

EVIDENCE®

User`s Manual



Cross-8/SP

Cross-8/SP

User's Manual

Industrial 8-Port L2+ Managed Fast Ethernet Switch
+ 2 TP/SFP Gigabit Dual Media

Release 5.32

The information in this document is subject to change without notice. Unless the explicit written permission of ManufactureTech Corporation, this document in whole or in part shall not be replicated or modified or amended or transmitted, in any form, or by any means manual, electric, electronic, electromagnetic, mechanical, optical or otherwise for any purpose.

DURATION OF HARDWARE WARRANTY

HARDWARE: In accordance with the provisions described under, ManufactureTech Corporation (hereinafter called "ManufactureTech") warrants its hardware products (hereinafter referred to as "Product") specified.

Should a Product fail to perform during the effective warranty period as described above, ManufactureTech shall replace the defective Product or part, or delivering a functionally equivalent Product or part in receipt of customer's request, provided that the customer complies with the return material authorization (RMA) procedures and returns all defective Product prior to installation of the replacements to ManufactureTech.

All defective Products must be returned to ManufactureTech with issuance of a Return Material Authorization number (RMA number) assigned to the reseller from whom the end customer originally purchased the Product. The reseller is responsible for ensuring the shipments are insured, with the transportation charges prepaid and the RMA number clearly marked on the outside of the package. ManufactureTech will not accept collect shipments or those returned without an RMA number.

ManufactureTech shall not be responsible for any software, firmware, information or memory data contained in, stored on or integrated with any Product returned to ManufactureTech pursuant to any warranty.

EXCLUSIONS. The warranty as mentioned above does not apply to the following conditions, in ManufactureTech's judgment, it contains (1) customer does not comply with the manual instructions offered by ManufactureTech in installation, operation, repair or maintenance, (2) Product fails due to damage from unusual external or electrical stress, shipment, storage, accident, abuse or misuse, (3) Product is used in an extra hazardous environment or activities, (4) any serial number on the Product has been removed or defaced, (5) this warranty will be of no effect if the repair is via anyone other than ManufactureTech or the approved agents, or (6) In the event of any failures or delays by either party hereto in the performance of all or any part of this agreement due to acts of God, war, riot, insurrection, national emergency, strike, embargo, storm, earthquake, or other natural forces, or by the acts of anyone not a party to this agreement, or by the inability to secure materials or transportation, when the party so affected shall be executed from any further performance for a period of time after the occurrence as may reasonably be necessary to remedy the effects of that occurrence, but in no event more than sixty (60) days. If any of the stated events should occur, Party A shall promptly notify Party B in writing as soon as commercially practicable, but in no event more than twenty (20) business days and provide documentation evidencing such occurrence. In no event shall the maximum liability of ManufactureTech under this warranty exceed the purchase price of the Product covered by this warranty.

DISCLAIMER. EXCEPT AS SPECIFICALLY PROVIDED ABOVE AS REQUIRED "AS IS" AND THE WARRANTIES AND REMEDIES STATED ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHERS, ORAL OR WRITTEN, EXPRESS OR IMPLIED. ANY AND ALL OTHER WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR THIRD PARTY RIGHTS ARE EXPRESSLY EXCLUDED.

MANUFACTURETECH SOFTWARE LICENSE AGREEMENT

NOTICE: Please carefully read this Software License Agreement (hereinafter referred to as this "Agreement") before copying or using the accompanying software or installing the hardware unit with pre-enabled software or firmware (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE PROVISIONS AND CONDITIONS OF THIS AGREEMENT. THE PROVISIONS EXPRESSED IN THIS AGREEMENT ARE THE ONLY PROVISION UNDER WHICH MANUFACTURETECH WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these provisions and conditions, please immediately return the unused software, manual and the related product. Written approval is NOT a prerequisite to the validity or enforceability of this Agreement and no solicitation of any such written approval by or on behalf of ManufactureTech shall be deemed as an inference to the contrary.

LICENSE GRANT. The end user (hereinafter referred to as "Licensee") of the Software is granted a personal, non-sublicensable, nonexclusive, nontransferable license by ManufactureTech Corporation ("ManufactureTech"): (1) To use the ManufactureTech's software ("Software") in object code form solely on a single central processing unit owned or leased by Licensee or otherwise embedded in the equipment offered by ManufactureTech. (2) To copy the Software only for backup purposes in support of authorized use of the Software. (3) To use and copy the documentation related to the Software solely in support of authorized use of the Software by Licensee. The License applies to the Software only except other ManufactureTech's software or hardware products. Without the prior written consent of ManufactureTech, Licensee has no right to receive any source code or design documentation with respect to the Software.

RESTRICTIONS ON USE; RESERVATION OF RIGHTS. The Software and related documentation are protected under copyright laws. ManufactureTech and/or its licensors retain all title and ownership in both the Software and its related documentation, including any revisions made by ManufactureTech. The copyright notice must be reproduced and included with any copy of any portion of the Software or related documentation. Except as expressly authorized above, Licensee shall not copy or transfer the Software or related documentation, in whole or in part. Licensee also shall not modify, translate, decompile, disassemble, use for any competitive analysis, reverse compile or reverse assemble all or any portion of the Software, related documentation or any copy. The Software and related documentation embody ManufactureTech's confidential and proprietary intellectual property. Licensee is not allowed to disclose the Software, or any information about the operation, design, performance or implementation of the Software and related documentation that is confidential to ManufactureTech to any third party. Software and related documentation may be delivered to you subject to export authorization required by governments of Taiwan and other countries. You agree that you will not export or re-export any Software or related documentation without the proper export licenses required by the governments of affected countries.

LIMITED SOFTWARE WARRANTY. ManufactureTech warrants that any media on which the Software is recorded will be free from defects in materials under normal use for a period of twelve (12) months from date of shipment. If a defect in any such media should occur during the effective warranty period, the media may be returned to ManufactureTech, then ManufactureTech will replace the media. ManufactureTech shall not be responsible for the replacement of media if the failure of the media results from accident, abuse or misapplication of the media.

EXCLUSIONS. The warranty as mentioned above does not apply to the Software, which (1) customer does not comply with the manual instructions offered by ManufactureTech in installation, operation, or maintenance, (2) Product fails due to damage from unusual external or electrical stress, shipment, storage, accident, abuse or misuse, (3) Product is used in an extra hazardous environment or activities, (4) any serial number on the Product has been removed or defaced, or (5) this warranty will be of no effect if the repair is via anyone other than ManufactureTech or the authorized agents. The maximum liability of ManufactureTech under this warranty is confined to the purchase price of the Product covered by this warranty.

DISCLAIMER. EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS " AND MANUFACTURETECH AND ITS LICENSORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION. MANUFACTURETECH AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES, INCLUSIVE OF WITHOUT LIMITATION, IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. FURTHER, MANUFACTURETECH DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR RELATED WRITTEN DOCUMENTATION IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

CONSEQUENTIAL DAMAGES. IN NO EVENT SHALL MANUFACTURETECH OR ITS AUTHORIZED RESELLER BE LIABLE TO LICENSEE OR ANY THIRD PARTY FOR (A) ANY MATTER BEYOND ITS REASONABLE CONTROL OR (B) ANY CONSEQUENTIAL, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES ARISING OUT OF THIS LICENSE OR USE OF THE SOFTWARE PROVIDED BY MANUFACTURETECH. EVEN IF MANUFACTURETECH HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. IN NO EVENT SHALL THE LIABILITY OF MANUFACTURETECH IN CONNECTION WITH THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO MANUFACTURETECH FOR THE LICENSE.

TERM AND TERMINATION. The License is effective until terminated; however, all of the restrictions in regard to ManufactureTech's copyright in the Software and related documentation will cease being effective at the date of expiration; Notwithstanding the termination or expiration of the term of this agreement, it is acknowledged and agreed that those obligations relating to use and disclosure of ManufactureTech's confidential information shall survive. Licensee may terminate this License at any time by destroying the software together with all copies thereof. This License will be immediately terminated if Licensee fails to comply with any term and condition of the Agreement. Upon any termination of this License for any reason, Licensee shall discontinue to use the Software and shall destroy or return all copies of the Software and the related documentation.

GENERAL. This License shall be governed by and construed pursuant to the laws of Taiwan. If any portion hereof is held to be invalid or unenforceable, the remaining provisions of this License shall remain in full force and effect. Neither the License nor this Agreement is assignable or transferable by Licensee without ManufactureTech's prior written consent; any attempt to do so shall be void. This License constitutes the entire License between the parties with respect to the use of the Software.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN MANUFACTURETECH AND LICENSEE.

Table of Contents

Caution.....	ix
Electronic Emission Notices.....	ix
Warning:.....	x
1. Introduction.....	2
1-1. Overview of Cross-8/SP.....	2
1-2. Checklist.....	5
1-3. Features.....	5
1-4. View of Cross-8/SP.....	7
1-4-1. User Interfaces on the Front Panel.....	7
1-5. View of the Optional Modules.....	9
2. Installation.....	10
2-1. Starting Cross-8/SP.....	10
2-1-1. Hardware and Cable Installation.....	10
2-1-2. DIN-Rail Mounting Installation.....	14
2-1-2-1. Wall Mounting Installation.....	14
2-1-3. Cabling Requirements.....	15
2-1-3-1. Cabling Requirements for TP Ports.....	15
2-1-3-2. Cabling Requirements for 1000SX/LX SFP Module.....	15
2-1-3-3. Switch Cascading in Topology.....	16
2-1-4. Configuring the Management Agent of Cross-8/SP.....	19
2-1-4-1. Configuring the Management Agent of Cross-8/SP through the Serial RS-232 Port.....	19
2-1-5. IP Address Assignment.....	21
2-2. Typical Applications.....	26
3. Operation of Web-based Management.....	28
3-1. Web Management Home Overview.....	29
3-1-1. System Information.....	31
3-1-2. IP Configuration.....	33
3-1-3. Time Configuration.....	35
3-1-4. Account Configuration.....	38
3-1-5. Management Security.....	39
3-1-6. Virtual Stack.....	42
3-1-7. R-Ring (Rapid-convergence Ring).....	44
3-2. DHCP Snooping.....	46
3-2-1. Config.....	46
3-2-2. Trust Group.....	48
3-2-3. Lease List.....	50
3-2-4. Counter.....	51
3-3. DHCP Relay.....	52

3-3-1. Config.....	52
3-4. IP-MAC Binding.....	54
3-4-1. State.....	54
3-4-2. Binding List.....	55
3-5. Port Configuration.....	57
3-5-1.Port Status.....	57
3-5-2. Port Configuration.....	61
3-5-3. Description.....	63
3-5-4. Simple Counter.....	64
3-5-5. Detail Counter.....	65
3-6. Loop Detection.....	68
3-7. SNMP Configuration.....	69
3-7-1. EngineID.....	69
3-7-2. SNMP Community.....	70
3-7-3. Users.....	71
3-7-4. Group.....	73
3-7-5. View.....	74
3-7-6. Access.....	75
3-7-7. Trap Host Config.....	76
3-8. DHCP Boot.....	78
3-9. Multicast.....	79
3-9-1. IGMP Mode.....	79
3-9-2. Proxy.....	80
3-9-3. Snooping.....	82
3-9-4. IGMP VLAN.....	83
3-9-5. Group Allow.....	85
3-9-6. Multicast Status.....	89
3-9-7. MVR Setting.....	90
3-9-8. MVR Group Allow.....	91
3-9-9. MVR Multicast Status.....	92
3-9-10. RADIUS IGMP.....	93
3-10. LLDP.....	95
3-10-1. LLDP Configuration.....	95
3-10-2. LLDP Neighbor Information.....	98
3-10-3. LLDP Statistics.....	99
3-11. VLAN.....	101
3-11-1. VLAN Mode.....	101
3-11-2. Tag-based Group.....	103
3-11-3. PVID.....	106
3-11-4. Port-based Group.....	108
3-11-5. Management VLAN.....	110
3-12. MAC Table.....	111
3-12-1. Information.....	111
3-12-2. Maintenance.....	113
3-12-3. Static.....	114
3-12-4. MAC Alias.....	116
3-12-5. Port Security.....	119
3-12-6. Port Static MAC.....	120
3-13. GVRP Configuration.....	122

3-13-1. Config.....	122
3-13-2. Counter.....	125
3-13-3. Group.....	127
3-14. STP Configuration.....	129
3-14-1. Status.....	129
3-14-2. Configuration.....	131
3-14-3. Port.....	133
3-15. MSTP.....	136
3-15-1. MSTP State.....	136
3-15-2. Region Config.....	137
3-15-3. Instance View.....	138
3-16. Trunk.....	149
3-16-1. Port.....	150
3-16-2. Aggregator View.....	152
3-16-3. LACP System Config.....	154
3-17. 802.1x Configuration.....	155
3-17-1. State.....	160
3-17-2. Mode.....	161
3-17-3. Security.....	162
3-18. TACACS+.....	165
3-18-1. State.....	165
3-18-2. Authentication.....	166
3-18-3. Authorization.....	167
3-18-4. Accounting.....	168
3-19. Alarm.....	169
3-19-1. Events.....	169
3-19-2. Email.....	171
3-19-3. Relay.....	172
3-20. Configuration.....	173
3-20-1. Save/Restore.....	174
3-20-2. Config File.....	177
3-21. Security.....	178
3-21-1. Mirror.....	178
3-21-2. Isolated Group.....	179
3-21-3. Arp Protect.....	180
3-21-3. Arp Protect.....	180
3-22. Bandwidth.....	181
3-22-1. Ingress.....	181
3-22-2. Egress.....	182
3-22-3. Storm.....	183
3-23. QoS.....	185
3-23-1. Global.....	185
3-23-2. 802.1p.....	186
3-23-3. DSCP.....	187
3-24. ACL.....	188
3-24-1. High-ACL List/Low-ACL List.....	188
3-25. Diagnostics.....	196
3-25-1. Diag.....	196

3-25-2. Loopback.....	197
3-25-3. Ping Test.....	198
3-25-4. Auto Ping.....	199
3-25-5. Cable.....	200
3-26. TFTP Server.....	201
3-27. SysLog.....	202
3-28. Log.....	203
3-29. Firmware Upgrade.....	205
3-30. Reboot.....	206
3-31. Logout.....	207
4. Operation of CLI Management.....	208
4-1. CLI Management.....	208
4-1-1. Login.....	208
4-2. Commands of CLI.....	209
4-2-1. Global Commands of CLI.....	211
4-2-2. Local Commands of CLI.....	217
5. Maintenance.....	349
5-1. Resolving No Link Condition.....	349
5-2. Q&A.....	349
Appendix A Technical Specifications.....	350
Appendix B Default Account.....	352
Appendix C Console Cable Specifications.....	353

Revision History

Release	Date	Revision
5.32	05/24/2011	B1

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
- Pick up the device by holding it on the left and right edges only.
- The switch supports the SFP Vendor includes Manufacturetech, Agilent, Avago and Finisa.
- The Web UI's Main Menu links are used to navigate to other menus, and display configuration parameters and statistics with suggestive value 1024x768.
- If you need using outdoor device connect to this device with cable then you need to add an arrester on the cable between outdoor device and this device.

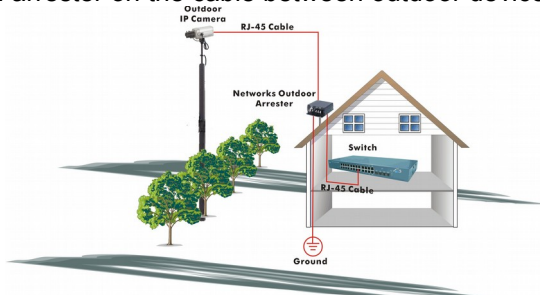


Fig. To add an arrester between outdoor device and this switch

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart B of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in an industrial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN61000-3 and the Generic European Immunity Standard EN55024.

EMI	EN55022:1998+A1:2000+A2:2003,Class A
	EN61000-3-2:2000
	EN61000-3-3:1995+A1:2001
EMS	EN55024/1998+A1:2001+A2:2003
	→IEC61000-4-2:2001
	→IEC61000-4-3:2002+A1:2002
	→IEC61000-4-4:1995+A1:2000+A2:2001
	→IEC61000-4-5:2001
	→IEC61000-4-6:2003
	→IEC61000-4-8:2001
	→IEC61000-4-11:2001

Warning:

- Self-demolition on Product is strictly prohibited. Damage caused by self-demolition will be charged for repairing fees.
- Do not place product at outdoor or sandstorm.
- Before installation, please make sure input power supply and product specifications are compatible to each other.
- Before importing / exporting configuration please make sure the firmware version is always the same.
- After firmware upgrade, the switch will remove the configuration automatically to latest firmware version.

About this user's manual

In this user's manual, it will not only tell you how to install and connect your network system but configure and monitor the Cross-8/SP through the RS-232 console port and Web UI step-by-step. Many explanations in detail of hardware and software functions are shown as well as the examples of the operation for web-based interface and command-line interface (CLI).

Overview of this user's manual

- Chapter 1 "Introduction" describes the features of Cross-8/SP
- Chapter 2 "Installation"
- Chapter 3 "Operation of Web-based Management"
- Chapter 4 "Operation of CLI Management"
- Chapter 5 "Maintenance"
- Appendix A "Technical Specifications"
- Appendix B "Default Account"

1. Introduction

1-1. Overview of Cross-8/SP

Cross-8/SP, 8 port Fast Ethernet +2 Gigabit L2 Plus Managed Switch, implemented 8 10/100Mbps TP + 2 Gigabit dual media ports with TP/SFP, is a standard switch that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet and Ethernet specifications. The switch can be managed through RS-232 serial console port via directly connection, or through Ethernet port using Telnet or Web-based management unit, associated with SNMP agent. With the SNMP agent, the network administrator can logon the switch to monitor, configure and control each port's activity in a friendly way. The overall network management is enhanced and the network efficiency is also improved to accommodate high bandwidth applications. In addition, the switch features comprehensive and useful function such as QoS (Quality of Service), Spanning Tree, VLAN, Port Trunking, Bandwidth Control, Port Security, SNMP/RMON and IGMP Snooping capability via the intelligent software. It is suitable for both metro-LAN and industrial application.

The device support DHCP Relay function. The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay Agent is therefore the routing protocol that enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or which is not located on the local subnet.

The switch also supports the IEEE Standard—802.1AB LLDP (Link Layer Discovery Protocol), provide more easy debug tool and enhance the networking management availability, others it can provide auto-discovery device and topology providing.

• Model Description

Model	Port 9,10 Configurations
Cross-8/SP	Two types of media --- TP and SFP Fiber

10/100/1000Mbps TP is a standard Ethernet port that meets all IEEE 802.3/u/x/z Gigabit, Fast Ethernet specifications. 100/1000Mbps SFP Fiber transceiver is a Gigabit Ethernet port that fully complies with all IEEE 802.3z and 1000Base-SX/LX standards.

1000Mbps Single Fiber WDM (BiDi) transceiver is designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signal over a single fiber simultaneously.

For upgrading firmware, please refer to the Section 3-27 or Section 4-2-2 for more details.

• Key Features in the Device

DHCP Option 82:

This feature enables the Dynamic Host Configuration Protocol (DHCP) relay agent information (option 82) (Cross-8/SP switch) to include information about itself and the attached client when forwarding DHCP requests from a DHCP client to a DHCP server via Trust Port. The DHCP server can use this information to assign IP addresses 、 gateway 、 subnet mask 、 DNS for each subscriber of a service-provider network.

QoS:

Support Quality of Service by the IEEE 802.1P standard. There are two priority queue and packet transmission schedule using Weighted Round Robin (WRR). User-defined weight classification of packet priority can be based on either VLAN tag on packets or user-defined port priority.

Link Layer Discovery Protocol (LLDP):

IEEE 802.1AB (Link Layer Discovery Protocol) provide more easy debug tool and enhance the networking management availability, it also can provide auto-discovery device and topology providing.

Spanning Tree:

Support IEEE 802.1D, IEEE 802.1w (RSTP: Rapid Spanning Tree Protocol) standards.

VLAN:

Support Port-based VLAN and IEEE802.1Q Tag VLAN. Support 256 active VLANs and VLAN ID 1~4094.

Port Trunking:

Support static port trunking and port trunking with IEEE 802.3ad LACP.

Bandwidth Control:

Support ingress and egress per port bandwidth control.

Port Security:

Support allowed, denied forwarding and port security with MAC address.

SNMP/RMON:

SNMP agent and RMON MIB. In the device, SNMP agent is a client software which is operating over SNMP protocol used to receive the command from SNMP manager (server site) and echo the corresponded data, i.e. MIB object. Besides, SNMP agent will actively issue TRAP information when happened.

RMON is the abbreviation of Remote Network Monitoring and is a branch of the SNMP MIB.

The device supports MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group 1,2,3,9, Ethernet-like MIB (RFC 1643) and so on.

IGMP Snooping:

Support IGMP version 2 (RFC 2236): The function IGMP snooping is used to establish the multicast groups to forward the multicast packet to the

member ports, and, in nature, avoid wasting the bandwidth while IP multicast packets are running over the network.

Access Control List (ACL):

The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

IP-MAC-Port Binding:

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC Addresses and port number with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet.

Q-in-Q VLAN for performance & security:

The VLAN feature in the switch offers the benefits of both security and performance. VLAN is used to isolate traffic between different users and thus provides better security. Limiting the broadcast traffic to within the same VLAN broadcast domain also enhances performance. Q-in-Q, the use of double VLAN tags is an efficient method for enabling Subscriber Aggregation. This is very useful in the MAN.

MVR:

Multicast VLAN Registration (MVR) can support carrier to serve content provider using multicast for Video streaming application in the network. Each content provider Video streaming has a dedicated multicast VLAN. The MVR routes packets received in a multicast source VLAN to one or more receive VLANs. Clients are in the receive VLANs and the multicast server is in the source VLAN.

1-2. Checklist

Before you start installing the switch, verify that the package contains the following:

- Cross-8/SP L2 Managed Switch
- Modules (optional)
- This User's Manual in CD-ROM
- RS-232 Serial Port Cable(One end is RJ-45, another is DB9)



Don't provide Power Adapter.

Please notify your sales representative immediately if any of the aforementioned items is "missing or damaged" or "buy one power adapter".

1-3. Features

The Cross-8/SP, a standalone off-the-shelf switch, provides the comprehensive features listed below for users to perform system network administration and efficiently and securely serve your network.

• Hardware

- Supports 8-port 10/100M TP ports with Nway and auto MDIX function
- In Cross-8/SP, it supports 2 Gigabit dual media ports(TP/SFP) and 2 slots for removable SFP module supporting 100M or 1000M SFP fiber module
- Supports on-line pluggable fiber transceiver modules
- Supports 256KB packet buffer and 128KB control memory
- Maximal packet length can be up to 2048 bytes
- Full-duplex flow control (IEEE802.3x) and half-duplex backpressure

- Management
 - Supports concisely the status of port and easily port configuration
 - Supports per port traffic monitoring counters
 - Supports a snapshot of the system Information when you login
 - Supports port mirror function
 - Supports the static trunk function
 - Supports 802.1Q VLAN with 4094 entries.
 - Supports DHCP Broadcasting Suppression to avoid network suspended or crashed
 - Supports to send the trap event while monitored events happened
 - Supports default configuration which can be restored to overwrite the current configuration which is working on via web browser and CLI
 - Supports on-line plug/unplug SFP modules
 - Supports QoS, MAC Priority, 802.1p Priority and DiffServ DSCP Priority.
 - Built-in web-based management and CLI management, providing a more convenient UI for the user
 - Supports port mirror function with ingress/egress traffic
 - Supports rapid spanning tree (802.1w RSTP)
 - Supports 802.1x port security on a VLAN
 - Supports user management and only first login administrator can configure the device. The rest of users can only view the switch
 - SNMP access can be disabled and prevent from illegal SNMP access
 - Supports Ingress, Non-unicast and Egress Bandwidth rating management
 - The trap event and alarm message can be transferred via e-mail
 - Supports diagnostics to let administrator knowing the hardware status
 - Supports external loopback test to check the link status
 - TFTP for firmware upgrade, system log upload and configure file import/export
 - Supports remote boot the device through user interface and SNMP
 - Supports network time synchronization and daylight saving
 - Supports 120 event log records in the main memory and display on the local console
 - Supports Alarm Relay function through Web UI management, BIOS version 1.22 and firmware version 5.20 or later

1-4. View of Cross-8/SP



Fig. 1-1 Full View of Cross-8/SP with SFP Module

1-4-1. User Interfaces on the Front Panel

There are 8 TP Fast Ethernet ports and 2 slots for optional removable modules(100 or 1000Mbps SFP) on the front panel of the switch. LED display area which is located on the front panel of the switch.

