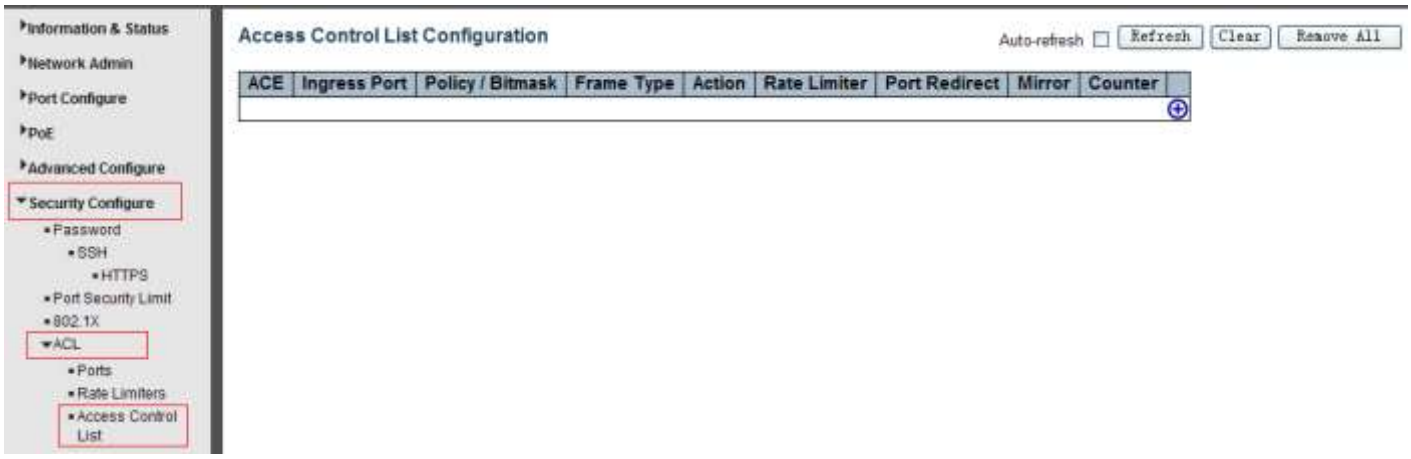


Figure 7-12 Access Control List Configuration Screen

Click ⊕ button, to go to Access Control List, and edit it.

8. Diagnostics

8.1 Ping Test

Ping is a well known software program that can issue ICMP Echo packets to an IP address you defined, e.g., xxx.xxx.xxx.xxx. The destination node IP address will respond to those packets sent from the Ping command. So Ping test is to troubleshoot IP connectivity issues.

After click "Diagnostics ">"Ping", the following screen appear.

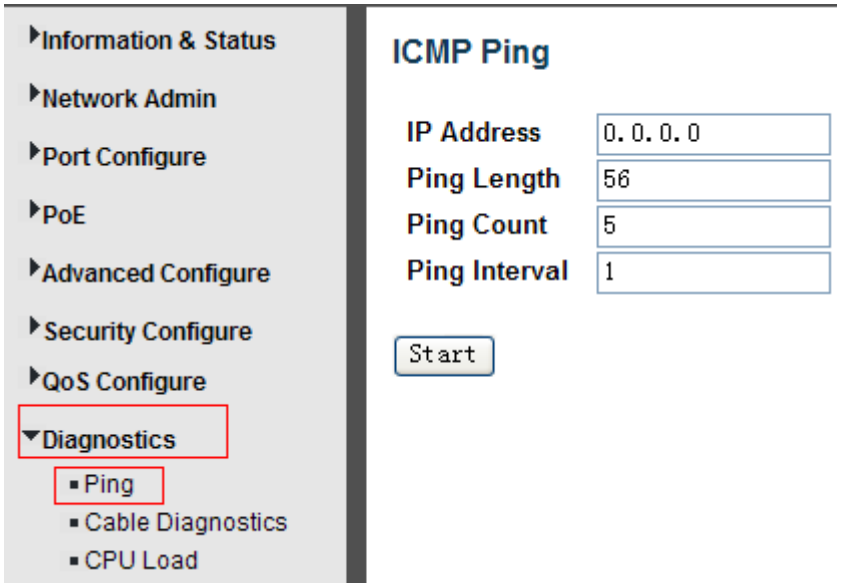


Figure 8-1 Ping Test Screen

Configuration object and description is:

Object	Description
IP Address	The destination IP Address that needed to Ping
Ping Length	Input a number between 1 and 1452. Default: 56
Ping Count	The times for inputting Ping IPv4 address or IPv6 address (Number of echo requests to send). User can input a number between 1 and 60.
Ping Interval	Interval time for Ping (Send interval for each ICMP packet)

Click "Start" button to start Ping testing.

8.2 Cable Diagnostics

The Cable Diagnostics performs tests on 10/100/1000BASE-T copper cables. These functions have the ability to identify the cable length and operating conditions, and to isolate a variety of common faults that can occur on a CAT5 twisted-pair cabling.

After click "Diagnostics ">"Cable Diagnostics", the following screen will appear.

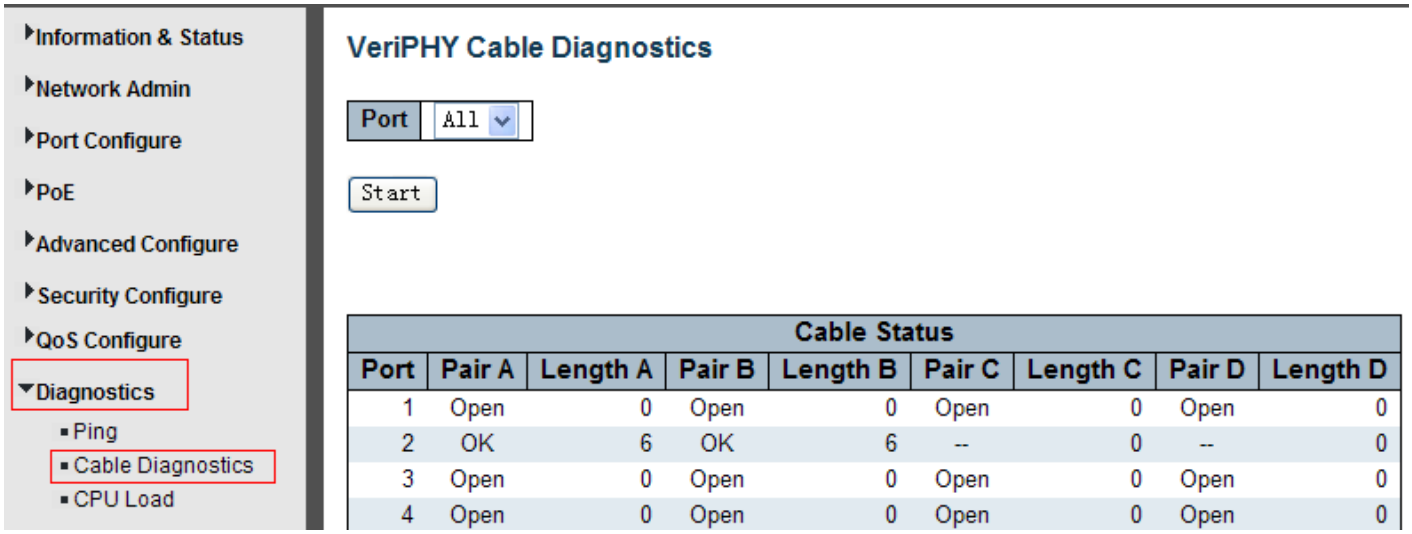


Figure 8-2 Cable Diagnostics Screen

Click "Start" button to start ''Cable Diagnostics'' testing.