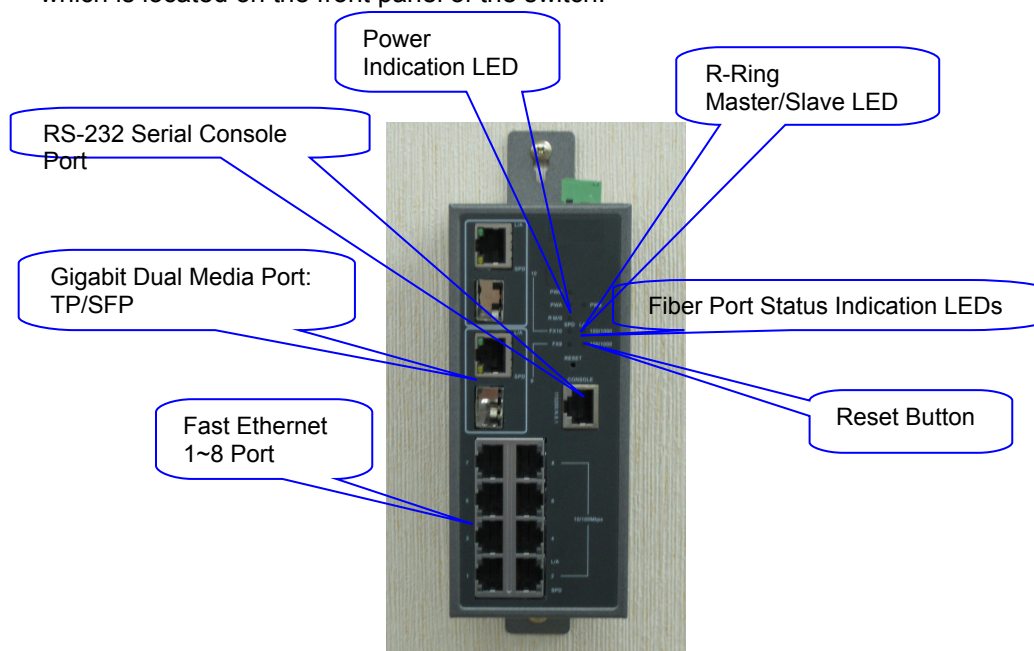


Fig. 1-2 Front View of Cross-8/SP

LED Indicators Description

Item	LED	Color	Description
GLOBAL	PWR	Green	Lit when any power input(Power A, B or DC jack) is coming up
Power A	PWA	Green	Lit when Power A is Active
Power B	PWB	Green	Lit when Power B is Active
R-RING	R.M/S	Green/ Amber	Lit Green when R-Ring is configured to Master Lit Amber when R-Ring is configured to Slave Off when no R-Ring function
FX9~10	L/A	Green	Lit when link up Blinks when any traffic is present
FX9~10	SPD	Green/ Amber	Lit Green when 1000Mbps SFP Transceiver is active Lit Amber when 100Mbps SFP Transceiver is active
TP Port 9~10 10/100/1000Mbps	L/A	Green	Lit when connection with remote device is good Blinks when any traffic is present
TP Port 9~10 10/100/1000Mbps	SPD	Green/ Amber	Lit Green when TP link on 1000Mbps speed Lit Amber when TP link on 100Mbps speed Off when 10Mbps or no link occur
TP Port 1~8 (10/100Mbps)	L/A	Green	Lit when connection with remote device is good Blinks when any traffic is present
TP Port 1~8 (10/100Mbps)	SPD	Amber	Lit Amber when TP link on 100Mbps speed Off when 10Mbps or no link occur

Table1-1

1-5. View of the Optional Modules

In the switch, Port 9, 10 includes two types of media --- TP or SFP Fiber (LC, BiDi LC...). TP port supports 10/100/1000Mbps. FX supports 100Mbps SFP or 1000Mbps SFP with auto-detected function. 1000Mbps SFP Fiber transceiver is used for high-speed connection expansion; the followings are optional SFP types provided for the switch:

Model	Description
SFP.LC	1000Base-SX GE SFP Fiber Module, LC Multi-Mode 850nm
SFP.LC.S10	1000Base-LX GE SFP Fiber Module, LC Single-Mode 10km
SFP.LC.S30	1000Base-LX GE SFP Fiber Module, LC Single-Mode 30km
SFP.LC.S50	1000Base-LX GE SFP Fiber Module, LC Single-Mode 50km
SFP.FLC	100Base-FX FE SFP Fiber Module, LC Multi-Mode
SFP.FLC.S20	100Base-FX FE SFP Fiber Module, LC Single-Mode 20km

*Available upon request



Fig. 1-3 Front View of 1000Base-SX/LX LC, SFP Fiber Transceiver



Fig. 1-4 Front View of 1000Base-LX BiDi LC, SFP Fiber Transceiver

2. Installation

2-1. Starting Cross-8/SP Up

This section will give users a quick start for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

2-1-1. Hardware and Cable Installation

First of all:

⇒ Wear a grounding device to avoid the damage from electrostatic discharge

- **Installing Optional SFP Fiber Transceivers to the Cross-8/SP L2+ Managed Switch**

Note: If you have no modules, please skip this section.

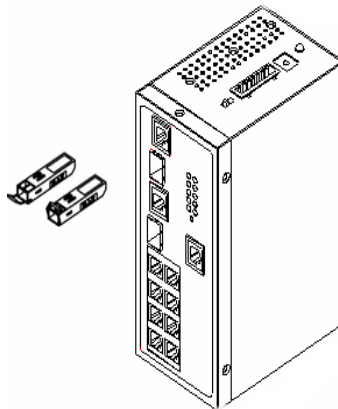


Fig. 2-1 Installation of Optional SFP Fiber Transceiver

- **Connecting the SFP Module to the Chassis:**

The optional SFP modules are hot swappable, so you can plug or unplug it before or after powering on.

1. Verify that the SFP module is the right model and conforms to the chassis
2. Slide the module along the slot. Also be sure that the module is properly seated against the slot socket/connector
3. Install the media cable for network connection
4. Repeat the above steps, as needed, for each module to be installed into slot(s)

- **TP Port and Cable Installation**

- ⇒ In the switch, TP port supports MDI/MDI-X auto-crossover, so both types of cable, straight-through (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 1, 2, 3, 6 in 10/100M TP; 1, 2, 3, 4, 5, 6, 7, 8 to 1, 2, 3, 4, 5, 6, 7, 8 in Gigabit TP) and crossed-over (Cable pin-outs for RJ-45 jack 1, 2, 3, 6 to 3, 6, 1, 2) can be used. It means you do not have to tell from them, just plug it.
- ⇒ Use Cat. 5 grade RJ-45 TP cable to connect to a TP port of the switch and the other end is connected to a network-aware device such as a workstation or a server.
- ⇒ Repeat the above steps, as needed.

Now, you can start having the switch in operation.

- **Power installation**

Power requirement 24VDC (12~48V)

You have to add DC power through the removable terminal block or DC jack from external DC power source.

- **Wiring the Power Input**

1. Insert the positive and negative wires into the PWR + and – contact on the removable terminal block connector or add power from DC jack.

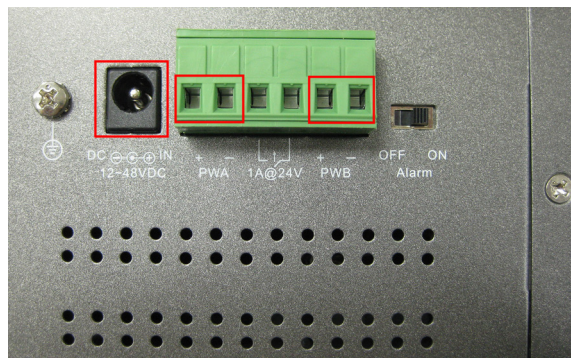


Fig. 2-2

2. Tighten the wire-clamp screw to prevent the DC wires from being loosened.

Note: The Suitable working voltage is from 12 to 48 VDC.

- **Power On**

It does not matter whether any connection plugged into the switch when power on, even modules as well. PWR LED indicator will lit.

- **Firmware Loading**

After resetting, the bootloader will load the firmware into the memory. It will take about 30 seconds.

- **Wiring the Relay Contact**

The alarm relay is energized (open) for normal operation and will close for fault conditions. This contact does not supply any power and is rated up to 24VDC at 1 A. Cross-8/SP provide an alarm slide switch too, it can turn off the alarm function by this switch.

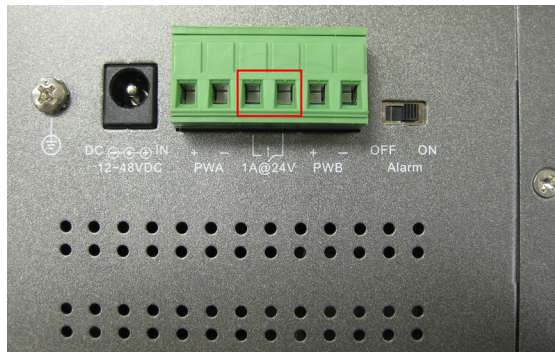


Fig. 2-3 Insert suitable alarm device

- **Alarm Relay Management through Web UI**

Normal:

Fig. 2-4 will be shown on the top of Web UI when alarm wasn't occurred.



Fig. 2-4 Normal

Alarm:

Fig. 2-5 will be shown on the top of Web UI when (1) or (2) was occurred.

- (1) Power A or Power B or Power C failure
- (2) Port(1-10) Link up→Link down



Fig. 2-5 Alarm

Clear Alarm(After trouble shooting):

Step 1: To click **<Clear>** button(Fig. 2-6)

Step 2: To click **<Yes>** button of "Confirm Message Box"(Fig. 2-7)

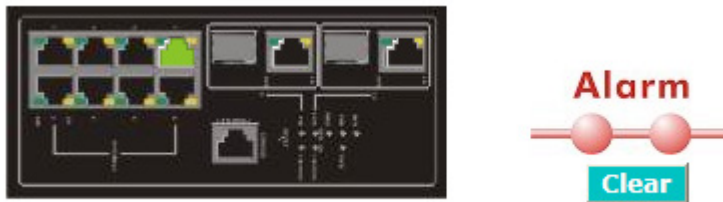


Fig. 2-6

Do you want to clear alarm?



Fig. 2-7

2-1-2. DIN-Rail Mounting Installation

The aluminum DIN-Rail attachment plate should already be fixed to the rear panel of Cross-8/SP when you take it out of the box. If you need to reattach the DIN-Rail attachment plate, make sure the stiff metal spring is situated towards the top, as shown by the following figure.

STEP 1: Insert the top of the DIN-Rail into the slot just below the stiff metal spring.



STEP 2: The DIN-Rail attachment plate will snap into rail as shown.



Fig. 2-4 DIN-Rail installation

To remove Cross-8/SP from the DIN-Rail, simply reverse STEP 1 and 2

2-1-2-1. Wall Mounting Installation

For some applications, you will find it convenient to mount Cross-8/SP on the wall, as Fig. 2-5.



Fig. 2-5 Wall Mounting Installation

2-1-3. Cabling Requirements

To help ensure a successful installation and keep the network performance good, please take a care on the cabling requirement. Cables with worse specification will render the LAN to work poorly.

2-1-3-1. Cabling Requirements for TP Ports

- ⇒ For Fast Ethernet TP network connection
 - The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters.
- ⇒ Gigabit Ethernet TP network connection
 - The grade of the cable must be Cat. 5 or Cat. 5e with a maximum length of 100 meters. Cat. 5e is recommended.

2-1-3-2. Cabling Requirements for 1000SX/LX SFP Module

It is more complex and comprehensive contrast to TP cabling in the fiber media. Basically, there are two categories of fiber, multi mode (MM) and single mode (SM). The later is categorized into several classes by the distance it supports. They are SX, LX, LHX, XD, and ZX. From the viewpoint of connector type, there mainly are LC and BiDi LC.

- Gigabit Fiber with multi-mode LC SFP module
- Gigabit Fiber with single-mode LC SFP module
- Gigabit Fiber with BiDi LC 1310nm SFP module
- Gigabit Fiber with BiDi LC 1550nm SFP module

The following table lists the types of fiber that we support and those else not listed here are available upon request.

IEEE 802.3z Gigabit Ethernet 1000SX 850nm	Multi-mode Fiber Cable and Modal Bandwidth			
	Multi-mode 62.5/125μm		Multi-mode 50/125μm	
	Modal Bandwidth	Distance	Modal Bandwidth	Distance
	160MHz-Km	220m	400MHz-Km	500m
	200MHz-Km	275m	500MHz-Km	550m
1000Base-LX/LHX/XD/ZX	SFP.LC.S10/30/50 Km			
	Single-mode Fiber 9/125μm			
	Single-mode transceiver 1310nm 10/30Km			
	Single-mode transceiver 1550nm 50Km			
1000Base-LX Single Fiber WDM Module	SFP.BL3.S20	Single-Mode *20Km	TX(Transmit)	1310nm
			RX(Receive)	1550nm
	SFP.BL5.S20	Single-Mode *20Km	TX(Transmit)	1550nm
			RX(Receive)	1310nm

Table2-1

2-1-3-3. Switch Cascading in Topology

• Takes the Delay Time into Account

Theoretically, the switch partitions the collision domain for each port in switch cascading that you may up-link the switches unlimitedly. In practice, the network extension (cascading levels & overall diameter) must follow the constraint of the IEEE 802.3/802.3u/802.3z and other 802.1 series protocol specifications, in which the limitations are the timing requirement from physical signals defined by 802.3 series specification of Media Access Control (MAC) and PHY, and timer from some OSI layer 2 protocols such as 802.1d, 802.1q, LACP and so on.

The fiber, TP cables and devices' bit-time delay (round trip) are as follows:

1000Base-X TP, Fiber		100Base-TX TP		100Base-FX Fiber	
Round trip Delay: 4096		Round trip Delay: 512			
Cat. 5 TP Wire:	11.12/m	Cat. 5 TP Wire:	1.12/m	Fiber Cable:	1.0/m
Fiber Cable :	10.10/m	TP to fiber Converter: 56			
Bit Time unit : 1ns (1sec./1000 Mega bit)		Bit Time unit: 0.01μs (1sec./100 Mega bit)			

Table 2-2

Sum up all elements' bit-time delay and the overall bit-time delay of wires/devices must be within Round Trip Delay (bit times) in a half-duplex network segment (collision domain). For full-duplex operation, this will not be applied. You may use the TP-Fiber module to extend the TP node distance over fiber optic and provide the long haul connection.

- **Typical Network Topology in Deployment**

A hierarchical network with minimum levels of switch may reduce the timing delay between server and client station. Basically, with this approach, it will minimize the number of switches in any one path; will lower the possibility of network loop and will improve network efficiency. If more than two switches are connected in the same network, select one switch as Level 1 switch and connect all other switches to it at Level 2. Server/Host is recommended to connect to the Level 1 switch. This is general if no VLAN or other special requirements are applied.

Case1: All switch ports are in the same local area network. Every port can access each other (See Fig. 2-6).

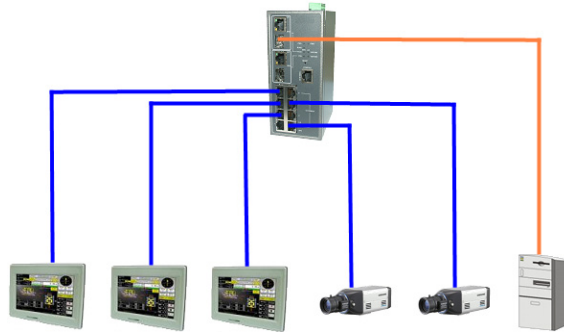


Fig. 2-6 No VLAN Configuration Diagram

If VLAN is enabled and configured, each node in the network that can communicate each other directly is bounded in the same VLAN area.

Here VLAN area is defined by what VLAN you are using. The switch supports both port-based VLAN and tag-based VLAN. They are different in practical deployment, especially in physical location. The following diagram shows how it works and what the difference they are.

Case2a: Port-based VLAN (See Fig.2-7).

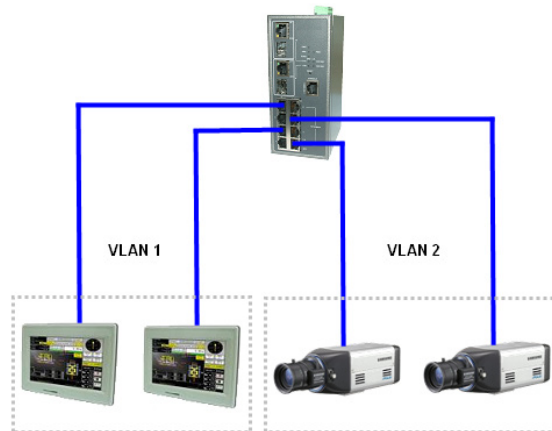


Fig. 2-7 Port-based VLAN Diagram

1. The same VLAN members could not be in different switches.
2. VLAN1 members could not access VLAN2 members.
3. The switch manager has to assign different names for each VLAN groups at one switch.

Case 2b: Port-based VLAN (See Fig.2-8).

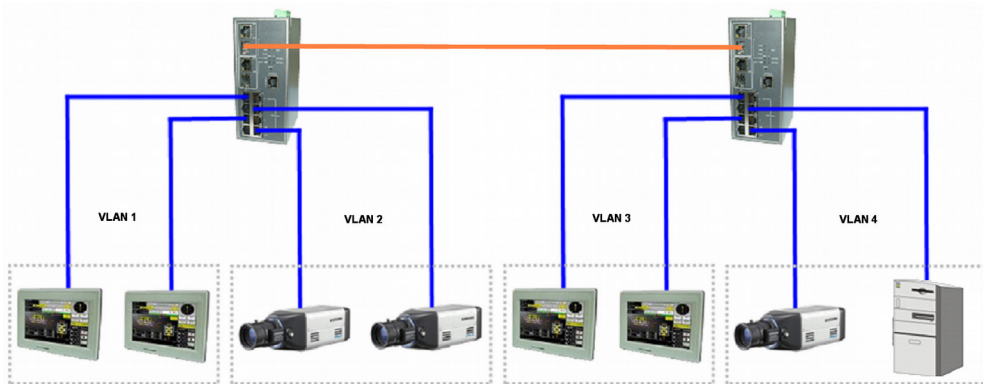


Fig. 2-8 Port-based VLAN Diagram

1. VLAN1 members could not access VLAN2, VLAN3 and VLAN4 members.
2. VLAN2 members could not access VLAN1 and VLAN3 members, but they could access VLAN4 members.
3. VLAN3 members could not access VLAN1, VLAN2 and VLAN4.
4. VLAN4 members could not access VLAN1 and VLAN3 members, but they could access VLAN2 members.

Case3a: The same VLAN members can be at different switches with the same VID (See Fig. 2-9).

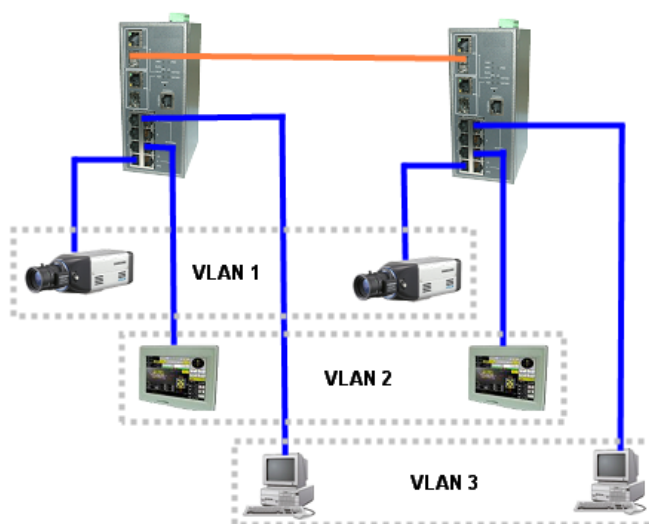


Fig. 2-9 Attribute-based VLAN Diagram

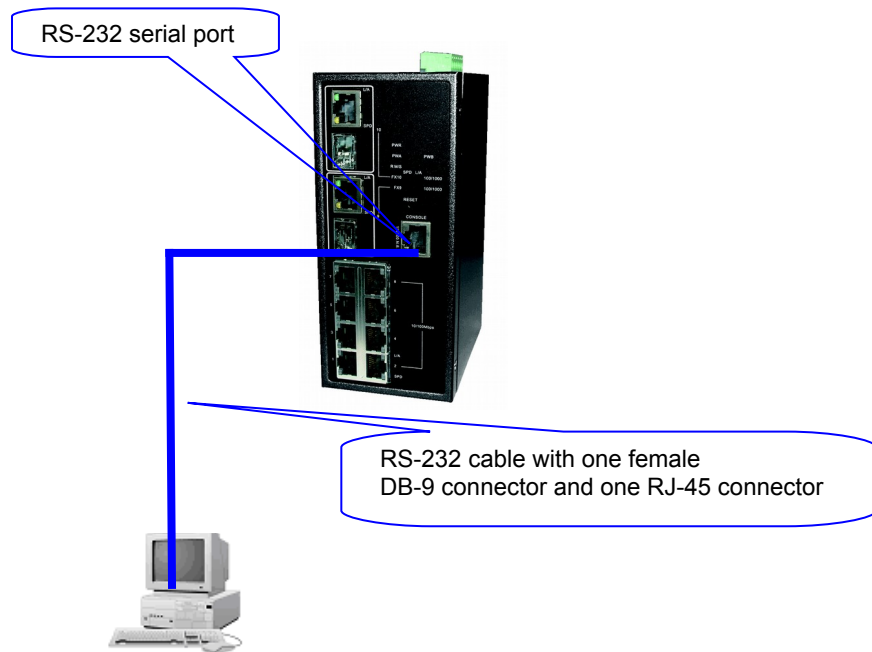
2-1-4. Configuring the Management Agent of Cross-8/SP

We offer you two ways to startup the switch management function. They are RS-232 serial CLI and Web. Users can use any one of them to monitor and configure the switch. You can touch them through the following procedures.

Section 2-1-4-1: Configuring the Management Agent of Cross-8/SP through the Serial RS-232 Port

Section 2-1-4-2: Configuring the Management Agent of Cross-8/SP through the Ethernet Port

2-1-4-1. Configuring the Management Agent of Cross-8/SP through the Serial RS-232 Port



Terminal or Terminal Emulator

Fig. 2-10 Configure with RS-232

To configure the switch, please follow the procedures below:

1. Find the RS-232 serial cable with connector bundled. Normally, it just uses pins 2, 3 and 5.
2. Attaches the DB-9 female connector to the DB-9 male connector on the PC.
3. Attaches the other end of the serial RS-232 RJ-45 connector to switch's serial port, running a terminal emulator supporting VT100/ANSI terminal with the switch's serial port default settings. For example, Windows98/2000/XP HyperTerminal utility.

Note: The switch's serial port default settings are listed as follows:

Baud rate	57600
Stop bits	1
Data bits	8
Parity	N
Flow control	none

4. When you complete the connection, then press **<Enter>** key. The login prompt will be shown on the screen. The default accounts are shown as Appendix B.

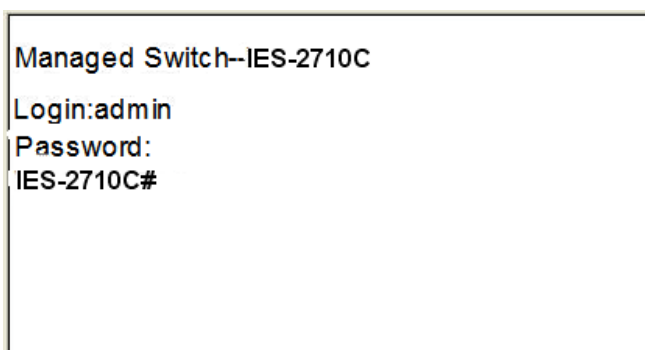
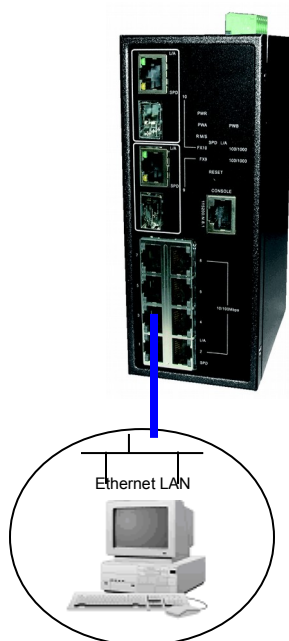


Fig. 2-11 Login Screen for CLI

2-1-4-2. Configuring the Management Agent of Cross-8/SP through the Ethernet Port



Cross-8/SP L2 Managed Switch
Default IP Setting:
IP = 192.168.1.1
Subnet Mask = 255.255.255.0
Default Gateway = 192.168.1.254

Assign a reasonable IP address,
For example:
IP = 192.168.1.100
Subnet Mask = 255.255.255.0
Default Gateway = 192.168.1.254

Fig. 2-12 Configure Cross-8/SP through Ethernet Port

- **Managing Cross-8/SP through Ethernet Port**

Before you communicate with the switch, you have to use the default IP address of the switch. Then follow the procedures listed below.

1. Set up a physical path between the configured switch and a PC by a qualified UTP Cat. 5 cable with RJ-45 connector.

Note: If PC directly connects to the switch, you have to setup the same subnet mask between them. But, subnet mask may be different for the PC in the remote site. Please refer to Fig. 2-12 about the switch's default IP address information.

2. For more information refer to Chapter 3.



Fig. 2-13 the Login Screen for Web

2-1-5. IP Address Assignment

For IP address configuration, there are three parameters needed to be filled in. They are IP address, Subnet Mask, Default Gateway and DNS.

IP address:

The address of the network device in the network is used for internet working communication. Its address structure is shown in the below. It is “classful” because it is split into predefined address classes or categories.

Each class has its own network range between the network identifier and host identifier in the 32 bits address. Each IP address comprises two parts: network identifier (address) and host identifier (address). The former indicates the network where the addressed host resides, and the later indicates the individual host in the network which the address of host refers to. And the host identifier must be unique

in the same LAN. Here the term of IP address we used is version 4, known as IPv4.

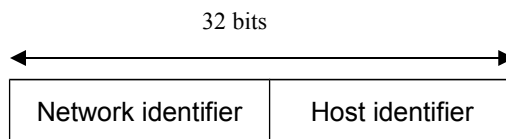


Fig. 2-14 IP address structure

With the classful addressing, it divides IP address into three classes, class A, class B and class C. The rest of IP addresses are for multicast and broadcast. The bit length of the network prefix is the same as that of the subnet mask and is denoted as IP address/X, for example, 192.168.1.0/24. Each class has its address range described below.

Class A:

Address is less than 126.255.255.255. There are a total of 126 networks can be defined because the address 0.0.0.0 is reserved for default route and 127.0.0.0/8 is reserved for loopback function.

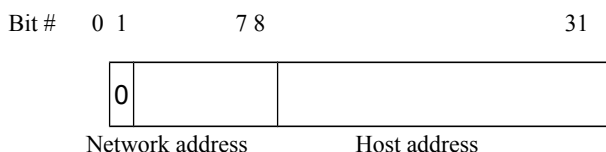


Fig. 2-15 Class A

Class B:

IP address range between 128.0.0.0 and 191.255.255.255. Each class B network has a 16-bit network prefix followed 16-bit host address. There are $16,384 = (2^{14})/16$ networks able to be defined with a maximum of $65534 = (2^{16} - 2)$ hosts per network.

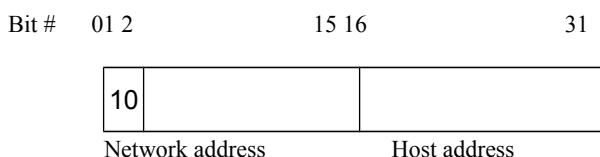


Fig. 2-16 Class B

Class C:

IP address range between 192.0.0.0 and 223.255.255.255. Each class C network has a 24-bit network prefix followed 8-bit host address. There are $2,097,152 = (2^{21})/24$ networks able to be defined with a maximum of $254 = (2^8 - 2)$ hosts per network.

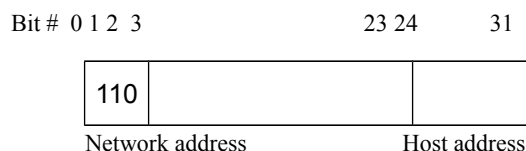


Fig. 2-17 Class C

Class D and E:

Class D is a class with first 4 MSB (Most significance bit) set to 1-1-1-0 and is used for IP Multicast. See also RFC 1112. Class E is a class with first 4 MSB set to 1-1-1-1 and is used for IP broadcast.

According to IANA (Internet Assigned Numbers Authority), there are three specific IP address blocks reserved and able to be used for extending internal network. We call it Private IP address and list below:

Class A	10.0.0.0 --- 10.255.255.255
Class B	172.16.0.0 --- 172.31.255.255
Class C	192.168.0.0 --- 192.168.255.255

Please refer to RFC 1597 and RFC 1466 for more information.

Subnet mask:

It means the sub-division of a class-based network or a CIDR block. The subnet is used to determine how to split an IP address to the network prefix and the host address in bitwise basis. It is designed to utilize IP address more efficiently and ease to manage IP network.

For a class B network, 128.1.2.3, it may have a subnet mask 255.255.0.0 in default, in which the first two bytes is with all 1s. This means more than 60 thousands of nodes in flat IP address will be at the same network. It's too large to manage practically. Now if we divide it into smaller network by extending network prefix from 16 bits to, say 24 bits, that's using its third byte to subnet this class B network. Now it has a subnet mask 255.255.255.0, in which each bit of the first three bytes is 1. It's now clear that the first two bytes is used to identify the class B network, the third byte is used to identify the subnet within this class B network and, of course, the last byte is the host number.

Not all IP address is available in the sub-netted network. Two special addresses are reserved. They are the addresses with all zero's and all one's host number. For example, an IP address 128.1.2.128, what IP address reserved will be looked like? All 0s mean the network itself, and all 1s mean IP broadcast.

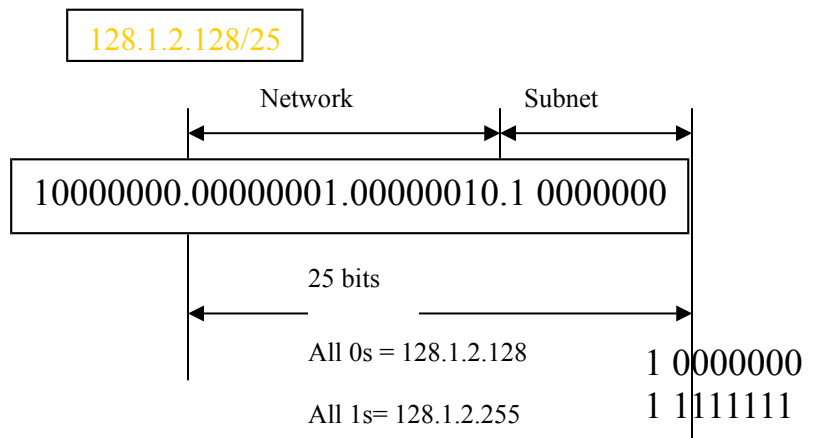


Fig. 2-18 subnet mask

In this diagram, you can see the subnet mask with 25-bit long, 255.255.255.128, contains 126 members in the sub-netted network. Another is that the length of network prefix equals the number of the bit with 1s in that subnet mask. With this, you can easily count the number of IP addresses matched. The following table shows the result.

Prefix Length	No. of IP matched	No. of Addressable IP
/32	1	-
/31	2	-
/30	4	2
/29	8	6
/28	16	14
/27	32	30
/26	64	62
/25	128	126
/24	256	254
/23	512	510
/22	1024	1022
/21	2048	2046
/20	4096	4094
/19	8192	8190
/18	16384	16382
/17	32768	32766
/16	65536	65534

Table 2-4

According to the scheme above, a subnet mask 255.255.255.0 will partition a network with the class C. It means there will have a maximum of 254 effective nodes existed in this sub-netted network and is considered a physical network in an autonomous network. So it owns a network IP address which may looks like 168.1.2.0.

With the subnet mask, a bigger network can be cut into small pieces of network. If we want to have more than two independent networks in a network, a partition to the network must be performed. In this case, subnet mask must be applied.

For different network applications, the subnet mask may look like 255.255.255.240. This means it is a small network accommodating a maximum of 15 nodes in the network.

Default gateway:

For the routed packet, if the destination is not in the routing table, all the traffic is put into the device with the designated IP address, known as default router. Basically, it is a routing policy. The gateway setting is used for Trap Events Host only in the switch.

For assigning an IP address to the switch, you just have to check what the IP address of the network will be connected with the switch. Use the same network address and append your host address to it.

IP Configuration

DHCP Setting	Disable
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DNS Server	Manual 0.0.0.0

Apply

Fig. 2-19 IP Configuration

First, IP Address: as shown in the Fig. 2-19, enter “192.168.1.1”, for instance. For sure, an IP address such as 192.168.1.x must be set on your PC.

Second, Subnet Mask: as shown in the Fig. 2-19, enter “255.255.255.0”. Any subnet mask such as 255.255.255.x is allowable in this case.

DNS:

The Domain Name Server translates human readable machine name to IP address. Every machine on the Internet has a unique IP address. A server generally has a static IP address. To connect to a server, the client needs to know the IP of the server. However, user generally uses the name to connect to the server. Thus, the switch DNS client program (such as a browser) will ask the DNS to resolve the IP address of the named server.

2-2. Typical Applications

The Cross-8/SP implements 8 Fast Ethernet TP ports with auto MDIX and 2 Gigabit dual media ports with SFP for removable module supported comprehensive fiber types of connection, including LC, BiDi LC for SFP. For more details on the specification of the switch, please refer to Appendix A.

The switch is suitable for the following applications.

- Central Site/Remote site application is used in Industry Environment (See Fig. 2-20)
- Peer-to-peer application is used in factory line1 and line2(See Fig. 2-21)
- R-Ring network(See Fig. 2-22)

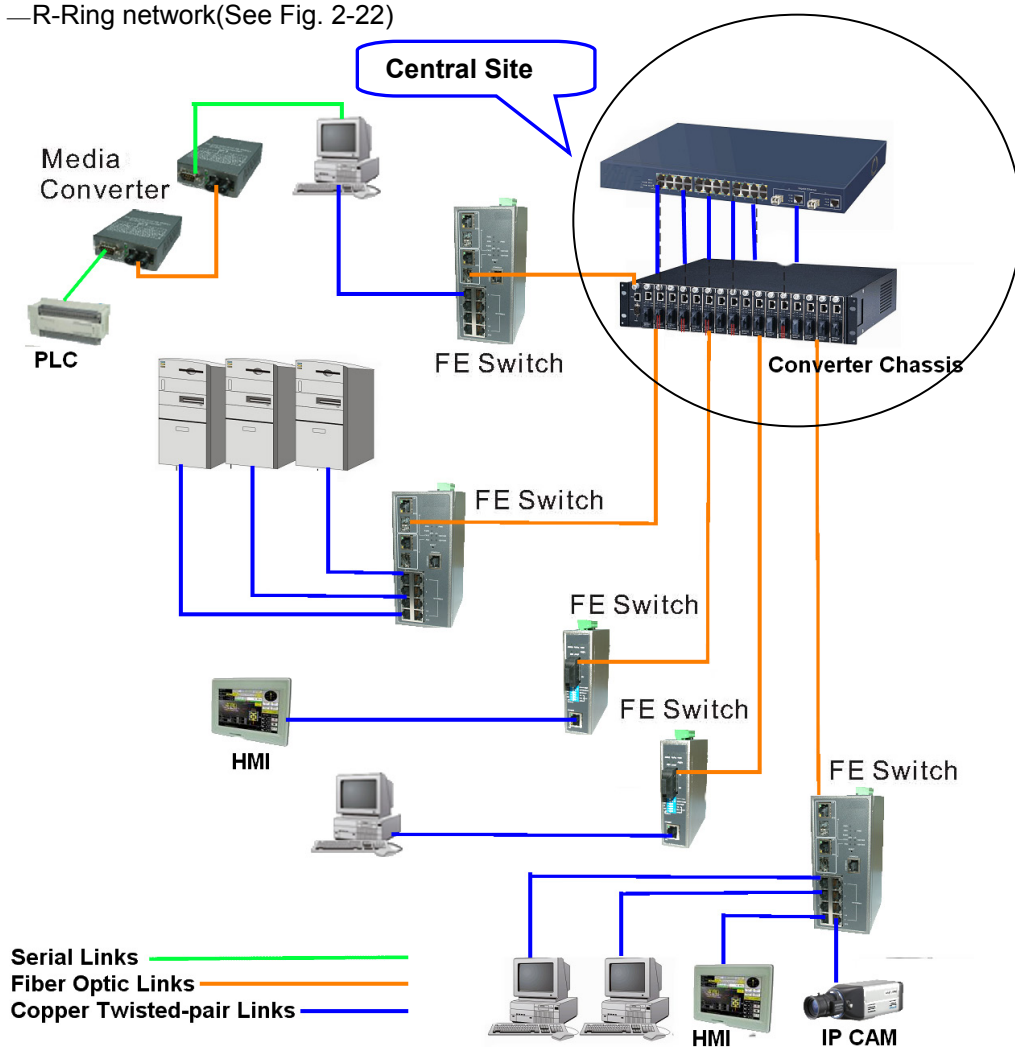


Fig. 2-20 Network Connection between Remote Site and Central Site

Fig. 2-20 is a system wide basic reference connection diagram. This diagram demonstrates how the switch connects with other network devices and hosts.

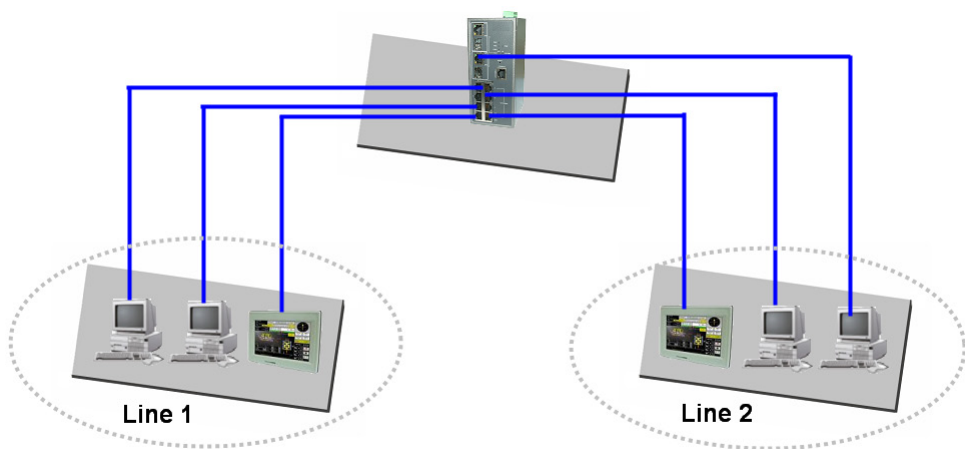


Fig. 2-21 Peer-to-peer Network Connection

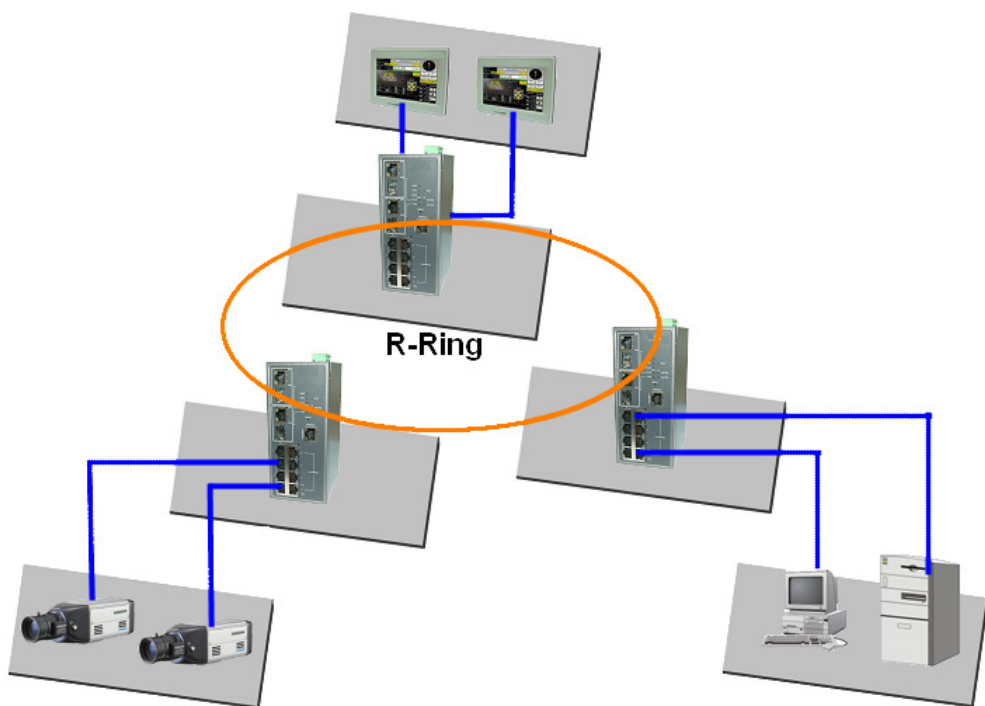


Fig. 2-22 R-Ring Network Connection

3. Operation of Web-based Management

This chapter instructs you how to configure and manage the Cross-8/SP through the web user interface it supports, to access and manage the 8 10/100Mbps TP + 2 Gigabit dual media ports with TP/SFP management Ethernet switch. With this facility, you can easily access and monitor all the status through any port of the switch, including each port activity, spanning tree status, port aggregation status, multicast traffic, VLAN and priority status, even illegal access record and so on.

The default values of the managed switch are listed in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	Admin
Password	1234

Table 3-1

You can browse it. For instance, type <http://192.168.1.1> in the address row in a browser, it will show the following screen (see Fig.3-1) and ask you inputting username and password in order to login and access authentication. The default username “Admin” and password “1234” (Table 3-1). For the first time to use, please enter the default username and password, then click the **<Login>** button. The login process now is completed. The switch will not give you a shortcut to username automatically. This looks inconvenient, but safer.

Please Input Username & Password

Username:

Password:

[Forget Password?](#)



Fig. 3-1 Login

Just click the link of “Forget Password” in WebUI (See Fig. 3-1) or input “Ctrl+Z” in CLI’s login screen (See Fig. 4-1~4-2) in case the user forgets the manager’s password. Then, the system will display a serial No. for the user. Write down this serial No. and contact your vendor, the vendor will give you a temporary password. Use this new password as ID and Password, and it will allow the user to login the system with manager authority temporarily. Due to the limit of this new password, the user only can login the system one time, therefore, please modify your password immediately after you login in the system successfully.

In the switch, it supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users login with administrator’s identity, the switch will allow the only one who logins first to configure the system. The rest of users, even with administrator’s identity, can only monitor the system same as those who have no administrator’s identity.

To optimize the display effect, we recommend you use Microsoft IE 6.0 above, Netscape V7.1 above or FireFox V1.0.0 above and have the resolution 1024x768. The switch supported neutral web browser interface.

3-1. Web Management Home Overview

After you login, the switch shows you the system information as Fig. 3-2. With this information, you will know the software version used, MAC address, serial number and so on. Left of the Fig. 3-2 is the whole function tree with web user interface and we will travel it through this chapter.

The screenshot displays the web management interface for the IFEL2P-SW8C01 switch. On the left is a navigation tree with categories like System, DHCP, Port, and Security. The main area is titled 'System Information' and contains a table of device details. At the top right, there is a status indicator showing 'Normal' with a green light icon. An 'Auto Logout' dropdown is set to '3 min'. An 'Apply' button is located at the bottom right of the system information table.

System Information	
Model Name	IFEL2P-SW8C01
System Description	Industrial 8-Port L2 Managed Fast Ethernet Switch + 2 TP/(100/1000M)SFP Dual Media
Location	
Contact	
Device Name	IFEL2P-SW8C01
System Up Time	0 Days 4 Hours 10 Mins 38 Secs
Current Time	Fri Jan 01 04:20:35 2010
BIOS Version	v1.22
Firmware Version	v5.32
Hardware-Mechanical Version	v1.01 - v1.01
Serial Number	033001000012
Host IP Address	192.168.1.1
Host MAC Address	00-40-C7-2F-20-D3
Device Port	UART *1, TP *8, Dual-Media(TP/SFP) *2
RAM Size	32 M
Flash Size	4 M
CPU Load	7 %

Fig. 3-2 System Information

- **The Information of Page Layout**

On the top side, it shows the front panel of the switch. In the front panel, the linked ports will display green; as to the ports, which are link off, they will be dark. For the optional modules, the slot will show only a cover plate if no module exists and will show a module if a module is present. The image of module depends on the one you inserted. The same, if disconnected, the port will show just dark, if linked, green. When clicking the link up port (Green color) on the front panel, a pop-up window will show detail information about this clicked port.(See Fig. 3-3)

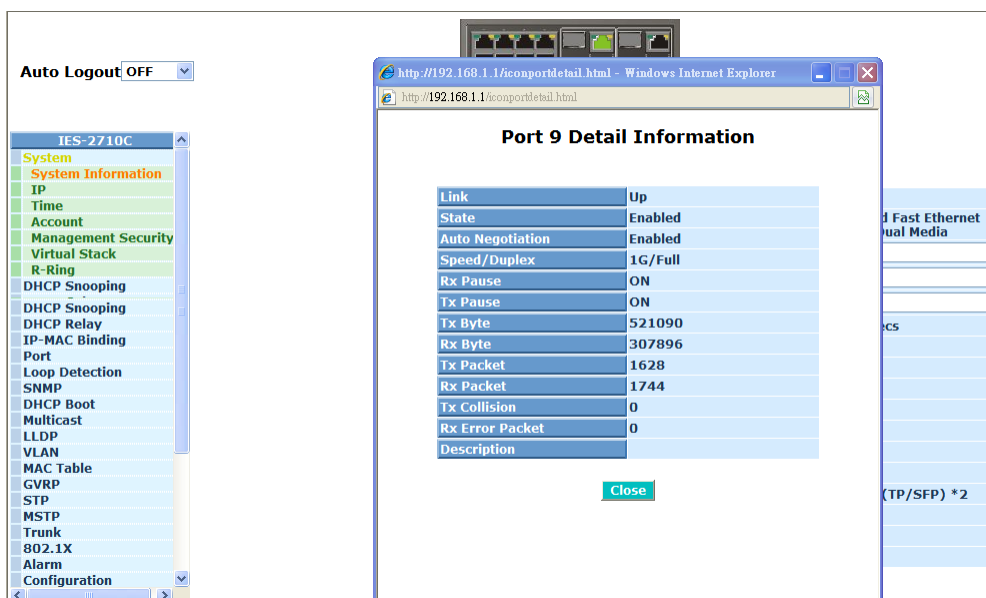


Fig. 3-3 port detail information

- On the left-top corner, there is a pull-down list for Auto Logout. For the sake of security, we provide auto-logout function to protect you from illegal user as you are leaving. If you do not choose any selection in Auto Logout list, it means you turn on the **Auto Logout function and the system will be logged out automatically when no action on the device 3 minutes later. If OFF is chosen, the screen will keep as it is. Default is ON.**
- On the left side, the main menu tree for web is listed in the page. They are hierarchical menu. Open the function folder, a sub-menu will be shown. The functions of each folder are described in its corresponded section respectively. When clicking it, the function is performed.

3-1-1. System Information

Function name:

System Information

Function description:

Show the basic system information.

Parameter description:

Model name:

The model name of this device.

System description:

As it is, this tells what this device is. Here, it is “**Industrial 8-Port L2 Managed Fast Ethernet Switch + 2 TP/SFP Gigabit Dual Media**”.

Location:

Basically, it is the location where this switch is put. User-defined.

Contact:

For easily managing and maintaining device, you may write down the contact person and phone here for getting help soon. You can configure this parameter through the device's user interface or SNMP.

Device name:

The name of the switch. User-defined. Default is Cross-8/SP.

System up time:

The time accumulated since this switch is powered up. Its format is day, hour, minute, second.

Current time:

Show the system time of the switch. Its format: day of week, month, day, hours : minutes : seconds, year. For instance, **Tue Apr 14 11:25:58 2009**

BIOS version:

The version of the BIOS in this switch.

Firmware version:

The firmware version in this switch.

Hardware-Mechanical version:

The version of Hardware and Mechanical. The figure before the hyphen is the version of electronic hardware; another one after the hyphen is the version of mechanical.

Serial number:

The serial number is assigned by the manufacturer.

Host IP address:

The IP address of the switch.

Host MAC address:

It is the Ethernet MAC address of the management agent in this switch.

Device Port:

Show all types and numbers of the port in the switch.

RAM Size:

The size of the DRAM in this switch is 32M.

Flash Size:

The size of the flash memory in this switch is 4M.

CPU Load:

CPU loading percentage

3-1-2. IP Configuration

IP configuration is one of the most important configurations in the switch. Without the proper setting, network manager will not be able to manage or view the device. The switch supports both manual IP address setting and automatic IP address setting via DHCP server. When IP address is changed, you must reboot the switch to have the setting taken effect and use the new IP to browse for web management and CLI management.

Function name:

IP

Function description:

Set IP address, subnet mask, default gateway and DNS for the switch.

IP Configuration

DHCP Setting	Disable ▾
IP Address	192.168.1.1
Subnet Mask	255.255.255.0 ▾
Default Gateway	192.168.1.254
DNS Server	Manual ▾ 0.0.0.0

Apply

Fig. 3-4 IP Configuration

Parameter description:

DHCP Setting:

DHCP is the abbreviation of Dynamic Host Configuration Protocol. Here DHCP means a switch to turn ON or OFF the function.

The switch supports DHCP client used to get an IP address automatically if you set this function "Enable". When enabled, the switch will issue the request to the DHCP server resided in the network to get an IP address. If DHCP server is down or does not exist, the switch will issue the request and show IP address is under requesting, until the DHCP server is up. Before getting an IP address from DHCP server, the device will not continue booting procedures. If set this field "Disable", you'll have to input IP address manually. For more details about IP address and DHCP, please see the Section 2-1-5 "IP Address Assignment" in this manual.

Default: Disable

IP address:

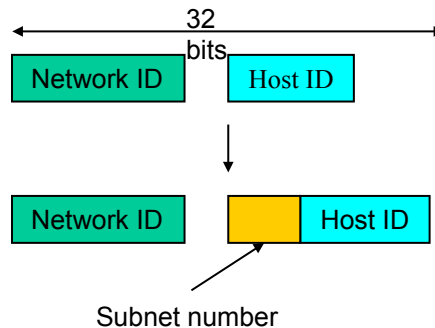
Users can configure the IP settings and fill in new values if users set the DHCP function "Disable". Then, click **<Apply>** button to update.

When DHCP is disabled, Default: 192.168.1.1

If DHCP is enabled, this field is filled by DHCP server and will not allow user manually set it any more.