8.3 CPU Load

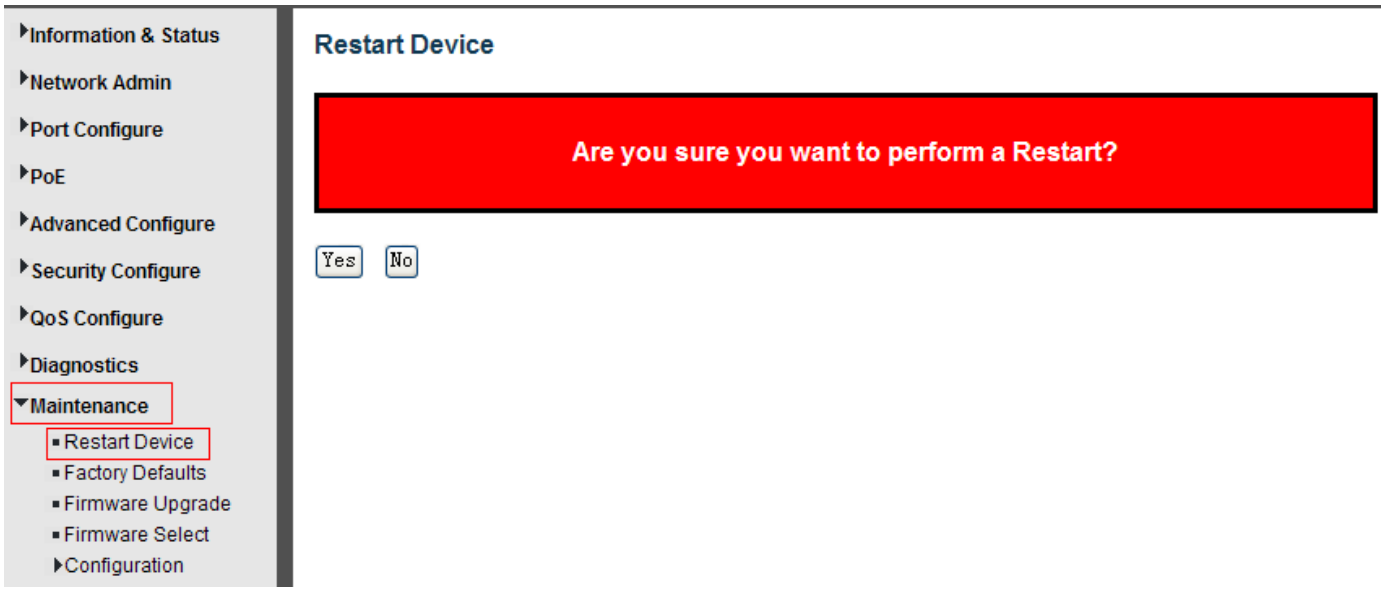
This function shows the percent of CPU load. After click "Diagnostics" > "CPU Load", the following screen will appear.

Figure 8-3 CPU Load Screen

9. Maintenance

9.1 Restart Device

This page is for restarting switch. After click "Maintenance ">"Restart Device", the following screen will appear.



Please click "Yes" to restart the switch.