Subnet mask:

Subnet mask is made for the purpose to get more network address because any IP device in a network must own its IP address, composed of Network address and Host address, otherwise can't communicate with other devices. But unfortunately, the network classes A, B, and C are all too large to fit for almost all networks, hence, subnet mask is introduced to solve this problem. Subnet mask uses some bits from host address and makes an IP address looked Network address, Subnet mask number and host address. It is shown in the following figure. This reduces the total IP number of a network able to support, by the amount of 2 power of the bit number of subnet number ($2^{\text{bit number of subnet number}}$).



Subnet mask is used to set the subnet mask value, which should be the same value as that of the other devices resided in the same network it attaches.

For more information, please also see the Section 2-1-5 "IP Address Assignment" in this manual.

Default: 255.255.255.0

Default gateway:

Set an IP address for a gateway to handle those packets that do not meet the routing rules predefined in the device. If a packet does not meet the criteria for other pre-defined path, it must be forwarded to a default router on a default path. This means any packet with undefined IP address in the routing table will be sent to this device unconditionally.

Default: 192.168.1.254

DNS:

It is Domain Name Server used to serve the translation between IP address and name address.

The switch supports DNS client function to re-route the mnemonic name address to DNS server to get its associated IP address for accessing Internet. User can specify a DNS IP address for the switch. With this, the switch can translate a mnemonic name address into an IP address.

There are two ways to specify the IP address of DNS. One is fixed mode, which manually specifies its IP address, the other is dynamic mode, which is assigned by DHCP server while DHCP is enabled. DNS can help you easily remember the mnemonic address name with the meaningful words in it. Default is no assignment of DNS address.

Default: 0.0.0.0

3-1-3. Time Configuration

The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input "Year", "Month", "Day", "Hour", "Minute" and "Second" within the valid value range indicated in each item. If you input an invalid value, for example, 61 in minute, the switch will clamp the figure to 59.

NTP is a well-known protocol used to synchronize the clock of the switch system time over a network. NTP, an internet draft standard formalized in RFC 1305, has been adopted on the system is version 3 protocol. The switch provides four built-in NTP server IP addresses resided in the Internet and an user-defined NTP server IP address. The time zone is Greenwich-centered which uses the expression form of GMT+/- xx hours.

Function name:

Time

Function description:

Set the system time by manual input or set it by syncing from Time servers. The function also supports daylight saving for different area's time adjustment.

System Time Setting

Current Time		Fri Jan 01 00:58:29 2010	
☒ Manual	Year	2010	(2000~2036)
	Month	1	(1~12)
	Day	1	(1~31)
	Hour	0	(0~23)
	Minute	58	(0~59)
	Second	29	(0~59)
☐ NTP	☒ 209.81.9.7(USA)		
	☐ 137.189.8.174(HK)		
	☐ 133.100.9.2(JP)		
	☐ 131.188.3.222(Germany)		
	☐ []		
Time Zone		GMT+8:00	
Daylight Saving		0	
Daylight Saving Start		Mth	1
		Day	1
		Hour	0
Daylight Saving End		Mth	1
		Day	1
		Hour	0
Apply			

Fig. 3-5 System Time Setting

Parameter description:

Current Time:

Show the current time of the system.

Default : 2010/1/1

Manual:

This is the function to adjust the time manually. Filling the valid figures in the fields of Year, Month, Day, Hour, Minute and Second respectively and

click **<Apply>** button, time is adjusted. The valid figures for the parameter Year, Month, Day, Hour, Minute and Second are ≥ 2000 , 1-12, 1-31, 0-23, 0-59 and 0-59 respectively. Input the wrong figure and click **<Apply>** button, the device will reject the time adjustment request. There is no time zone setting in Manual mode.

NTP:

NTP is Network Time Protocol and is used to sync the network time based Greenwich Mean Time (GMT). If use the NTP mode and select a built-in NTP time server or manually specify an user-defined NTP server as well as Time Zone, the switch will sync the time in a short after pressing **<Apply>** button. Though it synchronizes the time automatically, NTP does not update the time periodically without user's processing.

Time Zone is an offset time off GMT. You have to select the time zone first and then perform time sync via NTP because the switch will combine this time zone offset and updated NTP time to come out the local time, otherwise, you will not able to get the correct time. The switch supports configurable time zone from -12 to $+13$ step 1 hour.

Default Time zone: +8 Hrs.

Daylight Saving:

Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time since it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time since it passed over.

The switch supports valid configurable day light saving time is $-5 \sim +5$ step one hour. The zero for this parameter means it need not have to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

Default for Daylight Saving: 0.

The following parameters are configurable for the function Daylight Saving and described in detail.

Day Light Saving Start :

This is used to set when to start performing the day light saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

Day Light Saving End :

This is used to set when to stop performing the daylight saving time.

Mth:

Range is 1 ~ 12.

Default: 1

Day:

Range is 1 ~ 31.

Default: 1

Hour:

Range is 0 ~ 23.

Default: 0

3-1-4. Account Configuration

Function name:

Account

Function description:

In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/operator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 20 accounts can be created(Including Default Account Fig. 3-6).

Account Configuration

Account Name	Authorization
admin	Administrator
operator	Operator
guest	Guest



Fig. 3-6 Default Account

Function parameter:

Create New

Account Configuration

Authorization	Guest
User Name	gt125
New Password	
Confirm Password	

Apply Cancel

Fig. 3-6-1 Create New

Select an "Authorization" from pull down list box, key in "User Name", "New Password" and "Confirm Password". Then click **<Apply>** button to create a new one or click **<Cancel>** button to abort.

5 <= User Name, New Password, Confirm Password <= 47 characters

Edit

Select an account to edit and key in the new data, then click **<Apply>** button to edit or click **<Cancel>** button to abort.

Delete

Select an account to delete, then click **<Delete>** button to take effect.

3-1-5. Management Security

Through the management security configuration, the manager can do the strict setup to control the switch and limit the user to access this switch.

The following rules are offered for the manager to manage the switch:

Rule 1) : When no lists exists, then it will accept all connections.

Accept

Rule 2) : When only “accept lists” exist, then it will deny all connections, excluding the connection inside of the accepting range.

Accept Deny Accept Deny Accept

Rule 3) : When only “deny lists” exist, then it will accept all connections, excluding the connection inside of the denying range.

Deny Accept Deny Accept Deny

Rule 4) : When both “accept and deny” lists exist, then it will deny all connections, excluding the connection inside of the accepting range.

Accept Deny Deny Deny Accept

Rule 5) : When both “accept and deny” lists exist, then it will deny all connections, excluding the connection inside of the accepting range and NOT inside of the denying range at the same time.

Accept Deny Accept

Deny| Acc | Deny | Acc | Deny

Function name:

Management Security Configuration

Function description:

The switch offers Management Security Configuration function. With this function, the manager can easily control the mode that the user connects to the switch. According to the mode, users can be classified into two types: Those who are able to connect to the switch (Accept) and those who are unable to connect to the switch (Deny). Some restrictions also can be placed on the mode that the user connect to the switch, for example, we can decide that which VLAN VID is able to be accepted or denied by the switch, the IP range of the user could be accepted or denied by the switch, the port that the user is allowed or not allowed to connect with the switch, or the way of controlling and connecting to the switch via Http, Telnet or SNMP.

Management Security Configuration

Name	VID	IP Range
	☒ Any Custom:	☒ Any Custom: --

Incoming Port	Access Type	Action
☒ Any Custom: ☐ 1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐ 6. ☐ 7. ☐ 8. ☐ 9. ☐ 10.	☒ Any ☐ Custom: ☐ Http ☐ Telnet ☐ SNMP	☒ Deny ☐ Accept

No	Name	VID	IP Range	Incoming Port	Access Type	Action
----	------	-----	----------	---------------	-------------	--------

Fig. 3-7 Management Security Configuration

Parameter description:

Name:

A name is composed of any letter (A-Z, a-z) and digit (0-9) with maximal 8 characters.

VID:

The switch supports two kinds of options for managed valid VLAN VID, including "Any" and "Custom". Default is "Any". When you choose "Custom", you can fill in VID number. The valid VID range is 1~4094.

IP Range:

The switch supports two kinds of options for managed valid IP Range, including "Any" and "Custom". Default is "Any". In case that "Custom" had been chosen, you can assigned effective IP range. The valid range is 0.0.0.0~255.255.255.255.

Incoming Port:

The switch supports two kinds of options for managed valid Port Range, including "Any" and "Custom". Default is "Any". You can select the ports that you would like them to be worked and restricted in the management

security configuration if "Custom" had been chosen.

Access Type:

The switch supports two kinds of options for managed valid Access Type, including "Any" and "Custom". Default is "Any". "Http", "Telnet" and "SNMP" are three ways for the access and managing the switch in case that "Custom" had been chosen.

Action:

The switch supports two kinds of options for managed valid Action Type, including "Deny" and "Accept". Default is "Deny". When you choose "Deny" action, you will be restricted and refused to manage the switch due to the "Access Type" you choose. However, while you select "Accept" action, you will have the authority to manage the switch.

Edit/Create:

A new entry of Management Security Configuration can be created after the parameters as mentioned above had been setup and then press **<Edit/Create>** button. Of course, the existed entry also can be modified by pressing this button.

Delete:

Remove the existed entry of Management Security Configuration from the management security table.

3-1-6. Virtual Stack

Function name:

Virtual Stack

Function description:

Virtual Stack Management(VSM) is the group management function. Through the proper configuration of this function, switches in the same LAN will be grouped automatically. And among these switches, one switch will be a master device, and the others in this group will become the slave devices.

VSM offers a simple centralized management function. It is not necessary to remember the address of all devices, manager is capable of managing the network with knowing the address of the Master device. Instead of SNMP or Telnet UI, VSM is only available in Web UI. While one switch become the Master, two rows of buttons for group device will appear on the top of its Web UI. By pressing these buttons, user will be allowed to connect the Web UI of the devices of the group in the same window without the login of this device.

The most top-left button is only for Master device(See Fig. 3-9). The background color of the button you press will be changed to represent that the device is under your management.

Note: It will remove the grouping temporarily in case that you login the switch via the console.

The device of the group will be shown as station address (the last number of IP Address) + device name on the button (e.g. 196_Cross-8/SP), otherwise it will show " ---- " if no corresponding device exists.

Once the devices join the group successfully, then they are merely able to be managed via Master device, and user will fail to manage them via telnet/console/web individually.

Up to 16 devices can be grouped for VSM, however, only one Master is allowed to exist in each group. For Master redundancy, user may configure more than two devices as Master device, however, the Master device with the smaller MAC value will be the Master one.

Virtual Stack Configuration

State	Disable ▾
Role	Slave ▾
Group ID	default

Apply

Note: You should be logout every time when you change the state of Virtual Stack.

Fig. 3-8 Virtual Stack Configuration 1

Parameter description:

State:

It is used for the activation or de-activation of VSM. Default is Disable.

Role:

The role that the switch would like to play in virtual stack. Two types of roles, including master and slave are offered for option. Default is Slave.

Group ID:

It is the group identifier (GID) which assigns to VSM. Valid letters are A-Z, a-z, 0-9, “ - “ and “ _ ” characters. The maximal length is 15 characters.

1	IES-2710	----	----	----	----	----	----
		----	----	----	----	----	----



IP Configuration

DHCP Setting	Disable
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DNS Server	Manual 0.0.0.0

Apply

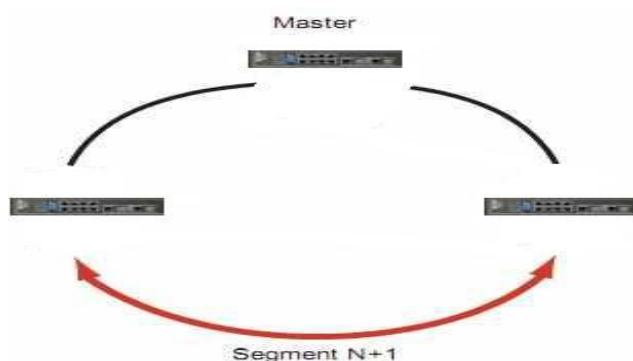
Fig. 3-9 Virtual Stack Configuration 2

3-1-7. R-Ring (Rapid-convergence Ring)

The proprietary R-Ring protocol was developed by Manufacture Tech to optimize communication redundancy and achieve a faster recovery time on the ring network topology. The R-Ring provides system integrators with a cost-effective, easy-to-configure, highly-reliable redundant ring capability.

The R-Ring protocol specify one switch as the “Master” in one ring network, the other switches must be set to “Member” slave role. You have to select two ports on each switch for ring connection. Each switch only join one ring.

Redundancy plays an important role in increasing the reliability of systems used for industrial automation applications, and the redundant network technology called “R-Ring”, now provides the redundant Ethernet recovery time under 30 milliseconds. If any segment of the network is disconnected, the R-Ring automation mechanism will be back to normal in less than 30 milliseconds, even at a full load of 100 switches.



Function name:

R-Ring

Function description:

The switch supports Network Redundancy function: R-Ring, and the recovery time is less than 30ms.

Note:R-Ring function can't run with

1. LACP
2. STP/RSTP/MSTP
3. IEEE802.1X
4. Loop Detection
5. IGMP Snooping , IGMP Proxy

R-Ring

	Config	Status
Role	Master ▼	
Port 1	Port 1 ▼	Block
Port 2	Port 10 ▼	Block



Fig. 3-10 R-Ring setting

Parameter description:

Role:

Set R-Ring role as Master, Member, or in Disable status.

Port 1,2 Config:

To select a port from list.

Port 1 to port 10 available.

Port 1,2 Status:

“Block” when Role is set to Master or Member.

“ - - - ” when Role is set to Disable.

3-2. DHCP Snooping

3-2-1. Config

Function name:

DHCP Snooping Config

Function description:

The addresses assigned to DHCP clients on unsecure 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.

When DHCP servers are allocating IP addresses to the clients on the LAN, DHCP snooping can be configured on LAN switches to harden the security on the LAN to only allow clients with specific IP/MAC addresses to have access to the network.

DHCP snooping is a series of layer 2 techniques. It works with information from a DHCP server to:

- Track the physical location of hosts.
- Ensure that hosts only use the IP addresses assigned to them.
- Ensure that only authorized DHCP servers are accessible.

In short, DHCP snooping ensures IP integrity on a Layer 2 switched domain.

With DHCP snooping, only a whitelist of IP addresses may access the network. The whitelist is configured at the switch port level, and the DHCP server manages the access control. Only specific IP addresses with specific MAC addresses on specific ports may access the IP network.

DHCP Snooping Config

State	Disable ▾
Per Port Client Count Setup	
Port	Count
1	128
2	128
3	128
4	128
5	128
6	128
7	128
8	128
9	128
10	128

Apply

Fig. 3-11 DHCP Snooping Config

DHCP snooping also stops attackers from adding their own DHCP servers to the network. An attacker could set up a server to wreak havoc in the network or even control it.

Parameter description:

State:

It is used for the activation or de-activation of DHCP snooping.

Default : disable

Per Port Client Count Setup:

It is used for per port client count setup.

Default : 128

3-2-2. Trust Group

Function name:

DHCP Snooping Trust Group Config

Function description:

DHCP Snooping Trust Group Config allows a switch to add a trust DHCP server and its port to build the DHCP Snooping Trust Group.

DHCP Snooping Trust Group Config

Trust VID	Server Port	Server VID	DHCP Server IP	Option 82	Action
DHCP Snooping is disabled					

Delete

Server Port 1	Disable ▾	Server Port 2	Disable ▾
Option 82	Disable ▾	Action	Replace ▾
Server VID		Server IP	0.0.0.0
Turst VID			

Edit/Create

Default Group

Server Port 1	Disable ▾	Server Port 2	Disable ▾
Option 82	Disable ▾	Action	Keep ▾
Server VID	1	Server IP	0.0.0.0

Apply

Fig. 3-12 DHCP Snooping Trust Group Config

Parameter description:

Server Port 1:

If DHCP snooping is enabled globally, and also enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port. It set available port from 1 to 10.

Default : Disabled

Server Port 2:

It set a trust port 2 available port from 1 to 10.

Default : Disabled

Option 82:

It set the DHCP Option 82 function on the switch.
Default : Disabled

Action:

It set the switch when received a client DHCP request packet then action for filtering. Available action : keep/drop/replace.

Server VID:

Available VID from 1 to 4094.

Server IP:

It set a trust DHCP Server IP address for DHCP Snooping.

Trust VID:

Available VID from 1 to 4094.

Note : Filtering rules are implemented as follows:

If the DHCP snooping is disabled, all DHCP packets are forwarded.

If DHCP snooping is enabled on the VLAN where the DHCP packet is received, all DHCP packets are forwarded for a trusted port.

If DHCP snooping is enabled on the VLAN where the DHCP packet is received, but the port is not trusted, it is processed as follows:

If the DHCP packet is reply packet from a DHCP server, the packet is dropped.

If the DHCP packet is from a client, such as a DISCOVER, REQUEST INFORMATION, DECLINE or RELEASE message, the packet is forwarded

if MAC address verification is disabled. However , if MAC address verification is enabled, then the packet will only be forwarded if the client's hardware address stored in the DHCP packet is the same as the source MAC address in the Ethernet header.

If the DHCP packet is not a recognizable type, it is dropped.

If a DHCP packet from a client passes the filtering criteria above, it will only be forwarded to trusted ports in the same VLAN.

If a DHCP packet is from server and is received on a trusted port, it will be forwarded to both trusted and un-trusted ports in the same VLAN.

3-2-3. Lease List

Function name:

DHCP Snooping Lease List

Function description:

DHCP Snooping Lease List

MAC	IP	Port	VID	Lease (Day:Hour:Min:Sec)
DHCP Snooping is disabled				

Fig. 3-13 DHCP Snooping Lease List

Parameter description:

MAC : To show the DHCP snooping client's MAC address.

IP : To show the DHCP snooping client's IP address.

Port : To show the DHCP snooping client's port.

VID : To show the DHCP snooping client's VLAN ID.

Lease : To show the DHCP snooping client's lease. (Day:Hour:Min:Sec)

3-2-4. Counter

Function name :

DHCP Snooping Counter

Function description :

To display per port the DHCP Snooping Counter status. Includes Port No., Discovery, Offer, Request, Decline, Ack, Nack, Release and Inform.

DHCP Snooping Counter									
Refresh Interval 3 sec ▼									Reset
Port No	Discovery	Offer	Request	Decline	Ack	Nack	Release	Inform	
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	1	0	0	0	0	0	4
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

Fig. 3-14 DHCP Snooping Counter

Parameter description :

Refresh Interval: Available value from 3 to 10 seconds

Reset: Reset port 1~10 data

3-3. DHCP Relay

The DHCP is a service that runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients. DHCP clients request IP addresses, and obtain leases for IP addresses from the DHCP server.

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP Relay Agent is therefore by the routing protocol that enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or which is not located on the local subnet. If you have no configured DHCP Relay Agent, your clients would only be able to obtain IP addresses from the DHCP server which is on the same subnet.

If you are using the switches to [insert DHCP Option 82 information](#) and you are also using as DHCP relay-agents (via 'ip helper-address'), you'll notice right away that your Option 82 enabled DHCP requests are not being forwarded by your switches.

3-3-1. Config

Function name :

DHCP Relay Config

Function description :

The switch enable clients to obtain IP addresses from a DHCP server on a remote subnet, you have to configure the DHCP Relay Agent on the subnet that contains the remote clients, so that it can relay DHCP broadcast messages to your DHCP server.

DHCP Relay

DHCP Relay State	Disable ▾
DHCP Relay LifeTime	5 ▾ seconds
DHCP Relay Agent Information Option82 State	Disable ▾
DHCP Relay Agent Information Option82 Policy	Keep ▾
Server Port	1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐ 6. ☐ 7. ☐ 8. ☐ 9. ☐ 10. ☐
Server IP	0.0.0.0

[Apply](#)

Fig. 3-15

Parameter description :

DHCP Relay State:

To enable or disable the DHCP Relay function on the switch.
Default is "Disable".

DHCP Relay LifeTime:

Use to set the default lifetime for which a prefix delegated by this DHCP

local server is valid. This default is overridden by an interface-specific lifetime.

Available values from 1 to 10 seconds.

Default: 5 seconds

DHCP Relay Agent Information Option82 State:

Enables the system to insert the DHCP relay agent information option 82 in forwarded BOOT REQUEST messages to a DHCP server.

Default: Disable

DHCP Relay Agent Information Option82 Policy:

A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. If this behavior is not suitable for your network, you can use the command "Replace, keep, Drop" to change it.

Default: Keep

Server Port:

To evoke which port will enable the DHCP Relay Agent service.

Available port from 1 to 10.

Server IP:

To set the DHCP Server IP address.

3-4. IP-MAC Binding

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC Addresses and port number with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet.

3-4-1. State

Function name:

IP MAC Binding State

Function description:

The switch has client and server two classes of IP-MAC binding table. The maximum number of IP-MAC binding client table is 512 entries. The maximum number of IP-MAC binding server table is 64 entries. The creation of authorized users can be manually. The function is global, this means a user can enable or disable the function for all ports on the switch.

IP-MAC-Binding

Mode	Disable ▾							
Binding Port	1. ☒	2. ☒	3. ☒	4. ☒	5. ☒	6. ☒	7. ☒	8. ☒
	9. ☐	10. ☐						

Fig. 3-16

Parameter description :

Mode:

It is used for the activation or de-activation of IP-MAC Binding. Default is disable.

Binding Port:

These are the ports which signs for IP-MAC Binding.

3-4-2. Binding List

Function name:

IP MAC Binding List

Function description:

To list the current IP MAC Binding List.

Current User List

No	Name	MAC	IP	Method	Type
Delete ☐	Binding Ports				
1	Test	00-11-2A-FD-22-33	192.168.1.210	IP-MAC	Static
☐ 6					
Add	Delete				

Page: 1

Fig. 3-17

Parameter description :

Current user list:

The maximum number of IP-MAC Binding client table is 512 entries. The maximum number of IP-MAC Binding server table is 64 entries.

No.:

The entry number of IP-MAC Binding.

Name:

That is composed of any letter (A-Z, a-z) and digit (0-9) with maximum 8 characters.

MAC:

Six-byte MAC Address: xx-xx-xx-xx-xx-xx
For example:00-40-C7-00-00-01

IP:

Four-byte IP Address: xxx-xxx-xxx-xxx
For example:192.168.1.1

Delete:

Check this ☒, then click **<Delete>** button to delete all entries.

Current User List					
No	Name	MAC	IP	Method	Type
Delete ☒	Binding Ports				
1	Test2	00-00-00-00-00-00	192.168.1.102	IP	Static
☒ 2	Test1	AA-BB-CC-11-22-33	192.168.1.101	IP-MAC	Static
☒ 1	Test3	AB-BC-AC-12-23-32	0.0.0.0	MAC	Static
☒ 3					
Add	Delete				

Page: 1

Fig. 3-18

Check this “☐”, then click **<Delete>** button to delete one entry.

Current User List

No	Name	MAC	IP	Method	Type
Delete ☐					
Binding Ports					
1	Test2	00-00-00-00-00-00	192.168.1.102	IP	Static
☒	2	Test1	AA-BB-CC-11-22-33	192.168.1.101	IP-MAC
☐	1	Test3	AB-BC-AC-12-23-32	0.0.0.0	MAC
3					Static
☐	3				
Add Delete					

Page: 1

Fig. 3-19

Binding Method:

Three kinds of binding methods (IP-MAC/IP/MAC) to be chosen.

Add:

Click **<Add>** button to create a new entry and input the relative settings, then click **<Apply>** button to take effect.

Current User List

No	Name	MAC	IP	Method	Type
Delete ☐					
Binding Ports					
(None)					
Add Delete					

Fig. 3-20

IP-MAC Binding User

Name	Test1
Binding Method	IP-MAC
MAC	aa - bb - cc - 11 - 22 - 33
IP	192.168.1.101
Port	1. ☒ 2. ☐ 3. ☐ 4. ☐ 5. ☐ 6. ☐ 7. ☐ 8. ☐ 9. ☐ 10. ☐
Apply cancel	

Fig. 3-21

Current User List

No	Name	MAC	IP	Method	Type
Delete ☐					
Binding Ports					
1	Test1	AA-BB-CC-11-22-33	192.168.1.101	IP-MAC	Static
☐	1				
Add Delete					

Page: 1

Fig. 3-22

3-5. Port Configuration

Five functions, including Port Status, Port Configuration, Port Description, Simple Counter and Detail Counter are contained in this function folder for port monitor and management. Each of them will be described in detail orderly in the following sections.

3-5-1.Port Status

The function Port Status gathers the information of all ports' current status and shows it by the order of port number, media, link status, port state, Auto-Negotiation status, speed/duplex, Rx Pause, Tx Pause. An extra media type information for the module ports 9 and 10 is also offered.

Function name:

Port Status

Function Description:

Show the latest updated status of all ports in this switch. When any one of the ports in the switch changes its parameter displayed in the page, it will be automatically refreshed the port current status about every 5 seconds.

Port Current Status

Port No	Media	Link	State	Auto Nego.	Speed/Duplex	Rx Pause	Tx Pause	Port Description
1	TP	Down	Enabled	Enabled	---/----	-----	-----	
2	TP	Up	Enabled	Enabled	100M/Full	On	On	
3	TP	Down	Enabled	Enabled	---/----	-----	-----	
4	TP	Down	Enabled	Enabled	---/----	-----	-----	
5	TP	Down	Enabled	Enabled	---/----	-----	-----	
6	TP	Down	Enabled	Enabled	---/----	-----	-----	
7	TP	Down	Enabled	Enabled	---/----	-----	-----	
8	TP	Down	Enabled	Enabled	---/----	-----	-----	
9	Fiber	Down	Enabled	Enabled	---/----	-----	-----	
10	TP	Down	Enabled	Enabled	---/----	-----	-----	

Fig. 3-23

Parameter Description:

Port No:

Display the port number. The number is 1 – 10.

Media:

Show the media type adopted in all ports. The Port 9 and Port 10 are optional modules, which support either fiber (1000Mbps) or UTP (10/100/1000Mbps).

Link:

Show the port is link up or link down. Up→Link up, Down→Link down

No default value.

State:

Show that the communication function of the port is “Enabled” or “Disabled”. When it is enabled, traffic can be transmitted and received via this port. When it is disabled, no traffic can be transferred through this port. Port State is configured by user.

Default: Enabled.

Auto Nego.:

Show the exchange mode of Ethernet MAC. There are two modes supported in the switch. They are auto-negotiation mode “Enabled” and forced mode “Disabled”. When in “Enabled” mode, this function will automatically negotiate by hardware itself and exchange each other the capability of speed and duplex mode with other site which is linked, and comes out the best communication way. When in “Disabled” mode, both parties must have the same setting of speed and duplex, otherwise, both of them will not be linked. In this case, the link result is “Down”.

Default: Enabled

Speed / Duplex :

Display the speed and duplex of all ports.

Port 1~8:

10M/Half, 10M/Full, 100M/Half, 100M/Full

Port 9~10:

TP→10M/Half, 10M/Full, 100M/Half, 100M/Full, 1G/Full

SFP(1G)→1G/Full

Default: None, depends on the result of the negotiation.

Rx Pause:

The way that the port adopts to process the PAUSE frame. If it shows “on”, the port will care the PAUSE frame; otherwise, the port will ignore the PAUSE frame. Default: None

Tx Pause:

It decides that whether the port transmits the PAUSE frame or not. If it shows “on”, the port will send PAUSE frame; otherwise, the port will not send the PAUSE frame. Default: None

Port Description:

Show the port description which user has defined.

Parameter Description of Port 9 and Port 10:

Port Current Status

Port No	Media	Link	State	Auto Nego.	Speed/Duplex	Rx Pause	Tx Pause	Port Description
1	TP	Down	Enabled	Enabled	---/----	-----	-----	
2	TP	Up	Enabled	Enabled	100M/Full	On	On	
3	TP	Down	Enabled	Enabled	---/----	-----	-----	
4	TP	Down	Enabled	Enabled	---/----	-----	-----	
5	TP	Down	Enabled	Enabled	---/----	-----	-----	
6	TP	Down	Enabled	Enabled	---/----	-----	-----	
7	TP	Down	Enabled	Enabled	---/----	-----	-----	
8	TP	Down	Enabled	Enabled	---/----	-----	-----	
9	Fiber	Down	Enabled	Enabled	---/----	-----	-----	
10	TP	Down	Enabled	Enabled	---/----	-----	-----	

Port 9 Detail Information

Connector Type	SFP - LC
Fiber Type	Reserved
Tx Central Wavelength	1310
Baud Rate	
Vendor OUI	00:0f:99
Vendor Name	APAC Opto
Vendor PN	LM38-A3S-TI-N
Vendor Rev	0000
Vendor SN	9806060378
Date Code	090825
Temperature [Degrees Centigrade]	none
Vcc [Volt]	none
Mon1 (Bias) [mA]	none
Mon2 (TX PWR) [dBm]	none
Mon3 (RX PWR) [dBm]	none

Close

Fig. 3-24

Connector Type:

Display the connector type, for instance: SFP-LC

Fiber Type:

Display the fiber mode, for instance, Multi-Mode, Single-Mode.

Tx Central Wavelength:

Display the fiber optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

Baud Rate:

Display the maximum baud rate of the fiber module supported, for instance, 100M, 1G and so on.

Vendor OUI:

Display the Manufacturer's OUI code which is assigned by IEEE.

Vendor Name:

Display the company name of the module manufacturer.

Vendor P/N:

Display the product name of the naming by module manufacturer.

Vendor Rev (Revision):

Display the module revision.

Vendor SN (Serial Number):

Show the serial number assigned by the manufacturer.

Date Code:

Show the date this module was made.

Temperature:

Show the current temperature of module.

Vcc:

Show the working DC voltage of module.

Mon1(Bias) mA:

Show the Bias current of module.

Mon2(TX PWR):

Show the transmit power of module.

Mon3(RX PWR):

Show the receiver power of module.

3-5-2. Port Configuration

Port Configuration is applied to change the setting of each port. In this configuration function, you can set/reset the following functions. All of them are described in detail below.

Function name:

Port Configuration

Function description:

It is used to set each port's operation mode. The switch supports 4 parameters for each port. They are State, Speed/Duplex, Flow Control and Power Saving.

Port Configuration

Port No	State	Speed/Duplex	Flow Control	Power Saving
1	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾
2	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾
3	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾
4	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾
5	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾
6	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾
7	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾
8	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾
9	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾
10	Enable ▾	Auto ▾	Symmetric ▾	Disable ▾

Apply

Fig. 3-25

Parameter description:

State:

Set the communication capability of the port is Enabled or Disabled. When enabled, traffic can be transmitted and received via this port. When disabled, the port is blocked and no traffic can be transferred through this port. Port State is configurable by the user. There are only two states "Enable" and "Disable" able to choose. If you set a port's state "Disable", then that port is prohibited to pass any traffic, even it looks Link up.

Default: Enable

Speed/Duplex:

Set the speed and duplex of the port. In speed, 10/100Mbps baud rate is available for Fast Ethernet, Gigabit module in port 9, 10. If the media is

1Gbps fiber, it is always 1000Mbps and the duplex is full only. If the media is TP, the Speed/Duplex is comprised of the combination of speed mode, 10/100/1000Mbps, and duplex mode, full duplex and half duplex. The following table summarized the function the media supports.

Media type	NWay	Speed	Duplex
100M TP	ON/OFF	10/100M	Full/Half
1000M TP	ON/OFF	10/100/1000M	Full for all, Half for 10/100
1000M Fiber	ON/OFF	1000M	Full

In Auto-negotiation mode, no default value. In Forced mode, default value depends on your setting.

Flow Control:

There are two modes to choose in flow control, including Symmetric and Disable. If flow control is set Symmetric, both parties can send PAUSE frame to the transmitting device(s) if the receiving port is too busy to handle. When it is set Disable, no flow control function.

Default: Symmetric.

Power Saving:

The parameter will enable or disable to verify switches have the ability to consider the length of any Ethernet cable connected for adjustment of power usage accordingly. Shorter lengths require less power. link-down mode removes power for each port that does not have a device attached.

Default: Disable.

3-5-3. Description

Function name:

Description

Function description:

Allow users to input the description for each port.

Port Description

Port	Description
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Fig. 3-26

Parameter description:

Port:

Port number.

Description:

The description for each port.

3-5-4. Simple Counter

The function of Simple Counter collects any information and provides the counting about the traffic of the port, no matter the packet is good or bad.

In the Fig. 3-27, the window can show all ports' counter information at the same time. Each data field has 20-digit long. If the counting is overflow, the counter will be reset and restart counting. The data is updated every time interval defined by the user. The valid range is 3 to 10 seconds. The Refresh Interval is used to set the update frequency. Default update time is 3 seconds.

Function name:

Simple Counter

Function description:

Display the summary counting of each port's traffic, including Tx Byte, Rx Byte, Tx Packet, Rx Packet, Tx Collision and Rx Error Packet.

Simple Counter

Refresh Interval 3 sec

Reset

Time elapsed since last reset: 0 Days 3 Hours 59 Mins 32 Secs

Port No	Tx Byte	Rx Byte	Tx Packet	Rx Packet	Tx Collision	Rx Error Packet
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	5264	0	46	0	0
9	0	0	0	0	0	0
10	5001922	4243114	19819	23784	0	0

Fig. 3-27

Parameter description:

Tx Byte:

Total transmitted bytes.

Rx Byte:

Total received bytes.

Tx Packet:

The counting number of the packet transmitted.

Rx Packet:

The counting number of the packet received.

Tx Collision:

Number of collisions transmitting frames experienced.

Rx Error Packet:

Rx Unicast Packets:

The number of received unicast packet.

Rx Broadcast Packets:

The number of received broadcast packet.

Rx Multicast Packets:

The number of received multicast packet.

Rx Pause Packets:

The number of received pause packet.

Tx Collisions:

The number of collisions transmitting frames experienced.

Tx Single Collision:

The number of frames transmitted that experienced exactly one collision.

Tx Multiple Collision:

The number of frames transmitted that experienced more than one collision.

Tx Drop Packets:

The number of frames dropped due to excessive collision, late collision, or frame aging.

Tx Deferred Transmit:

The number of frames delayed to transmission due to the medium is busy.

Tx Late Collision:

The number of times that a collision is detected later than 512 bit-times into the transmission of a frame.

Tx Excessive Collision:

The number of frames that are not transmitted because the frame experienced 16 transmission attempts.

Packets 64 Octets:

The number of 64-byte frames in good and bad packets received.

Packets 65-127 Octets:

The number of 65 ~ 127-byte frames in good and bad packets received.

Packets 128-255 Octets:

The number of 128 ~ 255-byte frames in good and bad packets received.

Packets 256-511 Octets:

The number of 256 ~ 511-byte frames in good and bad packets received.

Packets 512-1023 Octets:

The number of 512 ~ 1023-byte frames in good and bad packets received.

Packets 1024-1522 Octets:

The number of 1024-1522-byte frames in good and bad packets received.

Tx Packets:

The number of packet transmitted.

Tx Octets:

Total transmitted bytes.

Tx Unicast Packets:

The number of transmitted unicast packet.

Tx Broadcast Packets:

The number of transmitted broadcast packet.

Tx Multicast Packets:

The number of transmitted multicast packet.

Tx Pause Packets:

The number of transmitted pause packet.

Rx FCS Errors:

The number of bad FSC packets received.

Rx Alignment Errors:

The number of Alignment errors packets received.

Rx Fragments:

The number of short frames (< 64 bytes) with invalid CRC.

Rx Jabbers:

The number of long frames(according to max length register) with invalid CRC.

Rx Drop Packets:

The frames dropped due to lack of receiving buffer.

Rx Undersize Packets:

The number of short frames (<64 Bytes) with valid CRC.

Rx Oversize Packets:

The number of long frames(according to max length register) with valid CRC.

3-6. Loop Detection

Function name:

Loop Detection

Function description:

This function is used to detect loops by LDCP (Loop Detection Control Protocol), and unlock them.

Loop Detection

Port No	State	Current Status	Resume Action
1	Disable ▾	Unlocked	☐ Unlock
2	Disable ▾	Unlocked	☐ Unlock
3	Disable ▾	Unlocked	☐ Unlock
4	Disable ▾	Unlocked	☐ Unlock
5	Disable ▾	Unlocked	☐ Unlock
6	Disable ▾	Unlocked	☐ Unlock
7	Disable ▾	Unlocked	☐ Unlock
8	Disable ▾	Unlocked	☐ Unlock
9	Disable ▾	Unlocked	☐ Unlock
10	Disable ▾	Unlocked	☐ Unlock
Action	☒ Enable		

Fig. 3-29

Parameter description:

Port No: Display the Port Number. The number is 1-10.

State – Disable / Enable:

When Port No. is chosen, and enable port's loop detection, the port can detect loop happens. When detects loop happen, port will be locked else port maintains unlocked.

Default: Disable

Current Status:

Display Loop Detection current status as Unlocked or Locked.

Locked Port-Resume:

Users may check “Unlock” to resume the action.

Action:

Users may check “Action” to activate Loop Detection function.

3-7. SNMP Configuration

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP “Enable”, SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set “Disable”, SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

3-7-1. EngineID

Function name:

SNMP EngineID

Function description:

Enable or disable SNMP function.

SNMP EngineID

SNMP	☒ Enable ☐ Disable
Engine ID:	80001455030040C7F8B00A
EngineBoots	1

Apply

Fig. 3-7-1 SNMP EngineID setting

Parameter description:

SNMP:

Enable: Enable SNMP operation.

Disable: Disable SNMP operation.

Default: Enable.

Engine ID:

To set the SNMPv3 engine ID. syntax: 0-9,a-f,A-F, min 5 bytes, max 32 bytes,the fifth byte can't input 00. IF change the Engine ID that will clear all original user.

EngineBoots:

To display the EngineBoots.

3-7-2. SNMP Community

Function name:

SNMP Community

Function description:

To set SNMP community entry.

Parameter description:

Add new community:

Step 1: To click **<Add new community>** button, then input relative data.

Step 2: To click **<Apply>** button.

Community: Max. up to 32 characters.

UserName: Max. up to 32 characters

Source IP: IPv4, xxx.xxx.xxx.xxx

Source Mask: xxx.xxx.xxx.xxx

SNMPv1/v2 Communities to Security Configuration

Delete	Community	UserName	Source IP	Source Mask
Delete	private	operator	192.168.11.16	255.255.255.0

Add new community **Apply**

Fig. 3-7-3

Delete community:

Step: To click **<Delete>** button.

SNMPv1/v2 Communities to Security Configuration

Delete	Community	UserName	Source IP	Source Mask
Delete	public	admin	192.168.11.16	255.255.255.0

Add new community **Apply**

Fig. 3-7-4

3-7-3. Users

Function name:

Users

Function description:

To set SNMP users.

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Add new user Apply						

Fig. 3-7-5

Parameter description:

Add new user:

Step 1: To click **<Add new user>** button, then input relative data.

Step 2: To click **<Apply>** button.

UserName: Max. up to 32 characters.

Security Level: NoAuthNoPriv, AuthNoPriv or AuthPriv

Authentication Protocol: MD5 or SHA

Authentication Password: 8-32 characters

Privacy Protocol: DES

Privacy Password: 8-32 characters

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Add new user Apply						

Fig. 3-7-6

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	TestUser	Auth, Priv	MD5	••••••••	DES	••••••••
Add new user Apply						

Fig. 3-7-7

Delete user: To click <Delete> button.

SNMPv3 Users Configuration

Delete	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
Delete	TestUser	Auth, Priv ▼	MD5 ▼	●●●●●●●●	DES ▼	●●●●●●●●

Add new user **Apply**

Fig. 3-7-8

3-7-4. Group

Function name:

Group

Function description:

To set SNMP group entry.

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
Add new group Apply			

Fig. 3-7-9

Parameter description:

Add new group:

Step 1: To click **<Add new group>** button, then input relative data.

Step 2: To click **<Apply>** button.

Security Model: v1, v2c, usm.

Security Name: Have been set in SNMP community "UserName"

Group Name: Max. up to 32 characters

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
Add new group Apply			

Fig. 3-7-9

SNMPv3 Groups Configuration

Delete	Security Model	Security Name	Group Name
Delete	v1	admin	ForChecking
Add new group Apply			

Fig. 3-7-10

Delete group: To click **<Delete>** button.

3-7-5. View

Function name:

View

Function description:

To set SNMP view entry.

SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
Add new view Apply			

Fig. 3-7-11

Parameter description:

Add new view:

Step 1: To click **<Add new view>** button, then input relative data.

Step 2: To click **<Apply>** button.

View Name: Max. up to 32 characters.

View Type: included or excluded

OID Subtree: The OID defining the root of the subtree to add to the named view.

SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
Add new view Apply			

Fig. 3-7-12

SNMPv3 Views Configuration

Delete	View Name	View Type	OID Subtree
Delete	operator	included	23567
Add new view Apply			

Fig. 3-7-13

Delete view: To click **<Delete>** button.

3-7-6. Access

Function name:

Access

Function description:

To set SNMP access entry.

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
Add new access Apply					

Fig. 3-7-14

Parameter description:

Add new access: (After Group Name has been set)

Step 1: To click **<Add new access>** button, then input relative data.

Step 2: To click **<Apply>** button.

Group Name: Max. up to 32 characters(Have been set in Add Group).

Security Model: Any, v1, v2c, usm

Security Level: NoAuthNoPriv, AuthNoPriv or AuthPriv

Read View Name: None or Group Name

Write View Name: None or Group Name

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
Add new access Apply					

Fig. 3-7-15

SNMPv3 Accesses Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
Delete	Tracking	any	Auth, NoPriv	Tracking	Tracking
Add new access Apply					

Fig. 3-7-16

Delete access: To click **<Delete>** button.

3-7-7. Trap Host Config

Function name:

Trap Host Config

Function description:

To set SNMP Trap Configuration.

Trap Host Configuration

No	State	Version	Security	Authentication Protocol	Community/Security Name	
	IP	Port	Authentication Password	Privacy Password		
1	Disable	V1 162				Edit
2	Disable	V1 162				Edit
3	Disable	V1 162				Edit
4	Disable	V1 162				Edit
5	Disable	V1 162				Edit
6	Disable	V1 162				Edit

Note : Privacy protocol always is DES

Fig. 3-7-17

Parameter description:

Edit:

Step 1: To click **<Edit>** button, then input relative data.

Step 2: To click **<Apply>** button to take effect.

To click **<Back>** button to the previous screen.

Trap Host Configuration

State	Enable ▾
Version	v1 ▾
IP	192.168.11.16
Port	162
Community/Security Name	public
Security	NoAuthNoPriv ▾
Authentication Protocol	MD5 ▾
Authentication Password	
Privacy Password	

Apply Back

Fig. 3-7-18

State:

Enable: Enable SNMP trap.

Disable: Disable SNMP trap.

Default: Disable

Version:

Version of SNMP.

Default: v1

Port:

SNMP port number.

Default: 162

Security:

It will be set when v3 was selected.

3-8. DHCP Boot

The DHCP Boot function is used to spread the request broadcast packet into a bigger time frame to prevent the traffic congestion due to broadcast packets from many network devices which may seek its NMS, boot server, DHCP server and many connections predefined when the whole building or block lose the power and then reboot and recover. At this moment, a bunch of switch or other network device on the LAN will try its best to find the server to get the services or try to set up the predefined links, they will issue many broadcast packets in the network.

The switch supports a random delay time for DHCP and boot delay for each device. This suppresses the broadcast storm while all devices are at booting stage in the same time. The maximum user-defined delay time is 30 seconds. If DHCP Broadcasting Suppression function is enabled, the delay time is set randomly, ranging from 0 to 30 seconds, because the exactly delay time is computed by the switch itself. The default is "Disable".

DHCP Boot

DHCP Broadcast Suppression	Disable	Delay Time	30	(1-30 seconds)
----------------------------	--	------------	---------------------------------	----------------

Fig. 3-31

3-9. Multicast

The function is used to establish the multicast groups to forward the multicast packet to the member ports, and, in nature, avoids wasting the bandwidth while IP multicast packets are running over the network. This is because a switch that does not support IGMP or IGMP Snooping can not tell the multicast packet from the broadcast packet, so it can only treat them all as the broadcast packet. Without IGMP Snooping, the multicast packet forwarding function is plain and nothing is different from broadcast packet.

A switch supported IGMP Snooping with the functions of query, report and leave, a type of packet exchanged between IP Multicast Router/Switch and IP Multicast Host, can update the information of the Multicast table when a member (port) joins or leaves an IP Multicast Destination Address. With this function, once a switch receives an IP multicast packet, it will forward the packet to the members who joined in a specified IP multicast group before.

The packets will be discarded by the IGMP Snooping if the user transmits multicast packets to the multicast group that had not been built up in advance.

3-9-1. IGMP Mode

Function name:

IGMP Mode

Function description:

IGMP mode is used to enable IGMP with either snooping , proxy or disable mode.



Fig. 3-32

Parameter description:

IGMP mode selection:

The switch supports to enable IGMP mode function

Disable: To disable IGMP

Proxy: To set IGMP mode as IGMP Proxy

Snooping: To set IGMP mode as IGMP Snooping

3-9-2. Proxy

Function name:

Proxy

Function description:

Proxy is used to IGMP Proxy setting the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. Enabling IGMP with either passive or active mode, you can monitor the IGMP Proxy information, which contains the multicast member list with the multicast groups, VID and member port.

IGMP Proxy Configuration

Unregister Multicast Flooding	☒ Enable
General Query Interval	125 (3 - 2000 sec)
General Query Max Response Time	10 (1 - 10 sec)
General Query Timeout	11 (2 - 30 sec)
Specific Query Count	2 (1 - 10 times)
Specific Query Max Response Time	1 (1 - 10 sec)
Specific Query Timeout	2 (2 - 30 sec)

Port	Multicast Group Limit	IGMP Router	Port	Multicast Group Limit	IGMP Router
1	256	☒	2	256	☐
3	256	☐	4	256	☐
5	256	☐	6	256	☐
7	256	☐	8	256	☐
9	256	☐	10	256	☐

Apply

Fig. 3-33

Parameter description:

IGMP Proxy mode selection:

Unregistered Multicast Flooding :

The switch supports to enable Unregistered Multicast Flooding function

Enable:

General Query Interval :

The general query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet).

Available value: 3-2000 sec

Default: 125

General Query Max Response Time :

The Maximum Response Time field is only used in general or group-

specific query messages. The Maximum Response Time is configured as the value for the Query response interval setting

Available value: 1-10 sec

Default:10

General Query Timeout :

The General Query Timeout field is the amount of time in seconds.

Available value: 2-30 sec

Default:11

Specific Query Count :

To set Specific Query Count on Switch .

Available value: 1-10 times

Default:2

Specific Query Max Response Time :

To set the specific Query Response Time field is used in specific or group-specific query messages. The Specific Maximum Response Time is configured as the value.

Available value: 1-10 sec

Default:1

Specific Query Timeout :

The Specific Query Timeout field is the amount of time in seconds.

Available value: 2-30 sec

Default:2

Multicast Group Limit :

The Multicast Group Limit field is the amount of Multicast Group.

Default:256

IGMP Router :

The IGMP Router to evoke the port become an IGMP Router port .

3-9-3. Snooping

Function name:

Snooping

Function description:

Snooping is used to IGMP Snooping the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. Enabling IGMP with either passive or active mode, you can monitor the IGMP snooping information, which contains the multicast member list with the multicast groups, VID and member port.

IGMP Snooping Configuration

Host Time Out (1 - 65535 sec)

Port	Multicast Group Limit	IGMP Router	Fast Leave	Port	Multicast Group Limit	IGMP Router	Fast Leave
1	256	☒	☐	2	256	☐	☐
3	256	☐	☐	4	256	☐	☐
5	256	☐	☐	6	256	☐	☐
7	256	☐	☐	8	256	☐	☐
9	256	☐	☐	10	256	☐	☒

Fig. 3-34

Parameter description:

Host Time Out:

To set the IGMP Snooping enable and the Host packet received by switch timeout period.

Available value: 1-65535 sec

Default:120

Multicast Group Limit :

The Multicast Group Limit field is the amount of Multicast Group.

Default value:256

Router Ports:

To set which port want to be a Router Port with IGMP snooping mode.

Fast Leave:

To set which port want to enable the Fast leave mode with IGMP snooping mode.

3-9-4. IGMP VLAN

Function name:

IGMP VLAN

Function description:

Specify a static connection to a multicast router for the VLAN.

IGMP VLAN

VID		Add
Index	VID	
Delete		

Fig. 3-35

Parameter description:

VID:(VLAN mode has to be set in Tag-based)

To set an IGMP snooping VLAN ID for each multicast group.

The valid VID range is 1~4094.

Add:

Step 1: To enable IGMP Snooping function then click **<Apply>** button.

IGMP Mode

IGMP Mode	Snooping ▼
Apply	

Fig. 3-36

Step 2 : To input a new VID and click **<Add>** button (Fig. 3-9-6), then show as Fig. 3-9-7.

IGMP VLAN

VID	2
Add	
Index	VID
Delete	

Fig. 3-37

IGMP VLAN

VID

Add

Index	VID
1	2

Delete

Fig. 3-38

Delete:

To select an existed entry then click **<Delete>** button.

IGMP VLAN

VID

Add

Index	VID
1	1
2	3
3	4094

Delete

Fig. 3-39

3-9-5. Group Allow

Function name:

Group Allow

Function description:

The Allowed Group function allows the IGMP Snooping to set up the IP multicast table based on user's specific conditions. IGMP report packets that meet the items you set up will be joined or formed the multicast group.

Group Allow

VID 0	Start Address		End Address							
	Port Member									
	1. ☐	2. ☐	3. ☐	4. ☐	5. ☐	6. ☐	7. ☐	8. ☐		
	9. ☐	10. ☐	Select/Unselect All ☐							

Index	Start Address	End Address	VID	Port Member
1	239.200.1.1	239.200.1.20	0	10

Fig. 3-40

Parameter description:

Start Address/End Address:

Input the suitable IP address.

The valid range is 224.0.0.0~239.255.255.255.

VID:

To show the IGMP VLAN which you have set.

The valid VID range is 1~4094.

Port Member:

You can select the ports that you would like them to be worked and restricted in the allowed group configuration.