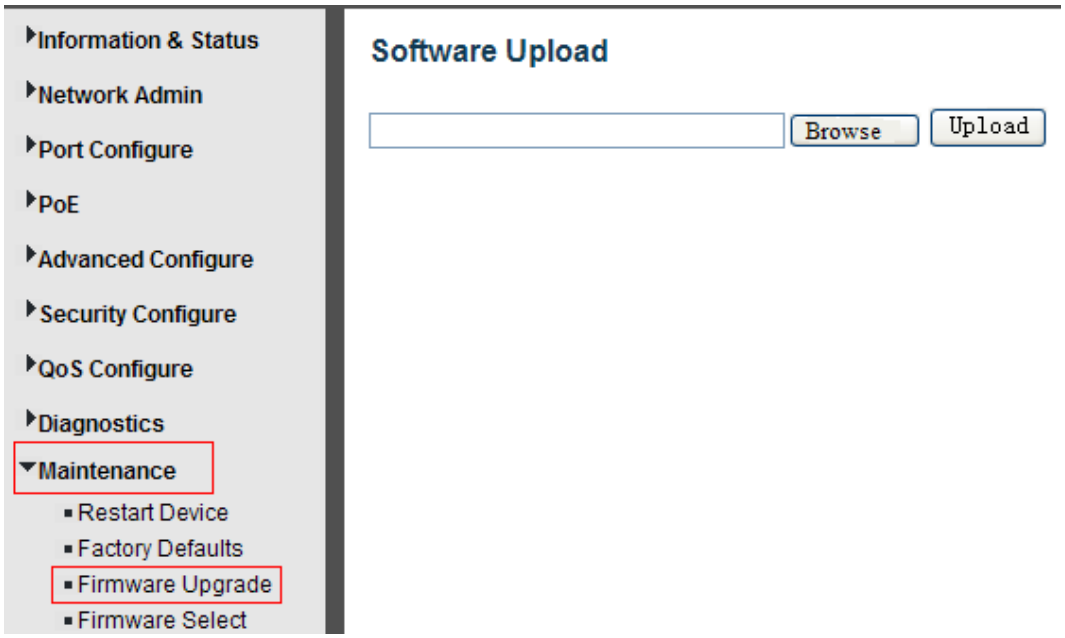
9.2 Factory Defaults

This page is for making all settings to factory defaults. After click "Maintenance ">"Factory Defaults", the following screen will appear.

Please click "Yes" to reset the configuration to Factory Defaults.

9.3 Firmware Upgrade

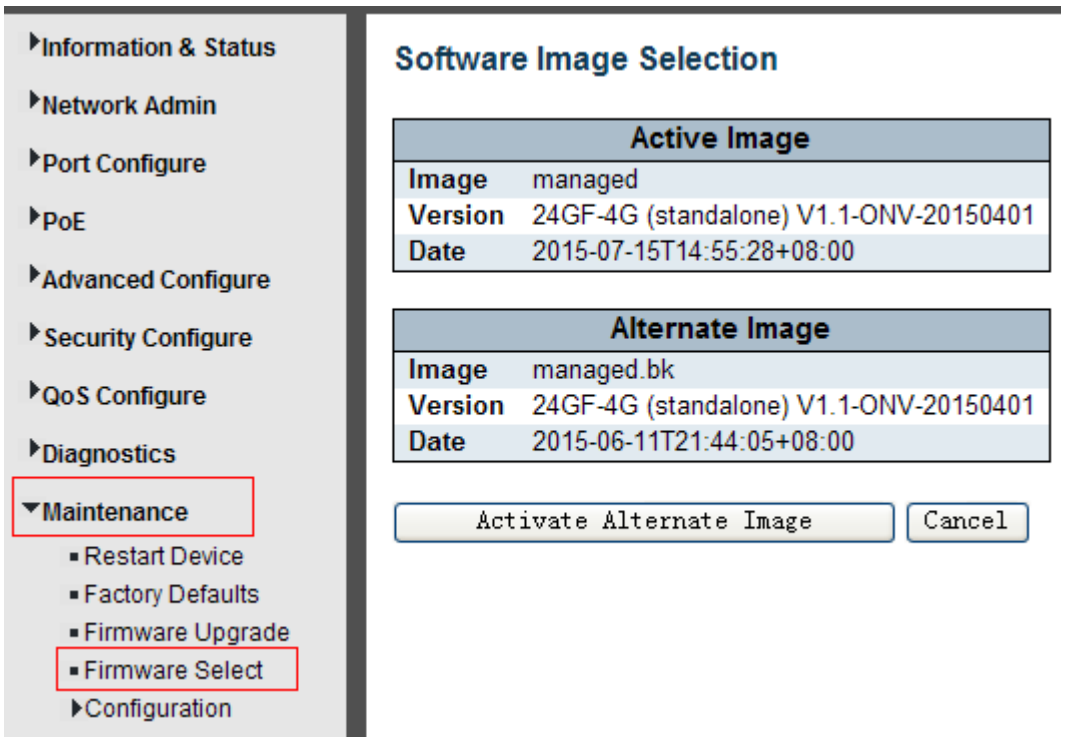
This page is for upgrading system firmware. After click "Maintenance ">"Firmware Upgrade", the following screen will appear.



Please click "Browse" to select the firmware that needed to upgrade. And then click "Upload " to start upgrading.

9.4 Firmware Select

This page is for upgrading system firmware. After click "Maintenance ">"Firmware Upgrade", the following screen will appear.