(a) One by one selection:

Group Allow

VID 1	Start Address		End Address							
	Port Member									
	1. ☒	2. ☐	3. ☐	4. ☐	5. ☐	6. ☐	7. ☐	8. ☐		
	9. ☐	10. ☐	Select/Unselect All ☐							

Fig. 3-41

(b) Select All

Group Allow

VID 1	Start Address		End Address	
	Port Member			
1. ☒	2. ☒	3. ☒	4. ☒	5. ☒
6. ☒	7. ☒	8. ☒	Select/Unselect All ☒	
9. ☒	10. ☒			

Add

Fig. 3-42

(c) Unselect All

Group Allow

VID 1	Start Address		End Address	
	Port Member			
1. ☐	2. ☐	3. ☐	4. ☐	5. ☐
6. ☐	7. ☐	8. ☐	Select/Unselect All ☐	
9. ☐	10. ☐			

Add

Fig. 3-43

Add:

Step 1: To select an IGMP VLAN which you have set.

Group Allow

Step 1

VID 3	Start Address		End Address	
	Port Member			
1. ☐	2. ☐	3. ☐	4. ☐	5. ☐
6. ☐	7. ☐	8. ☐	Select/Unselect All ☐	
9. ☐	10. ☐			

Add

Fig. 3-44

Step 2: To input "Start Address" and "End Address".

Step 3: To select "Port Member" then click **<Add>** button.

Group Allow

VID 3

Start Address: 224.0.0.1 End Address: 224.0.0.10

Port Member

1. ☒ 2. ☒ 3. ☒ 4. ☐ 5. ☐ 6. ☒ 7. ☒ 8. ☐
 9. ☒ 10. ☒ Select/Unselect All ☐

Step 2

Step 3

Add

Index	Start Address	End Address	VID	Port Member
1	239.200.1.1	239.200.1.20	0	10
2	239.200.0.30	239.200.0.60	0	1,3,5,7
3	239.200.0.80	239.200.0.90	3	8,9,10

Delete

Fig. 3-45

A new entry of “Group Allow” configuration can be created (Fig. 3-9-15).

Group Allow

VID 3

Start Address: End Address:

Port Member

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐ 6. ☐ 7. ☐ 8. ☐
 9. ☐ 10. ☐ Select/Unselect All ☐

Add

Index	Start Address	End Address	VID	Port Member
1	239.200.1.1	239.200.1.20	0	10
2	239.200.0.30	239.200.0.60	0	1,3,5,7
3	239.200.0.80	239.200.0.90	3	8,9,10
4	224.0.0.1	224.0.0.10	3	1,2,3,6,7,9,10

Delete

Fig. 3-46

Delete:

To remove the existed entry of “Group Allow” configuration.

STEP: To select an existed entry, then click <Delete> button.

Group Allow

VID 3

Start Address: End Address:

Port Member

1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐ 6. ☐ 7. ☐ 8. ☐
 9. ☐ 10. ☐ Select/Unselect All ☐

Add

Index	Start Address	End Address	VID	Port Member
1	239.200.1.1	239.200.1.20	0	10
2	239.200.0.30	239.200.0.60	0	1,3,5,7
3	239.200.0.80	239.200.0.90	3	8,9,10
4	224.0.0.1	224.0.0.10	3	1,2,3,6,7,9,10

Delete

Fig. 3-47

Group Allow

VID
3

Start Address

End Address

Port Member

1. 2. 3. 4. 5. 6. 7. 8. 9. 10. Select/Unselect All

Add

| Index | Start Address | End Address | VID | Port Member |
|-------|---------------|--------------|-----|----------------|
| 1 | 239.200.1.1 | 239.200.1.20 | 0 | 10 |
| 2 | 239.200.0.30 | 239.200.0.60 | 0 | 1,3,5,7 |
| 3 | 224.0.0.1 | 224.0.0.10 | 3 | 1,2,3,6,7,9,10 |

Delete

Fig. 3-48

3-9-6. Multicast Status

Function name:

Multicast Status

Function description:

The Multicast Status function allows to display the switch received multicast traffic status. If the switch doesn't receive any multicast traffic then it will display the "No multicast entry !"

No multicast entry!

| Multicast Status | | | |
|------------------|-----|-----------------|-------------|
| Index | VID | Multicast Group | Port Member |

Fig. 3-49

Parameter description:

Index:

To display current built-up multicast group entry index.

VID:

To display current built-up multicast VLAN ID .

Multicast Group :

To display current built-up multicast Group Address

Port Members:

To display current built-up multicast port members .

Previous Page:

To display previous page context.

Next Page:

To display next page context.

Refresh:

To Update multicast group membership.

3-9-7. MVR Setting

Function name:

MVR Setting

Function description:

Multicast VLAN Registration (MVR) routes packets received in a multicast source VLAN to one or more receive VLANs. Clients are in the receive VLANs and the multicast server is in the source VLAN. Multicast routing has to be disabled when MVR is enabled. Refer to the configuration guide at Understanding Multicast VLAN Registration for more information on MVR..

MVR Setting

| | |
|-----------------------------|--|
| Multicast VLAN Registration | ☒ Enable |
| Multicast VLAN ID | 2 |
| Host Time Out | 125 |

| Port | Service Type | Tagging | Fast Leave | Port | Service Type | Tagging | Fast Leave |
|------|--------------|--------------------------|--------------------------|------|--------------|-------------------------------------|--------------------------|
| 1 | None | ☐ | ☐ | 2 | None | ☐ | ☐ |
| 3 | None | ☐ | ☐ | 4 | None | ☐ | ☐ |
| 5 | None | ☐ | ☐ | 6 | None | ☐ | ☐ |
| 7 | None | ☐ | ☐ | 8 | None | ☐ | ☐ |
| 9 | None | ☐ | ☐ | 10 | Router | ☒ | ☐ |

Apply

Fig. 3-50

Parameter description:

Multicast VLAN Registration:

To Set the multicast VLAN registration function enable.

Multicast VLAN ID:

To Set the multicast VLAN ID.

Available Value:2~4094, 1 reserved for default VLAN.

Host Time Out:

To set the IGMP Snooping enable and the Host packet received by switch timeout period.

Available Value:1 ~ 65535.

Default:125 seconds

Port No:

Display the port number. The number is 1 – 10.

Service Type:

To elect the service type which has three types include “None”, “ Client” and “ Router”

Tagging:

To elect port tag-out or not.

Fast Leave:

To set which port want to enable the “Fast Leave” mode with IGMP snooping mode.

3-9-8. MVR Group Allow

Function name:

MVR Group Allow

Function description:

The Group Allow function allows the multicast VLAN Registration to set up the IP multicast group filtering conditions. IGMP join behavior that meet the items you set up will be joined or formed the multicast group.

Parameter description:

Add:

Step : To input “Start Address”, “End Address”, “Port Member” and select a MVID, then click **<Add>** button.

IP Address Range:

The valid range is 224.0.0.0~239.255.255.255.

MVID:

It has been set in group allow.

MVR Group Allow

| | | | | | | | | |
|-------------|--|--|--|--|--|-----------------------------|-----------------------------|-----------------------------|
| MVID
3 ▼ | Start Address | | End Address | | | | | |
| | <input type="text" value="239.200.1.1"/> | | <input type="text" value="239.200.1.20"/> | | | | | |
| | Port Member | | | | | | | |
| | 1. ☒ | 2. ☒ | 3. ☒ | 4. ☒ | 5. ☒ | 6. ☐ | 7. ☐ | 8. ☐ |
| | 9. ☐ | 10. ☐ | Select/Unselect All ☐ | | | | | |

Add

| Index | Start Address | End Address | VID | Port Member |
|-------|---------------|-------------|-----|-------------|
| | | | | |

Delete

Fig. 3-51

MVR Group Allow

| | | | | | | | | |
|-------------|-----------------------------|------------------------------|--|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| MVID
3 ▼ | Start Address | | End Address | | | | | |
| | <input type="text"/> | | <input type="text"/> | | | | | |
| | Port Member | | | | | | | |
| | 1. ☐ | 2. ☐ | 3. ☐ | 4. ☐ | 5. ☐ | 6. ☐ | 7. ☐ | 8. ☐ |
| | 9. ☐ | 10. ☐ | Select/Unselect All ☐ | | | | | |

Add

| Index | Start Address | End Address | VID | Port Member |
|-------|---------------|--------------|-----|-------------|
| 1 | 239.200.1.1 | 239.200.1.20 | 3 | 1,2,3,4,5 |

Delete

Fig. 3-52

3-9-9. MVR Multicast Status

Function name:

MVR Multicast Status

Function description:

The MVR Multicast Status function allows to display the switch received MVR multicast traffic status. If the switch doesn't receive any MVR multicast traffic then it will display the "No MVR multicast entry !"

| No mvr multicast entry! | | | |
|-------------------------|-----|-----------------|-------------|
| MVR Multicast Status | | | |
| Index | VID | Multicast Group | Port Member |

Fig. 3-53

Parameter description:

Index:

To display current built-up multicast group entry index.

VID:

To display current built-up multicast VLAN ID .

Multicast Group :

To display current built-up multicast Group Address

Port Members:

To display current built-up multicast port members .

Previous Page:

To display previous page context.

Next Page:

To display next page context.

Refresh:

To Update multicast group membership.

3-9-10. RADIUS IGMP

Function name:

RADIUS IGMP

Function description:

The RADIUS IGMP function allows to some multicast applications, such as IPTV and Internet Radio, may be of minimal interest to law enforcement agencies, other multicast traffic may contain information important to an investigation. The problem of not intercepting incoming multicast traffic affects not only targets directly intercepted by IP address, but also targets intercepted by login name, calling line identity, MAC address, and similar identities used by such protocols as RADIUS and DHCP for authentication and dynamic IP allocation.

A lawful interception solution that analyzes RADIUS and DHCP for target IP addresses will likely fail to intercept incoming multicast traffic to the target.

RADIUS-IGMP Setting

| | |
|-----------------------|-------------|
| Radius Server 1 | 192.168.1.1 |
| Port Number(1~65535) | 1812 |
| Radius Server 2 | 192.168.1.1 |
| Port Number(1~65535) | 1812 |
| Secret Key | Radius |
| Accounting Server 1 | 192.168.1.1 |
| Port Number(1~65535) | 1813 |
| Accounting Server 2 | 192.168.1.1 |
| Port Number(1~65535) | 1813 |
| Secret Key | Radius |
| Response Timeout | 2 |
| Number of Retry | 1 |

| | |
|-------------|---|
| Port Member | ☐ 01 ☐ 02 ☐ 03 ☐ 04 ☐ 05 |
| | ☐ 06 ☐ 07 ☐ 08 ☐ 09 ☐ 10 |
| | ☐ Select/Unselect All |

Apply

Fig. 3-54

Parameter description:

Radius Server 1 and 2:

RADIUS server 1 and 2 IP address for authentication.

Default: 192.168.1.1

Port Number:

The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535.

Default:1812

Secret Key:

The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense. It is not allowed for putting a blank between any two characters.

Default: Radius

Response Timeout:

A timeout condition in the exchange between the authenticator and the authentication server. The valid range: 1 –65535.

Default: 2 seconds

Number of Retry (1-10):

The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 – 10.

Default: 1 time

Port Members:

To set the RADIUS IGMP multicast port members .

3-10. LLDP

The Link Layer Discovery Protocol (LLDP) provides a standards-based method for enabling switches to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

3-10-1. LLDP Configuration

Function name:

LLDP Configuration

Function description:

The LLDP configuration function, you can set per port the LLDP configuration and the detail parameters, the settings will take effect immediately.

LLDP Configuration

| | | |
|-----------------------|----|---------------------|
| Tx Interval | 30 | (5 - 32768 seconds) |
| Tx Hold | 4 | (2 - 10 times) |
| Tx Delay | 2 | (1 - 8192 seconds) |
| Tx Reinit | 2 | (1 - 10 seconds) |
| Notification Interval | 5 | (5 - 3600 seconds) |

| Port | Mode | Optional TLVs | | | | | Notification |
|------|------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| | | Port Descr | Sys Name | Sys Descr | Sys Capa | Mgmt Addr | |
| 1 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |
| 2 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |
| 3 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |
| 4 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |
| 5 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |
| 6 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |
| 7 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |
| 8 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |
| 9 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |
| 10 | Disabled ▾ | ☒ | ☒ | ☒ | ☒ | ☒ | ☐ |

Apply

Fig. 3-55 LLDP parameter

Parameter description:

Tx Interval:

To change the interval between consecutive transmissions of LLDP advertisements on any given port.

Available value:5~32768

Default: 30 seconds

Tx Hold:

To specify the amount of time the receiving device holds a LLDP packet before discarding it.

Available value: 2~10 times

Default: 4 times

Tx Delay:

To specify the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB.

Available value: 1~8192 seconds

Default: 2 seconds

Tx Reinit:

To specify the minimum time an LLDP port waits before reinitializing LLDP transmission.

Available value: 1~10 seconds

Default: 2 seconds

Notification Interval:

A network management application can periodically check the switch MIB to detect any missed change notification traps. Refer to IEEE 802.1AB-2005 or later for more information.

Available value: 5~3600 seconds

Default: 5 seconds

Mode:

To enable or disable the LLDP mode per port Including "Disabled", "Tx_Rx", "Tx only" and "Rx only".

Default: Disabled

Port Descr:

To evoke the outbound LLDP advertisements, includes an alphanumeric string describing the port.

Sys Name:

To evoke the outbound LLDP advertisements, includes the system's assigned name.

Sys Descr:

To evoke outbound LLDP advertisements, includes an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application.

Sys Capa:

To evoke outbound advertisements, includes a bitmask of system capabilities (device functions) that are supported. Also includes information on whether the capabilities are enabled.

Mgmt Addr:

To evoke outbound advertisements, includes information on management address. You can use to include a specific IP address in the outbound LLDP advertisements for specific ports.

Notification:

To evoke outbound advertisements, includes information on notification.

3-10-2. LLDP Neighbor Information

Function name:

LLDP Neighbor Information

Function description:

The LLDP Neighbor Information function allows a switch to display each port which build the LLDP available entry. This information can be useful in tracking LLDP packets back to a physical port and enable or disable the LLDP.

| LLDP Neighbor Information | | | | | | |
|---|------------|----------------|-------------|------------------|---------------------|--------------------|
| | | | | Refresh Interval | 3 sec | |
| Local Port | Chassis ID | Remote Port ID | System Name | Port Description | System Capabilities | Management Address |
| There is no entry for LLDP remote table | | | | | | |

Fig. 3-56 LLDP Entry

Parameter description:

Local port:

To display the switch local port.

Chassis ID:

To display the Chassis ID which connect to the switch and what the neighbor Chassis ID.

Remote Port ID:

To display the Remote Port ID which connect to the switch and what the neighbor's remote port ID.

System name:

To display the system name which connect to the switch and which device supports the LLDP

Port Description:

To display an alphanumeric string describing the full name and version identification for the system's hardware type, software version, and networking application

System Capabilities:

To display an includes a bitmask of system capabilities (device functions) that are supported. Also includes information on whether the capabilities are enabled.

Management Address:

To display include a specific IP address in the outbound LLDP advertisements for specific ports.

Refresh Interval:

Available values from 3 to 10 seconds.

3-10-3. LLDP Statistics

Function name:

LLDP Statistics

Function description:

Display the detailed counting number of each port's LLDP traffic.

LLDP Statistics

Refresh Interval3 sec

Neighbor Entries List Last Updated: 0 Days 1 Hours 22 Mins 33 Secs

Reset

| Global Counters | |
|----------------------------------|---|
| Total Neighbors Entries Added | 0 |
| Total Neighbors Entries Deleted | 0 |
| Total Neighbors Entries Dropped | 0 |
| Total Neighbors Entries Aged Out | 0 |

| Local Counters | | | | | | | |
|----------------|-----------|-----------|-----------|------------------|----------------|-------------------|----------|
| Local Port | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Age-Outs |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Fig. 3-57 LLDP statistics

Parameter description:

Neighbor Entries List Last Updated:

The time period which neighbor entries list were updated.

Total Neighbors Entries Added:

The “total neighbors entries added” were received.

Total Neighbors Entries Deleted:

The “total neighbors entries deleted” were received.

Total Neighbors Entries Dropped:

The “total neighbors entries dropped” were received.

Total Neighbors Entries Aged Out:

The “total neighbors entries aged out” were received.

Local port:

Show the local port on the switch.

Tx Frames:

The number of frames transmitted.

Rx Frames:

The number of frames received.

Rx Errors:

The number of received frames errors.

Frames Discarded:

The number of frame discarded.

TLVs Discarded:

The number of TLVs discarded.

TLVs Unrecognized:

The number of TLVs unrecognized.

Age-Outs:

The number of "Age-Outs".

3-11. VLAN

The switch supports Tag-based VLAN (802.1q) and Port-based VLAN. Support 256 active VLANs and VLAN ID 1~4094. VLAN configuration is used to partition your LAN into small ones as your demand. Properly configuring it, you can gain not only improving security and increasing performance but greatly reducing VLAN management.

3-11-1. VLAN Mode

Function name:

VLAN Mode Setting

Function description:

The VLAN Mode Selection function includes three modes: Port-based, Tag-based and Metro Mode. You can choose one of them by pulling down list. Then, click **<Apply>** button, the settings will take effect immediately.

VLAN Mode

| | |
|----------------|---------------------------------------|
| VLAN Mode | Tag-based ▼ |
| | Tag-based
Port-based
Metro Mode |
| Symmetric Vlan | |
| SVL | Disable ▼ |
| Double Tag | Disable ▼ |
| Up-Link Port | 10 Port ▼ |

Apply

Fig. 3-58

Parameter description:

VLAN Mode:

Tag-based:

This is the default setting.

Tag-based VLAN identifies its member by VID. This is quite different from port-based VLAN. If there are any more rules in ingress filtering list or egress filtering list, the packet will be screened with more filtering criteria to determine if it can be forwarded. The switch supports supplement of IEEE802.1q.

Each tag-based VLAN you built up must be assigned VLAN name and VLAN ID. Valid VLAN ID is 1-4094. User can create total up to 256 Tag VLAN groups.

Port-based:

Port-based VLAN is defined by port. Any packet coming in or outgoing from any one port of a port-based VLAN will be accepted. No filtering criterion applies in port-based VLAN. The only criterion is the physical port you connect to. For example, for a port-based VLAN named PVLAN-1 contains port members Port 1&2&3&4. If you are on the port 1, you can communicate with port 2&3&4. If you are on the port 5, then you cannot talk to them. Each port-based VLAN you built up must be assigned a group name. This switch can

support up to maximal 10 port-based VLAN groups.

Metro Mode:

The Metro Mode is a quick configuration VLAN environment method on Port-based VLAN. It will create 9 or 10 Port-based VLAN groups.

Symmetric Vlan:

This is an Ingress Rule (Rule 1, The Ingress Filtering Rule 1 is “forward only packets with VID matching this port’s configured VID”). For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Symmetric-Vlan function is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped.

Note: If Symmetric is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, the packet then will be forwarded. But if the PVID of port 1 is not 100, the packet will be dropped.

SVL:

While SVL is enable, all VLANs use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. While SVL is disable, it means learning mode is IVL. In this mode, different VLAN uses different filtering database storing the membership information of the VLAN to learn or look up the information of a VLAN member.

Double Tag:

Double-tag mode belongs to the tag-based mode, however, it would treat all frames as the untagged ones, which means that tag with PVID will be added into all packets. Then, these packets will be forwarded as Tag-based VLAN. So, the incoming packets with tag will become the double-tag ones.

Up-link Port:

This function is enabled only when metro mode is chosen in VLAN mode.

9 Port:

Except Port 9, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 9, thus, total 8 groups consisting of 2 members are formed.

10 Port:

Except Port 10, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 10, thus, total 8 groups consisting of 2 members are formed.

9 and 10 Port:

Except Port 9 and Port 10, each port of the switch cannot transmit packets with each other. Each port groups a VLAN with Port 9 and Port 10, thus total 8 groups consisting of 3 members are formed.

3-11-2. Tag-based Group

Function name:

Tag-based Group Configuration

Function description:

It shows the information of existed Tag-based VLAN Groups. You can also easily create, edit and delete a Tag-based VLAN group by clicking **<Add>**, **<Edit>** and **<Delete>** function buttons.

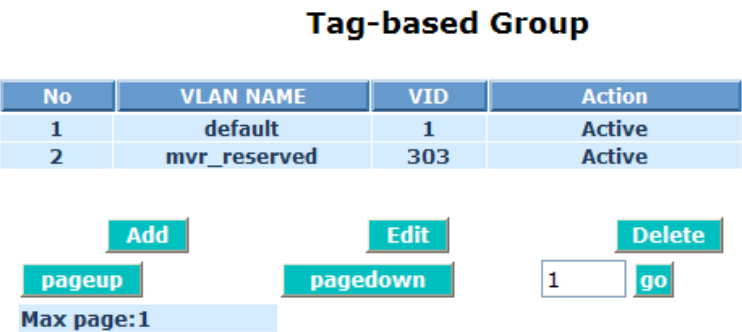


Fig. 3-60

Parameter description:

Add:

- Step 1: To click **<Add>** button (Fig. 3-61).
- Step 2: To input relative settings, then click **<Apply>** button (Fig. 3-62).

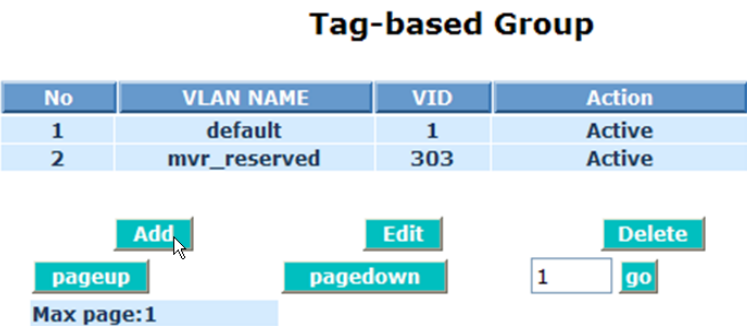


Fig. 3-61 Step 1

Tag-based VLAN

| | | | | | | | | |
|------------------|--|--|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| VLAN name | Test1 | | | | | | | |
| VID | 3 | | | | | | | |
| GVRP Propagation | Disable | | | | | | | |
| Member | 1. ☒ | 2. ☒ | 3. ☐ | 4. ☐ | 5. ☐ | 6. ☐ | 7. ☐ | 8. ☐ |
| | 9. ☐ | 10. ☐ | | | | | | |
| Untag | 1. ☐ | 2. ☒ | 3. ☐ | 4. ☐ | 5. ☐ | 6. ☐ | 7. ☐ | 8. ☐ |
| | 9. ☐ | 10. ☐ | | | | | | |
| Action | Active | | | | | | | |

Apply

Fig. 3-62 Step 2

VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, “ - ” and “ _ ” characters. The maximal length is 15 characters.

VID:

VLAN identifier. Each tag-based VLAN group has a unique VID. It appears only in tag-based and Double-tag mode.

Member:

This is used to enable or disable if a port is a member of the new added VLAN, “Enable” means it is a member of the VLAN. Just tick the check box beside the port x to enable it.

Untag:

It stands for an egress rule of the port. If you tick the check box beside the port No., packets with this VID outgoing from this port will be untagged.

Action:

Active: VLAN just added in active state.

NotInService: VLAN not in active state.

Tag-based Group

| No | VLAN NAME | VID | Action |
|----|--------------|-----|--------|
| 1 | default | 1 | Active |
| 2 | Test1 | 3 | Active |
| 3 | mvr_reserved | 303 | Active |

Fig. 3-63 Tag-based Group created

Delete:

To click an existed entry, then click **<Delete>** button. (Fig. 3-64).

Tag-based Group

| No | VLAN NAME | VID | Action |
|----|--------------|-----|--------|
| 1 | default | 1 | Active |
| 2 | Test1 | 3 | Active |
| 3 | mvr_reserved | 303 | Active |

Add

Edit

Delete

pageup

pagedown

1

go

Max page:1

Fig. 3-64 Tag-based Group deleted

Edit:

To click an existed entry, then click **<Edit>** button. (Fig. 3-65).

Tag-based Group

| No | VLAN NAME | VID | Action |
|----|--------------|-----|--------|
| 1 | default | 1 | Active |
| 2 | Test1 | 3 | Active |
| 3 | mvr_reserved | 303 | Active |

Add

Edit

Delete

pageup

pagedown

1

go

Max page:1

Fig. 3-65 Tag-based Group edited

3-11-3. PVID

Function name:

PVID

Function description:

In PVID Setting, user can input VID number to each port. The range of VID number is from 1 to 4094. User also can choose ingress filtering rule (Rule 2) to each port. The Ingress Filtering Rule 2 is “drop untagged frame”. While Rule 2 is enabled, the port will discard all Untagged-frames.

PVID

| Port No | PVID | Default Priority | Drop Untag |
|---------|------|------------------|------------|
| 1 | 1 | 0 | Disable |
| 2 | 1 | 0 | Disable |
| 3 | 1 | 0 | Disable |
| 4 | 1 | 0 | Disable |
| 5 | 1 | 0 | Disable |
| 6 | 1 | 0 | Disable |
| 7 | 1 | 0 | Disable |
| 8 | 1 | 0 | Disable |
| 9 | 1 | 0 | Disable |
| 10 | 1 | 0 | Disable |

Apply

Fig. 3-66

Parameter description:

Port 1-10:

Port number.