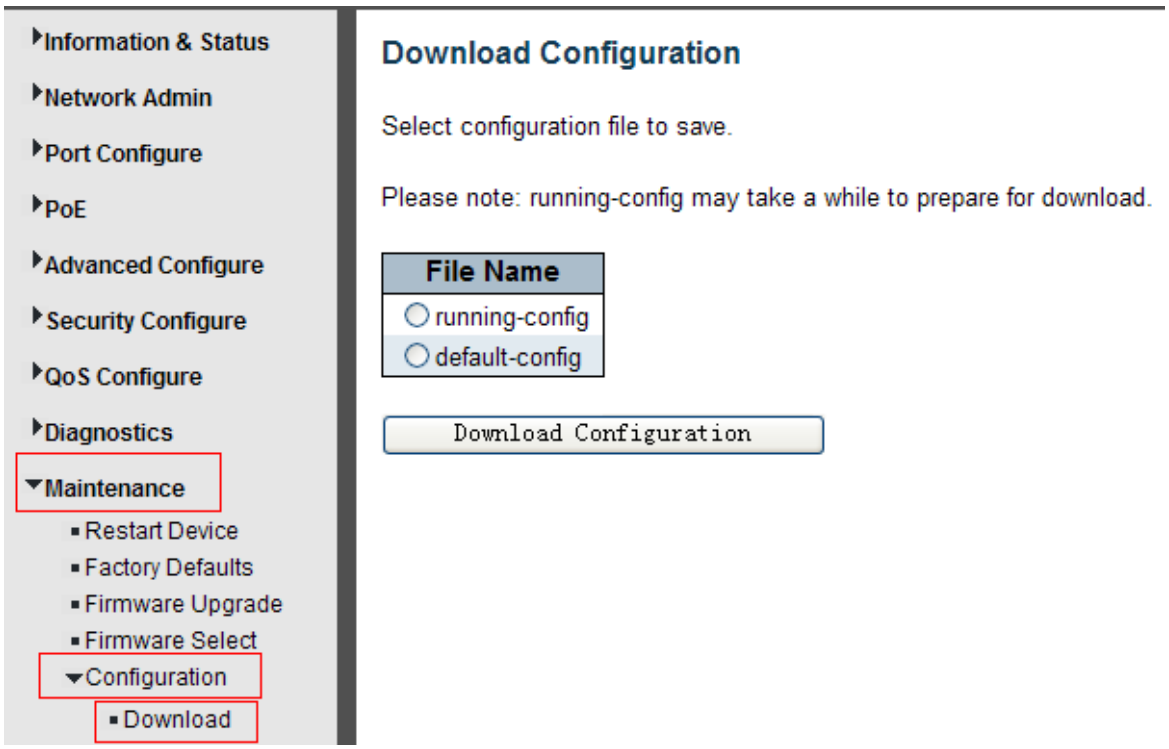
Please click "Activate Alternate Image" to select the firmware.

9.5 Firmware Select

In this page, user can download, upload, activated or delete configuration files.

9.5.1 Download Configuration File

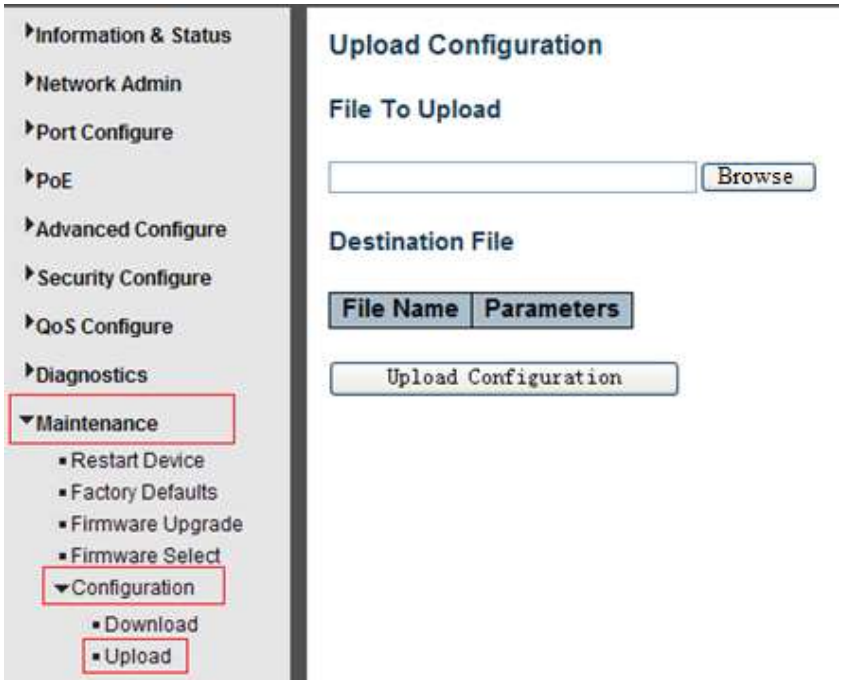
After click "Maintenance ">"Download", the following screen will appear.



Please choose a file and then click "Download Configuration" button to download.

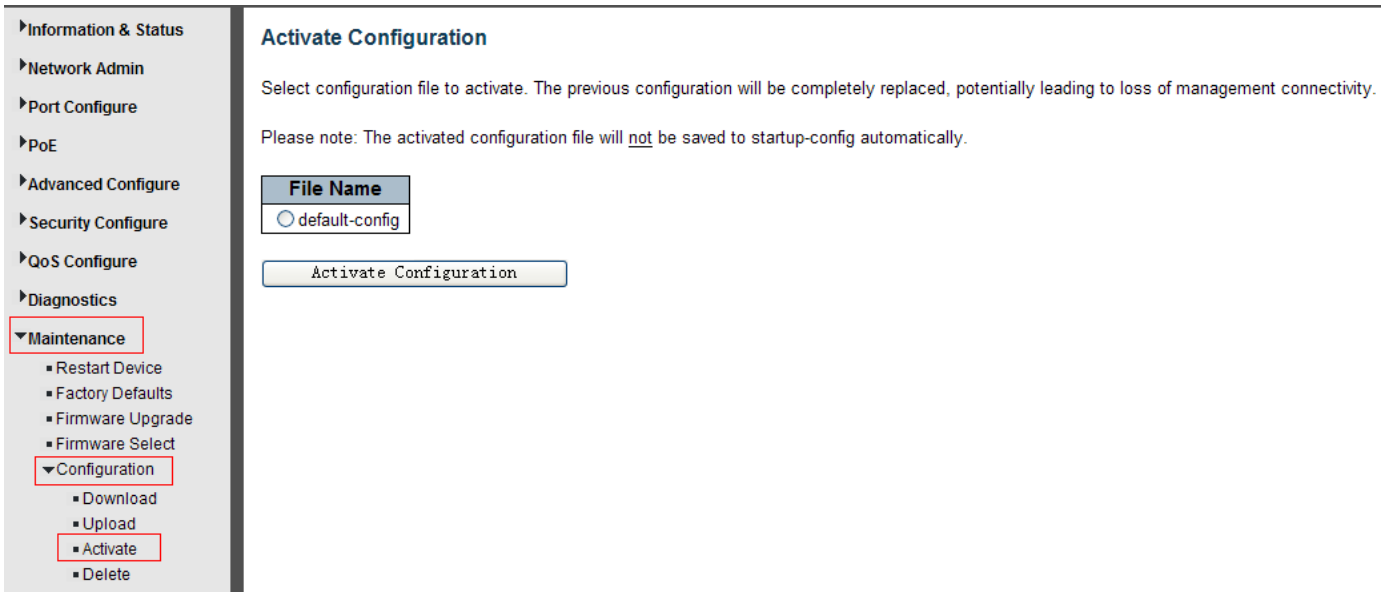
9.5.2 Upload Configuration File

After click "Maintenance " > "Upload", the following screen will appear. Then user can upload Configuration File.



9.5.3 Activate Configuration

After click "Maintenance " > "Activate", the following screen will appear. Then user can activate Configuration File.



9.5.4 Delete Configuration File

After click "Maintenance " > "Delete", the following screen will appear. Then user can delete Configuration File.