PVID:

This PVID range will be 1-4094. Before you set a number x as PVID, you have to create a Tag-based VLAN with VID x. For example, if port x receives an untagged packet, the switch will apply the PVID (assume as VID y) of port x to tag this packet, the packet then will be forwarded as the tagged packet with VID y.

Default Priority:

It bases on IEEE802.1p QoS and affects untagged packets. When the packets enter the switch, it would get the priority precedence according to your Default Priority setting and map to IEEE802.1p priority setting in QoS function. For example, while you set Default Priority of port 2 with 2 and transmit untagged packets to port 2, these packets will own priority 2 precedence due to your default IEEE802.1p Priority Mapping setting in

QoS function and be put into Queue 1.

Available value: 0~7

Default: 0

Drop Untag:

Drop untagged frame. You can configure a given port to accept all frames (Tagged and Untagged) or just receive tagged frame. If the former is the case, then the packets with tagged or untagged will be processed. If the later is the case, only the packets carrying VLAN tag will be processed, the rest packets will be discarded.

3-11-4. Port-based Group

Function name:

Port-based Group Configuration

Function description:

It shows the information of the existed Port-based VLAN Groups. You can easily create, edit and delete a Port-based VLAN group by clicking **<Add>**, **<Edit>** and **<Delete>** function buttons.

Port-based Group

| No | VLAN NAME |
|----|-----------|
| 1 | default |

Add

Edit

Delete

Fig. 3-67

Parameter description:

No:

Port number.

VLAN Name:

The name defined by administrator is associated with a VLAN group. Valid letters are A-Z, a-z, 0-9, “ - ” and “ _ ” characters. The maximal length is 15 characters.

Add:

Step 1: To click **<Add>** button.

Step 2: To input VLAN name and tick the check box beside the port x, then click **<Apply>** button.

Port-based Group

| No | VLAN NAME |
|----|-----------|
| 1 | default |

Add

Edit

Delete

Fig. 3-68

Port-based VLAN

| | | | | | | | | |
|-----------|--|--|--|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| VLAN name | Test1 | | | | | | | |
| Member | 1. ☒ | 2. ☒ | 3. ☒ | 4. ☐ | 5. ☐ | 6. ☐ | 7. ☐ | 8. ☐ |
| | 9. ☐ | 10. ☐ | | | | | | |

Apply

Fig. 3-69

Delete:

To select an existed entry, then click **<Delete>** button (Fig. 3-70).

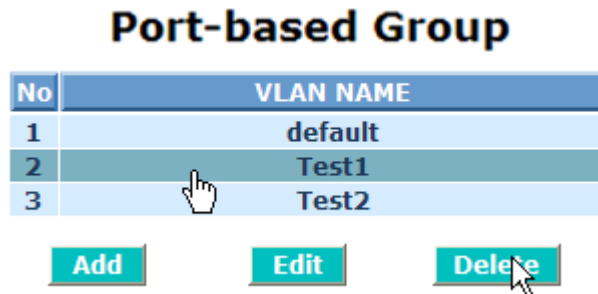


Fig. 3-70

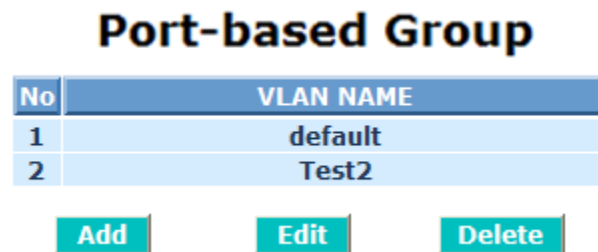


Fig. 3-71

Edit:

Step 1: To select an existed entry, then click **<Edit>** button.

Step 2: To modify member, then click **<Apply>** button.

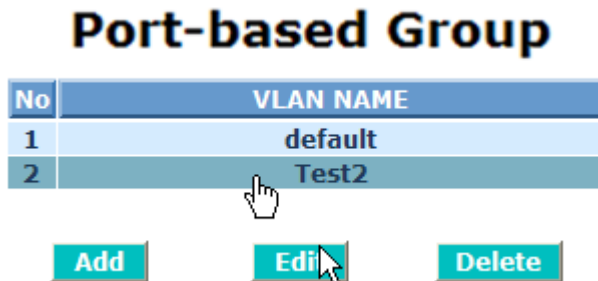


Fig. 3-72

Port-based VLAN

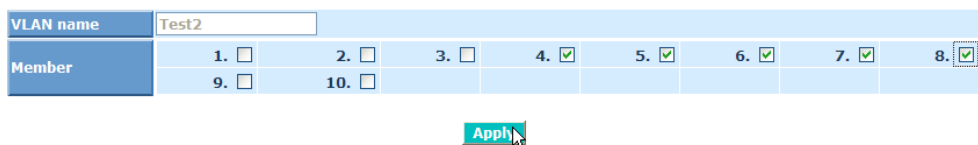


Fig. 3-74

3-11-5. Management VLAN

Function name:

Management VLAN

Function description:

The administrator may enable Management VLAN and set a VID to limit the VLAN management right.

The default value is Enable as VLAN Management is limited VID 1.

Management VLAN

| | |
|-------|----------|
| State | Enable ▾ |
| VID | 1 |

Apply

Fig. 3-75

Parameter description:

State:

It allows users to enable or disable Management VLAN. When this function is enabled, only the tagged packets with this VID can manage the switch.

VID:

Valid range 1~4094.

3-12. MAC Table

MAC Table Configuration gathers many functions, including MAC Table Information, MAC Table Maintenance, Static, MAC Alias, Port Security and Port Static MAC, which cannot be categorized to some function type. They are described below.

3-12-1. Information

Function name:

MAC Table Information

Function Description:

Display the static or dynamic learning MAC entry and the state for the selected port.

MAC Table Information

Port: ☒ 01 ☒ 02 ☒ 03 ☒ 04 ☒ 05
☒ 06 ☒ 07 ☒ 08 ☒ 09 ☒ 10
☐ Select/Unselect All

Search: MAC: ?? - ?? - ?? - ?? - ?? - ?? VID: ?

MAC:

Alias:

| Alias | MAC Address | Port | VID | State |
|-------|-------------|------|-----|-------|
|-------|-------------|------|-----|-------|

Fig. 3-76

Parameter description:

Port:

Select the port you would like to inquire.

Search:

Set up the MAC entry you would like to inquire.

The default is ??-??-??-??-??-??

MAC:

Display the MAC address of one entry you selected from the searched MAC entries table.

Alias:

Set up the Alias for the selected MAC entry.

Set Alias:

Save the Alias of MAC entry you set up.

Search:

Find the entry that meets your setup.

Previous Page Buttn:

Move to the previous page.

Next Page Button:

Move to the next page.

Alias field:

The Alias of the searched entry.

MAC Address field:

The MAC address of the searched entry.

Port field:

The port that exists in the searched MAC Entry.

VID field:

VLAN Group that MAC Entry exists.

State field:

Display the method that this MAC Entry is built. It may show "Dynamic MAC" or "Static MAC".

3-12-2. Maintenance

Function name:

MAC Table Maintenance

Function Description :

This function can allow the user to set up the processing mechanism of MAC Table. An idle MAC address exceeding MAC Address Age-out Time will be removed from the MAC Table. The range of Age-out Time is 10-1000000 seconds, and the setup of this time will have no effect on static MAC addresses.

In addition, the learning limit of MAC maintenance is able to limit the amount of MAC that each port can learn.

MAC Maintenance

| Aging time | |
|---|--|
| Enable <input type="button" value="v"/> | 300 Secs (10~1000000) <input type="button" value="Apply"/> |

| Flush MAC Table | |
|--------------------------------------|--|
| <input type="button" value="Flush"/> | |

| Learning Limit (0~8191) | | | |
|-------------------------|-------|---------|-------|
| Port No | Limit | Port No | Limit |
| 1 | 8191 | 2 | 8191 |
| 3 | 8191 | 4 | 8191 |
| 5 | 8191 | 6 | 8191 |
| 7 | 8191 | 8 | 8191 |
| 9 | 8191 | 10 | 8191 |

Fig. 3-77

Parameter description:

Aging Time:

Delete a MAC address idling for a period of time from the MAC Table, which will not affect static MAC address. Range of MAC Address Aging Time is 10-1000000 seconds.

Default: 300 seconds

Learning Limit:

To set up the maximum amount of MAC that each port can learn. Valid value of learning limit for port 1~10 ranges from 0-8191.

Default: 8191

3-12-3. Static

Function Name:

Static Setting

Function Description:

The function of Static is used to configure MAC's real manners inside of the switch. Three kinds of manners including static, static with destination drop and static with source drop are contained in this function .

As "static" is chosen, assign a MAC address to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port.

As "static with destination drop" is chosen, the packet will be dropped if its DA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports' transmission of the packets.

As "static with source drop" is chosen, the packet will be dropped if its SA is equal to the value you set up. Due to this setting belongs to the global one, so, it may affect all ports' transmission of the packets.

Static MAC

| MAC | | VID | Forwarding Rule | Port |
|----------------------|----------------------|----------------------|-----------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | Static | <input type="text"/> |

| No | MAC | VID | Forwarding Rule | Port |
|----|-------------------|-----|------------------------------|------|
| 1 | 12-4E-5F-42-F8-11 | 3 | Static with Destination Drop | 4 |
| 2 | 00-E3-4E-33-F3-11 | 2 | Static | 5 |

Fig. 3-78

Parameter description:

MAC:

It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00 - 40 - C7 - D6 - 00 - 01

VID:

VLAN identifier. This will be filled only when tagged VLAN is applied. Valid range is 1 ~ 4094.

Forwarding Rule(Drop Policy):

Static:

A MAC address is assigned to a specific port, all of the switch's traffics sent to this MAC address will be forwarded to this port.

Static with Destination Drop:

While the DA of the incoming packets meets the value you set up, these packets will be dropped.

Static with Source Drop:

While the SA of the incoming packets meets the value you set up, these packets will be dropped.

Port :

To input the port No. you would like to do setup in the switch. It is 1 ~10.

Add:

To input MAC, VID, Port and select a Forwarding Rule, then click **<Add>** button.

Static MAC

| MAC | | | | | | VID | Forwarding Rule | Port |
|-----|----|----|----|----|----|-----|-----------------|------|
| 00 | 11 | 22 | 33 | 44 | 55 | 1 | Static | 2 |

Add **Delete**

| No | MAC | VID | Forwarding Rule | Port |
|----|-------------------|-----|-----------------|------|
| 1 | 00-40-C7-2F-20-CA | 1 | Static | 6 |

Fig. 3-79

Delete:

To select an entry, then click **<Delete>** button.

Static MAC

| MAC | | | | | | VID | Forwarding Rule | Port |
|-----|--|--|--|--|--|-----|-----------------|------|
| | | | | | | | Static | |

Add **Delete**

| No | MAC | VID | Forwarding Rule | Port |
|----|-------------------|-----|-----------------|------|
| 1 | 00-11-22-33-44-55 | 1 | Static | 2 |
| 2 | 00-40-C7-2F-20-CA | 1 | Static | 6 |

Fig. 3-80

3-12-4. MAC Alias

Function name:

MAC Alias

Function description:

MAC Alias function is used to let you assign MAC address to an Alias in English. This will help you tell which MAC address belongs to which user in the illegal access report. At the initial time, it shows all pairs of the existed alias name and MAC address.

There are three MAC alias functions in this function folder, including MAC Alias Add, MAC Alias Edit and MAC Alias Delete. You can click **<Create/Edit>** button to add/modify a new or an existed alias name for a specified MAC address, or mark an existed entry to delete it. Alias name must be composed of A-Z, a-z and 0-9 only and has a maximal length of 15 characters.

MAC Alias

| MAC Address | | | | | | Alias |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Create/Edit Delete

| No | MAC Address | Alias |
|----|-------------------|--------|
| 1 | 11-e4-4f-21-23-11 | sales1 |

Fig. 3-81

Parameter description:

MAC Address:

It is a six-byte long Ethernet hardware address and usually expressed by hex and separated by hyphens. For example, 00-40-C7-D6-00-02

Alias:

MAC alias name you assign.

Create:

To input MAC Address and Alias name, then click **<Create/Edit>** button.

MAC Alias

| MAC Address | | | | | | Alias |
|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|---------------------------------|-------------------------------------|
| <input type="text" value="11"/> | <input type="text" value="22"/> | <input type="text" value="33"/> | <input type="text" value="44"/> | <input type="text" value="55"/> | <input type="text" value="66"/> | <input type="text" value="Switch"/> |

Create/Edit Delete

| No | MAC Address | Alias |
|----|-------------------|--------------|
| 1 | 00-11-2f-43-cb-dc | Server |
| 2 | 00-40-c7-f7-00-cf | IES-2310C_RD |
| 3 | 00-40-c7-2f-20-ca | IES-2710C |

Fig. 3-82

Edit:

Step 1: To select an existed entry, then Edit the data.

Step 2: To click **<Create/Edit>** button.

MAC Alias

| MAC Address | | | | | | Alias |
|-------------|----|----|----|----|----|-------|
| 11 | 22 | 33 | 44 | 55 | 66 | yes |

Create/Edit **Delete**

| No | MAC Address | Alias |
|----|-------------------|-------|
| 1 | 11-22-33-44-55-66 | yes |
| 2 | 11-22-33-44-55-77 | test2 |

Fig. 3-83

MAC Alias

| MAC Address | | | | | | Alias |
|-------------|----|----|----|----|----|-------|
| 11 | 22 | 33 | 44 | 55 | 66 | Good |

Create/Edit **Delete**

| No | MAC Address | Alias |
|----|-------------------|-------|
| 1 | 11-22-33-44-55-66 | yes |
| 2 | 11-22-33-44-55-77 | test2 |

Fig. 3-84

MAC Alias

| MAC Address | | | | | | Alias |
|-------------|--|--|--|--|--|-------|
| | | | | | | |

Create/Edit **Delete**

| No | MAC Address | Alias |
|----|-------------------|-------|
| 1 | 11-22-33-44-55-66 | Good |
| 2 | 11-22-33-44-55-77 | test2 |

Fig. 3-85

Delete:

To select an existed entry, then click **<Delete>** button.

MAC Alias

| MAC Address | | | | | | Alias |
|-------------|----|----|----|----|----|-----------|
| 00 | 40 | c7 | 2f | 20 | ca | IES-2710C |

[Create/Edit](#) [Delete](#)

| No | MAC Address | Alias |
|----|-------------------|--------------|
| 1 | 00-11-2f-43-cb-dc | Server |
| 2 | 00-40-c7-f7-00-cf | IES-2310C_RD |
| 3 | 00-40-c7-2f-20-ca | IES-2710C |

Fig. 3-86

Note: If there are too many MAC addresses learned in the table, we recommend you inputting the MAC address and alias name directly.

3-12-5. Port Security

Function name:

Port Security

Function description:

In its most basic form, the Port Security feature remembers the Ethernet MAC address connected to the switch port and allows only that MAC address to communicate on that port. If any other MAC address tries to communicate through the port, port security will disable the port.

Port Security

| | | | | | | | |
|-----------------------------|------------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|
| 1. ☐ | 2. ☐ | 3. ☐ | 4. ☐ | 5. ☐ | 6. ☐ | 7. ☐ | 8. ☐ |
| 9. ☐ | 10. ☐ | | | | | | |

Fig. 3-87

Parameter description:

When you enable the port security then the switch port only forwarding the static MAC what you have set. Others will drop or deny forwarding. The port number is 1 to 10.

3-12-6. Port Static MAC

Function name:

Port Static MAC

Function description:

The function of Static is used to configure MAC's real manners inside of the switch per port.

Port Static MAC Port 1 ▼

| No | MAC | VID |
|----|-------------------|-----|
| 1 | 00-E3-4F-22-35-11 | 3 |

Add Edit Delete

Fig. 3-88

Parameter description:

Add:

You can select a port which you want to set static MAC table. Click **<Add>** button. Then input MAC address and VID. Click **<Apply>** button to create a new Static MAC address entry.

Port Static MAC Port 2 ▼

| No | MAC | VID |
|--------|-----|-----|
| (None) | | |

Add Edit Delete

Fig. 3-89

Port 2 Static Mac

| | | | | | | |
|-----|----|----|----|----|----|----|
| MAC | 11 | 22 | 33 | 44 | 55 | 66 |
| VID | 2 | | | | | |

Apply

Fig. 3-90

Port Static MAC Port 2 ▼

| No | MAC | VID |
|----|-------------------|-----|
| 1 | 11-22-33-44-55-66 | 2 |

Add Edit Delete

Fig. 3-91

Edit:

You can select an entry which you want to edit, then click **<Edit>** button.

Port Static MAC Port 2 ▼

| No | MAC | VID |
|----|-------------------|-----|
| 1 | 11-22-33-44-55-66 | 2 |



Add Edit Delete

Fig. 3-92

Delete:

You can select an entry which you want to delete, then click **<Delete>** button.

Port Static MAC Port 2 ▼

| No | MAC | VID |
|----|-------------------|-----|
| 1 | 11-22-33-44-55-66 | 2 |



Add Edit Delete

Fig. 3-93

3-13. GVRP Configuration

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain the group membership information of the VLANs. The GVRP offers the function providing the VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

In GVRP Configuration function folder, there are three functions supported, including GVRP Config, GVRP Counter and GVRP Group explained below.

3-13-1. Config

Function name:

GVRP Config

Function description:

In the function of GVRP Config, it is used to configure each port's GVRP operation mode, in which there are seven parameters needed to be configured described below.

GVRP Configuration

GVRP State Enabled ▼ Apply

| Port | Join Time | Leave Time | LeaveAll Time | Default Applicant Mode | Default Registrar Mode | Restricted Mode |
|------|-----------|------------|---------------|------------------------|------------------------|-----------------|
| 1 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |
| 2 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |
| 3 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |
| 4 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |
| 5 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |
| 6 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |
| 7 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |
| 8 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |
| 9 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |
| 10 | 20 | 60 | 1000 | Normal ▼ | Normal ▼ | Disabled ▼ |

Apply

Fig. 3-94

Parameter description:

GVRP State Setting:

This function is simply to let you enable or disable GVRP function. You can pull down the list to choose “Enabled” or “Disabled”. Then, click the **<Apply>** button, the system will take effect immediately.

Join Time:

Used to declare the Join Time in unit of centisecond. Valid time range: 20

–100 centisecond, Default: 20 centisecond.

Leave Time:

Used to declare the Leave Time in unit of centisecond. Valid time range: 60 –300 centisecond, Default: 60 centisecond.

Leave All Time:

A time period for announcement that all registered device is going to be de-registered. If someone still issues a new join, then a registration will be kept in the switch. Valid range: 1000-5000 unit time, Default: 1000 unit time.

Default Applicant Mode:

The mode here means the type of participant. There are two modes, normal participant and non-participant, provided for the user's choice.

Normal:

It is Normal Participant. In this mode, the switch participates normally in GARP protocol exchanges. The default setting is Normal.

Non-Participant:

It is Non-Participant. In this mode, the switch does not send or reply any GARP messages. It just listens messages and reacts for the received GVRP BPDU.

Default Registrar Mode:

The mode here means the type of Registrar. There are three types of parameters for registrar administrative control value, normal registrar, fixed registrar and forbidden registrar, provided for the user's choice.

Normal:

It is Normal Registration. The Registrar responds normally to incoming GARP messages. The default setting is Normal.

Fixed:

It is Registration Fixed. The Registrar ignores all GARP messages, and all members remain in the registered (IN) state.

Forbidden:

It is Registration Forbidden. The Registrar ignores all GARP messages, and all members remain in the unregistered (EMPTY) state.

Restricted Mode:

This function is used to restrict dynamic VLAN be created when this port received GVRP PDU. There are two modes, disable and enable, provided for the user's choice.

Disabled:

In this mode, the switch dynamic VLAN will be created when this port received GVRP PDU. The default setting is Normal.

Enabled:

In this mode, the switch does not create dynamic VLAN when this port received GVRP PDU. Except received dynamic VLAN message of the GVRP PDU is an existed static VLAN in the switch, this port will be added into the static VLAN members dynamically.

3-13-2. Counter

Function name:

GVRP Counter

Function description:

All GVRP counters are mainly divided into Received and Transmitted two categories to let you monitor the GVRP actions. Actually, they are GARP packets.



| Counter Name | Received | Transmitted |
|----------------------|----------|-------------|
| Total GVRP Packets | 0 | 0 |
| Invalid GVRP Packets | 0 | ---- |
| LeaveAll message | 0 | 0 |
| JoinEmpty message | 0 | 0 |
| JoinIn message | 0 | 0 |
| LeaveEmpty message | 0 | 0 |
| Empty message | 0 | 0 |

Refresh

Fig. 3-95

Parameter description:

Received:

Total GVRP Packets:

Total GVRP BPDU is received by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU is received by the GARP application.

LeaveAll Message Packets:

Number of GARP BPDU with Leave All message is received by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU with Join Empty message is received by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU with Join In message is received by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU with Leave Empty message is received by the GARP application.

Empty Message Packets:

Number of GARP BPDU with Empty message is received by the GARP application.

Transmitted:

Total GVRP Packets:

Total GARP BPDU is transmitted by the GVRP application.

Invalid GVRP Packets:

Number of invalid GARP BPDU is transmitted by the GVRP application.

LeaveAll Message Packets:

Number of GARP BPDU with Leave All message is transmitted by the GARP application.

JoinEmpty Message Packets:

Number of GARP BPDU with Join Empty message is transmitted by the GARP application.

JoinIn Message Packets:

Number of GARP BPDU with Join In message is transmitted by the GARP application.

LeaveEmpty Message Packets:

Number of GARP BPDU with Leave Empty message is transmitted by the GARP application.

Empty Message Packets:

Number of GARP BPDU with Empty message is transmitted by the GARP application.

3-13-3. Group

Function name:

GVRP Group Information

Function description:

To show the dynamic group member and their information.

GVRP VLAN Group Information

| Current Dynamic Group Number | | 1 |
|------------------------------|-------------------------------|---------|
| VID | Member Port | |
| 1 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 | |
| Edit Administrative Control | | Refresh |

Fig. 3-96

Parameter description:

Current Dynamic Group Number:

The number of GVRP group that are created currently.

VID:

VLAN identifier. When GVRP group creates, each dynamic VLAN group owns its VID. Valid range is 1 ~ 4094.

Member Port:

Those are the members belonging to the same dynamic VLAN group.

Edit Administrative Control:

When you create GVRP group, you can use Administrative Control function to change Applicant Mode and Registrar Mode of GVRP group member.

To select an existed entry, then click **<Edit Administrative Control>** button.

GVRP VLAN Group Information

| Current Dynamic Group Number | | 1 |
|------------------------------|-------------------------------|---------|
| VID | Member Port | |
| 1 | 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 | |
| Edit Administrative Control | | Refresh |

Fig. 3-97

Administrative Control Configuration VID: 1 ▾

| Port | Applicant | Registrar |
|------|-----------|-----------|
| 1 | Normal ▾ | Fixed ▾ |
| 2 | Normal ▾ | Fixed ▾ |
| 3 | Normal ▾ | Fixed ▾ |
| 4 | Normal ▾ | Fixed ▾ |
| 5 | Normal ▾ | Fixed ▾ |
| 6 | Normal ▾ | Fixed ▾ |
| 7 | Normal ▾ | Fixed ▾ |
| 8 | Normal ▾ | Fixed ▾ |
| 9 | Normal ▾ | Fixed ▾ |
| 10 | Normal ▾ | Fixed ▾ |

Apply

Cancel

Fig. 3-98

Refresh:

Refresh function can help you to see current GVRP group status.

3-14. STP Configuration

The Spanning Tree Protocol (STP) is a standardized method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, ensure that only one path is active between any two nodes on the network at a time. User can enable Spanning Tree Protocol on switch's web management and then set up other advanced items. We recommend that you enable STP on all switches to ensure a single active path on the network.

3-14-1. Status

Function name:

STP Status

Function description:

In the Spanning Tree Status, user can read 12 parameters to know STP current status. The 12 parameters' descriptions are listed in the following table.

| STP Status | |
|--------------------------------------|-------------------|
| STP State | Disabled |
| Bridge ID | 00:40:C7:33:00:08 |
| Bridge Priority | 32768 |
| Designated Root | 00:40:C7:33:00:08 |
| Designated Priority | 32768 |
| Root Port | 0 |
| Root Path Cost | 0 |
| Current Max. Age(sec) | 20 |
| Current Forward Delay(sec) | 15 |
| Hello Time(sec) | 2 |
| STP Topology Change Count | 0 |
| Time Since Last Topology Change(sec) | 0 |

Fig. 3-99

Parameter description:

STP State:

Show the current STP Enabled / Disabled status. Default is "Disabled".

Bridge ID:

Show switch's bridge ID which stands for the MAC address of this switch.

Bridge Priority:

Show this switch's current bridge priority setting. Default is 32768.

Designated Root:

Show root bridge ID of this network segment. If this switch is a root bridge, the "Designated Root" will show this switch's bridge ID.

Designated Priority:

Show the current root bridge priority.

Root Port:

Show port number connected to root bridge with the lowest path cost.

Root Path Cost:

Show the path cost between the root port and the designated port of the root bridge.

Current Max. Age:

Show the current root bridge maximum age time. Maximum age time is used to monitor if STP topology needs to change. When a bridge does not receive a hello message from root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges.

All bridges in the LAN will re-learn and determine which the root bridge is. Maximum Age time is assigned by root bridge in unit of seconds. Default is 20 seconds.

Current Forward Delay:

Show the current root bridge forward delay time. The value of Forward Delay time is set by root. The Forward Delay time is defined as the time spent from Listening state moved to Learning state or from Learning state moved to Forwarding state of a port in bridge.

Hello Time:

Show the current hello time of the root bridge. Hello time is a time interval specified by root bridge, used to request all other bridges periodically sending hello message every "hello time" seconds to the bridge attached to its designated port.

STP Topology Change Count:

STP Topology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to 0. The figures showing in the screen may not be the exact time it spent but very close to, because the time is eclipsing.

Time Since Last Topology Change:

Time Since Last Topology Change is the accumulated time in unit of seconds the STP has been since the last STP Topology Change was made. When Topology Change is initiated again, this counter will be reset to 0. And it will also count again once STP topology Change is completed.

3-14-2. Configuration

The STP, Spanning Tree Protocol, actually includes RSTP. In the Spanning Tree Configuration, there are six parameters open for user to configure. Each parameter description is listed below.

Function name:

STP Configuration

Function description:

User can set the following Spanning Tree parameters to control STP function enable/disable, select mode RSTP/STP and affect STP state machine behavior to send BPDU in this switch. The default setting of Spanning Tree Protocol is “Disable”.

STP Configuration

| | |
|---------------------------|-----------|
| Spanning Tree Protocol | Disable ▾ |
| Bridge Priority (0-61440) | 32768 ▾ |
| Hello Time (1-10 sec) | 2 |
| Max. Age (6-40 sec) | 20 |
| Forward Delay (4-30 sec) | 15 |
| Force Version | RSTP ▾ |

**Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$
 $\text{Max Age} \geq 2 * (\text{Hello Time} + 1)$**

Apply

Fig. 3-100

Parameter description:

Spanning Tree Protocol:

Set 802.1W Rapid STP function Enable / Disable. Default is “Disable”

Bridge Priority:

The lower the bridge priority is, the higher priority it has. Usually, the bridge with the highest bridge priority is the root. If you want to have the device as root bridge, you can set this value lower than that of bridge in the LAN. The valid value is 0 ~ 61440. The default is 32768.

Hello Time:

Hello Time is used to determine the periodic time to send normal BPDU from designated ports among bridges. It decides how long a bridge should send this message to other bridge to tell I am alive. When the device is the root bridge of the LAN, for example, all other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1 ~ 10 in unit of second.

Default is 2 seconds.

Max. Age:

When the device is the root bridge, the whole LAN will apply this figure set by this switch as their maximum age time. When a bridge received a BPDU originated from the root bridge and if the message age conveyed in the BPDU exceeds the Max. Age of the root bridge, the bridge will treat the root bridge malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges in the LAN will re-calculate and determine who the root bridge is. The valid value of Max. Age is 6 ~ 40 seconds. Default is 20 seconds.

Forward Delay:

You can set the root bridge forward delay time. This figure is set by root bridge only. The forward delay time is defined as the time spent from Listening state moved to Learning state and also from Learning state moved to Forwarding state of a port in bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that forward delay time is 15 seconds, then total forward delay time will be 30 seconds. This has much to do with the STP convergent time which will be more than 30 seconds because some other factors.

The valid value is 4 ~ 30 seconds, default is 15 seconds.

Force Version:

Two options are offered for the user's choosing STP algorithm. One is RSTP and the other is STP. If STP is chosen, RSTP will run as a legacy STP. The switch supports RSTP (IEEE802.1w) which is backward compatible with STP (IEEE802.1d).

3-14-3. Port

Function name:

STP Port Setting

Function description:

In the STP Port Setting, one item selection and five parameters settings are offered for user's setup. User can disable and enable each port by selecting each Port Status item. User also can set "Path Cost" and "Priority" of each port by filling in the desired value and set "Admin Edge Port" and "Admin Point To Point" by selecting the desired item.

| STP Port Configuration | | | | | | |
|------------------------|-------------|------------------|----------------------|----------|-----------------|----------------------|
| Port No | Port Status | Path Cost Status | Configured Path Cost | Priority | Admin Port Type | Admin Point To Point |
| 1 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |
| 2 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |
| 3 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |
| 4 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |
| 5 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |
| 6 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |
| 7 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |
| 8 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |
| 9 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |
| 10 | FORWARDING | 200000 | 0 | 128 | Normal | Auto |

Fig. 3-101

Parameter description:

Port Status:

It displays the current state of a port. We cannot manually set it because it displays the status only. There are three possible states. (according to 802.1w specification)

- DISCARDING state indicates that this port can neither forward packets nor contribute learning knowledge.

Note: Three other states (Disable state, BLOCKING state and LISTENING state) defined in the 802.1d specification are now all represented as DISCARDING state.

- LEARNING state indicates this port can now contribute its learning knowledge but cannot forward packets still.
- FORWARDING state indicates this port can both contribute its learning knowledge and forward packets normally.

Path Cost Status:

It is the contribution value of the path through this port to Root Bridge. STP algorithm determines a best path to Root Bridge by calculating the sum of path cost contributed by all ports on this path. A port with a smaller path cost value would become the Root Port more possibly.

Configured Path Cost:

The range is 0 – 200,000,000. In the switch, if path cost is set to be zero, the STP will get the recommended value resulted from auto-negotiation of the link accordingly and display this value in the field of Path Cost Status. Otherwise, it may show the value that the administrator set up in Configured Path Cost and Path Cost Status.

802.1w RSTP recommended value: (Valid range: 1 – 200,000,000)

10 Mbps : 2,000,000

100 Mbps : 200,000

1 Gbps : 20,000

Default: 0

Priority:

Priority here means Port Priority. Port Priority and Port Number are mixed to form the Port ID. Port IDs are often compared in order to determine which port of a bridge would become the Root Port. The range is 0 – 240.

Default is 128.

Admin Edge Port:

If user selects “Yes”, this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because the edge ports cannot create bridging loops in the network. This will expedite the convergence. When the link on the edge port toggles, the STP topology keeps unchanged. Unlike the designate port or root port though, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU.

Default: No

Admin Point To Point:

We say a port is a point-to-point link, from RSTP's view, if it is in full-duplex mode but is shared link if it is in half-duplex mode. RSTP fast convergence can only happen on point-to-point links and on edge ports. This can expedite the convergence because this will have the port fast transited to forwarding state.

There are three parameters, Auto, True and False, used to configure the type of the point-to-point link. If configure this parameter to be Auto, it

means RSTP will use the duplex mode resulted from the auto-negotiation. In today's switched networks, most links are running in full-duplex mode. For sure, the result may be half-duplex, in this case, the port will not fast transit to Forwarding state. If it is set as True, the port is treated as point-to-point link by RSTP and unconditionally transited to Forwarding state. If it is set as False, fast transition to Forwarding state will not happen on this port.

Default: Auto

M Check:

Migration Check. It forces the port sending out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly get back to act as an RSTP port. Click **<M Check>** button to send a RSTP BPDU from the port you specified.

3-15. MSTP

The implementation of MSTP is according to IEEE802.1Q 2005 Clause13-Multiple Spanning Tree Protocol MSTP allows frames assigned to different VLANs to follow separate paths, each based on an independent Multiple Spanning Tree Instance (MSTI), within Multiple Spanning Tree (MST) Regions composed of LANs and or MST Bridges. Proper configuration of MSTP in an IEEE802.1Q VLAN environment can ensure a loop-free data path for a group of VLANs within an MSTI. Redundant path and load balancing in VLAN environment is also achieved via this feature. A spanning tree instance called CIST (Common and Internal Spanning Tree) always exists. Up to 64 more spanning tree instances (MSTIs) can be provisioned.

3-15-1. MSTP State

Function name:

MSTP State

Function description:

To enable or disable MSTP. And to select a version of Spanning Tree protocol which MSTP should operate on.

MSTP State

| | |
|---------------------------------|-----------|
| Multiple Spanning Tree Protocol | Disable ▾ |
| Force Version | MSTP ▾ |

Apply

Fig. 3-102

Parameter description:

Multiple Spanning Tree Protocol:

Disabled / Enabled

Force Version:

STP / RSTP / MSTP

3-15-2. Region Config

Function name:

MSTP Region Config

Function description:

To configure the basic identification of a MSTP bridge. Bridges participating in a common MST region must have the same Region Name and Revision Level.

MSTP Region Config

| | |
|-------------------------------|-------------------|
| Region Name (0~32 characters) | 00-40-C7-33-00-08 |
| Revision Level (0-65535) | 0 |

Fig. 3-103

Parameter description:

Region Name:

0-32 characters.

(A variable length text string encoded within a fixed field of 32 bytes, conforming to RFC 2271's definition of SnmpAdminString.)

Revision Level:

0-65535

3-15-3. Instance View

Function name:

MSTP Instance Config

Function description:

Providing an MST instance table which include information(vlan membership of a MSTI) of all spanning instances provisioned in the particular MST region which the bridge belongs to. Through this table, additional MSTP configuration data can be applied and MSTP status can be retrieved.



Fig. 3-104

Parameter description:

Instance ID:

Every spanning tree instance need to have a unique instance ID within 0~4094. Instance 0 (CIST) always exists and can not be deleted. Additional spanning tree instances (MSTIs) can be added or deleted. At least one VLAN must be provisioned for an MSTI to declare the need for the MSTI to be existent.

Corresponding VLANs:

1-4094.

Multiple VLANs can belong to an MSTI. All VLANs that are not provisioned through this will be automatically assigned to Instance 0(CIST).

Edit MSTI / VLAN:

To add an MSTI and provide its VLAN members or modify VLAN members for a specific MSTI.

Add:

Step 1: To click **<Edit MSTI/Vlan>** button.

Step 2: To input "Instance ID", "Vlan Mapping", then click **<Apply>** button.

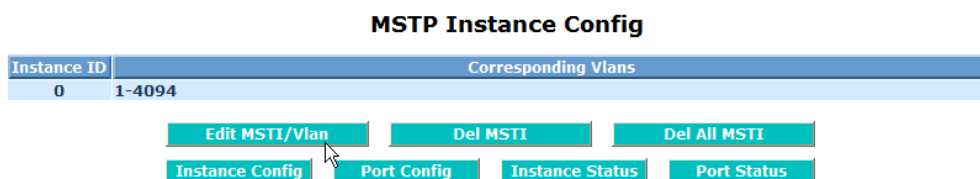


Fig. 3-105

MSTP Create MSTI/Add Vlan Mapping

| | |
|------------------------------|--|
| Instance ID
(1-4094) | 2 |
| Vlan Mapping
(VID STRING) | 5-7 |
| VID STRING
Example | 2,5-7,100-200,301,303,1000-1500 (Valid VID Range:1-4094) |

Apply

Fig. 3-106

MSTP Instance Config

| Instance ID | Corresponding Vlans |
|-------------|---------------------|
| 0 | 1-4,8-4094 |
| 2 | 5-7 |

Edit MSTI/Vlan
Del MSTI
Del All MSTI

Instance Config
Port Config
Instance Status
Port Status

Fig. 3-107

Edit:

Step 1: To select an existed entry, then click **<Edit MSTI/Vlan>** button.

Step 2: To input "Instance ID", "Vlan Mapping", then click **<Apply>** button.

MSTP Instance Config

| Instance ID | Corresponding Vlans |
|-------------|---------------------|
| 0 | 1-4,8-4094 |
| 2 | 5-7 |

Edit MSTI/Vlan
Del MSTI
Del All MSTI

Instance Config
Port Config
Instance Status
Port Status

Fig. 3-108

MSTP Create MSTI/Add Vlan Mapping

| | |
|------------------------------|--|
| Instance ID
(1-4094) | 2 |
| Vlan Mapping
(VID STRING) | 10-20 |
| VID STRING
Example | 2,5-7,100-200,301,303,1000-1500 (Valid VID Range:1-4094) |

App

Fig. 3-109

MSTP Instance Config

| Instance ID | Corresponding Vlans |
|-------------|---------------------|
| 0 | 1-4,8-9,21-4094 |
| 2 | 5-7,10-20 |

Edit MSTI/Vlan
Del MSTI
Del All MSTI

Instance Config
Port Config
Instance Status
Port Status

Fig. 3-110

Del MSTI:

To select an existed entry, then click **<Del MSTI>** button.

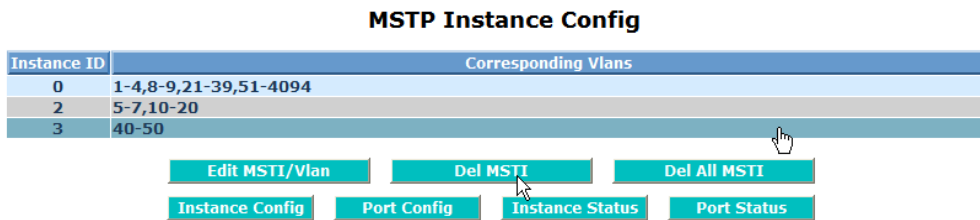


Fig. 3-111

Del All MSTI:

To click **<Del All MSTI>** button. Deleting all provisioned MSTIs at a time.

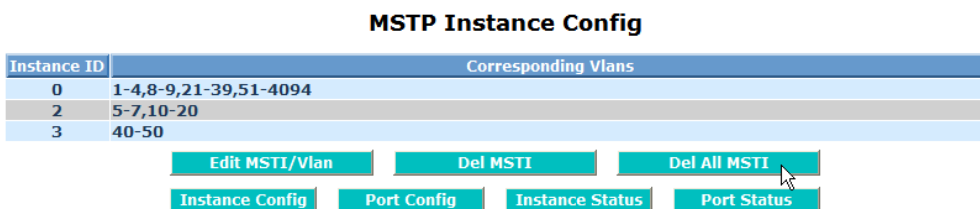


Fig. 3-112

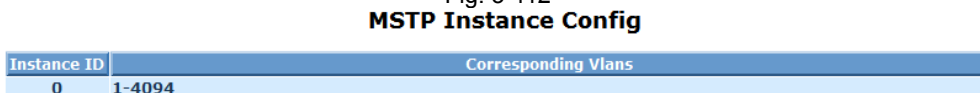


Fig. 3-113

Instance Config:

To provision spanning tree performance parameters per instance.

Step 1: To select an existed entry, then click **<Instance Config>** button.

Instance ID=3

Step 2: To select a priority, then click **<Apply>** button.

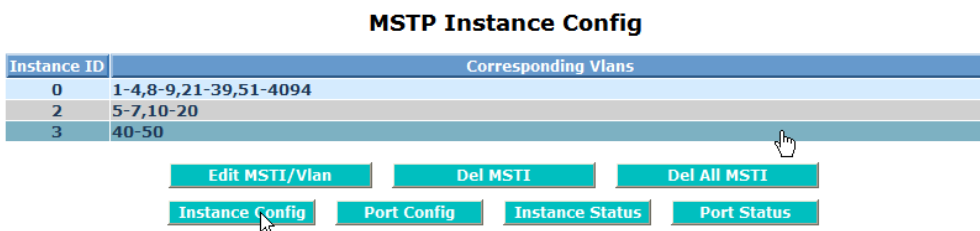


Fig. 3-114

Instance Configuration (ID=3)

Priority (0-61440)

Fig. 3-115

Instance ID=0(Fig. 3-15-15)

Step 2: To select a priority and input Max. Age, Forward Delay, Max. Hops, then click **<Apply>** button.

Instance Configuration (ID=0)

| | |
|--------------------------|---------|
| Priority (0-61440) | 32768 ▼ |
| Max. Age (6-40 sec) | 20 |
| Forward Delay (4-30 sec) | 15 |
| Max. Hops(6-40 sec) | 20 |

Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$

Max Age: available from 6 to 40. Recommended value is 20

Forward Delay(sec): available from 4 to 30. Recommended value is 15

Max Hops: available from 6 to 40. Recommended value is 20



Fig. 3-116

Priority:

The priority parameter used in the CIST(Common and Internal Spanning Tree) connection.

0 / 4096 / 8192 / 12288 / 16384 / 20480 / 24576 / 28672 /
32768 / 36864 / 40960 / 45056 / 49152 / 53248 / 57344 /
61440

MAX. Age:

6-40sec. The same definition as in the RSTP protocol.

Forward Delay:

4-30sec. The same definition as in the RSTP protocol.

MAX. Hops:

6-40sec. It's a new parameter for the multiple spanning tree protocol. It is used in the internal spanning tree instances. "CIST Remaining Hops" or "MSTI Remaining Hops" in the Spanning tree protocol message would decreased by one when the message is propagated to the neighboring bridge. If the Remaining Hops in a message is zero, the message (BPDU) would be regarded as invalid. Max Hops is used to specify the initial value of the Remaining Hops for Regional Root Bridge (Either CIST Regional Root or MSTI Regional Root).

Port Config:

To provision spanning tree performance parameters per instance per port.

Step 1: To select an existed entry, then click **<Port Config>** button.

Instance ID=3

Step 2: To input Path Cost and select a priority, then click **<Apply>** button.

MSTP Instance Config

| Instance ID | Corresponding Vlans |
|-------------|-----------------------|
| 0 | 1-4,8-9,21-39,51-4094 |
| 2 | 5-7,10-20 |
| 3 | 40-50 |

Fig. 3-117

Port Config of Instance 3

| Port | Path Cost | Priority |
|------|-----------|----------|
| 1 | 10 | 64 ▼ |
| 2 | 0 | 128 ▼ |
| 3 | 0 | 128 ▼ |
| 4 | 0 | 128 ▼ |
| 5 | 0 | 128 ▼ |
| 6 | 0 | 128 ▼ |
| 7 | 0 | 128 ▼ |
| 8 | 0 | 128 ▼ |
| 9 | 0 | 128 ▼ |
| 10 | 0 | 128 ▼ |

Fig. 3-118

Instance ID=0

Step 2: To input Path Cost and select a priority, Hello Time, Admin Edge, Admin P2P, Restricted Role, Restricted TCN, Mcheck, then click **<Apply>** button.

Port Config of Instance 0

| Port Config | | | | | | | | Migration Check |
|-------------|-----------|----------|------------|------------|-----------|-----------------|----------------|-----------------|
| Port | Path Cost | Priority | Hello Time | Admin Edge | Admin P2P | Restricted Role | Restricted TCN | Mcheck |
| 1 | 200000000 | 128 | 1 | No | False | Yes | Yes | Check |
| 2 | 0 | 128 | 2 | Yes | Auto | No | No | --- |
| 3 | 0 | 128 | 2 | Yes | Auto | No | No | --- |
| 4 | 0 | 128 | 2 | Yes | Auto | No | No | --- |
| 5 | 0 | 128 | 2 | Yes | Auto | No | No | --- |
| 6 | 0 | 128 | 2 | Yes | Auto | No | No | --- |
| 7 | 0 | 128 | 2 | Yes | Auto | No | No | --- |
| 8 | 0 | 128 | 2 | Yes | Auto | No | No | --- |
| 9 | 0 | 128 | 2 | Yes | Auto | No | No | --- |
| 10 | 0 | 128 | 2 | Yes | Auto | No | No | --- |

Apply

Fig. 3-119

Port:

1-10

Path Cost:

1 – 200,000,000

The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

Priority:

0 / 16 / 32 / 48 / 64 / 80 / 96 / 112 / 128 / 144 / 160 / 176 / 192 / 208 / 224 / 240

The same definition as in the RSTP specification. But in MSTP, this parameter can be respectively applied to ports of CIST and ports of any MSTI.

Hello Time:

1 / 2

In contrast with RSTP, Hello Time in MSTP is a per port setting for the CIST.

Admin Edge:

Yes / No

The same definition as in the RSTP specification for the CIST ports.

Admin P2P:

Auto / True / False

The same definition as in the RSTP specification for the CIST ports.

Restricted Role:

Yes / No

If “Yes” causes the Port not to be selected as Root Port for the CIST or any MSTI, even it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter is “No” by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

Restricted TCN:

Yes / No

If “Yes” causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter is “No” by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator. or the status of MAC operation for the attached LANs transitions frequently.

Mcheck:

The same definition as in the RSTP specification for the CIST ports.

Instance Status:

To show the status report of a particular spanning tree instance.

Step :To select an existed entry, then click **<Instance Status>** button.

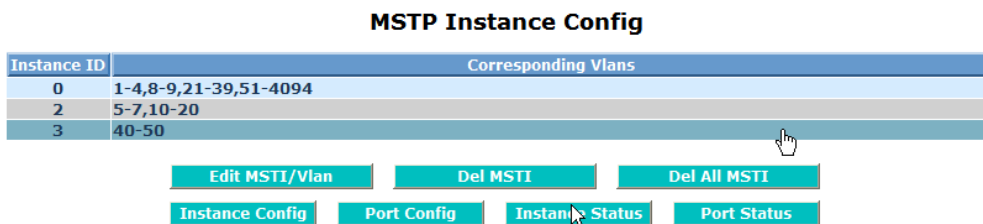


Fig. 3-120

Instance ID=3

Instance Status (ID=3)

| | |
|---------------------------------------|-------------------|
| MSTP State | Enabled |
| Force Version | MSTP |
| Instance Priority | 12288 |
| Bridge Mac Address | 00:40:c7:33:00:d1 |
| MSTI REGIONAL ROOT PRIORITY | 12288 |
| MSTI REGIONAL ROOT MAC | 00:40:c7:33:00:d1 |
| MSTI INTERNAL ROOT PATH COST | 0 |
| MSTI ROOT PORT ID | 0 |
| TIME SINCE LAST TOPOLOGY CHANGE(SECS) | 1405 |
| TOPOLOGY CHANGE COUNT(SECS) | 0 |

Refresh

Fig. 3-121

Instance ID=0

Instance Status (ID=0)

| | |
|---------------------------------------|-------------------|
| MSTP State | Enabled |
| Force Version | MSTP |
| Bridge Max Age | 20 |
| Bridge Forward Delay | 15 |
| Bridge Max Hops | 20 |
| Instance Priority | 32768 |
| Bridge Mac Address | 00:40:c7:33:00:d1 |
| CIST ROOT PRIORITY | 32768 |
| CIST ROOT MAC | 00:40:c7:33:00:d1 |
| CIST EXTERNAL ROOT PATH COST | 0 |
| CIST ROOT PORT ID | 0 |
| CIST REGIONAL ROOT PRIORITY | 32768 |
| CIST REGIONAL ROOT MAC | 00:40:c7:33:00:d1 |
| CIST INTERNAL ROOT PATH COST | 0 |
| CIST CURRENT MAX AGE | 20 |
| CIST CURRENT FORWARD DELAY | 15 |
| TIME SINCE LAST TOPOLOGY CHANGE(SECS) | 8374 |
| TOPOLOGY CHANGE COUNT(SECS) | 0 |

Refresh

Fig. 3-122

MSTP State:

MSTP protocol is Enable or Disable.

Force Version:

It shows the current spanning tree protocol version configured.

Bridge Max Age:

It shows the Max Age setting of the bridge itself.

Bridge Forward Delay:

It shows the Forward Delay setting of the bridge itself.

Bridge Max Hops:

It shows the Max Hops setting of the bridge itself.

Instance Priority:

Spanning tree priority value for a specific tree instance(CIST or MSTI)

Bridge Mac Address:

The Mac Address of the bridge itself.

CIST ROOT PRIORITY:

Spanning tree priority value of the CIST root bridge

CIST ROOT MAC:

Mac Address of the CIST root bridge

CIST EXTERNAL ROOT PATH COST:

Root path cost value from the point of view of the bridge's MST region.

CIST ROOT PORT ID:

The port ID of the bridge's root port. In MSTP, peer port of a root port may reside in different MST region or in the same MST region. The first case indicates that the root port's owner is the CIST regional root bridge.

CIST REGIONAL ROOT PRIORITY:

Spanning tree priority value of the CIST regional root bridge. Note that CIST Regional Root bridge is different from CIST Root bridge. One exception is that when a bridge belonging to an MST region happens to be the root bridge of the CST (Common Spanning Tree). An MST Region in the CST can be regarded as a common RSTP bridge. The IST (Internal Spanning Tree) and MSTIs are transparent to bridges outside this region.

CIST REGIONAL ROOT MAC:

Mac Address of the CIST regional root bridge.

CIST INTERNAL ROOT PATH COST:

Root path cost value from the point of view of the bridges inside the IST.

CIST CURRENT MAX AGE:

Max Age of the CIST Root bridge.

CIST CURRENT FORWARD DELAY:

Forward Delay of the CIST Root bridge.

TIME SINCE LAST TOPOLOGY CHANGE(SECs):

Time Since Last Topology Change is the elapsed time in unit of seconds for a bunch of "Topology Change and(or) Topology

Change Notification receiving” to occur. When new series of Topology Changes occur again, this counter will be reset to 0.

TOPOLOGY CHANGE COUNT(SECs):

The per spanning tree instanceTopology Change Count expresses the time spent in unit of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once there is no topology change occurring and no more topology change notification received, the Topology Change count will be reset to 0.

Port Status:

To show the status report of all ports regarding a specific spanning tree instance.

Step :To select an existed entry, then click **<Port Status>** button.

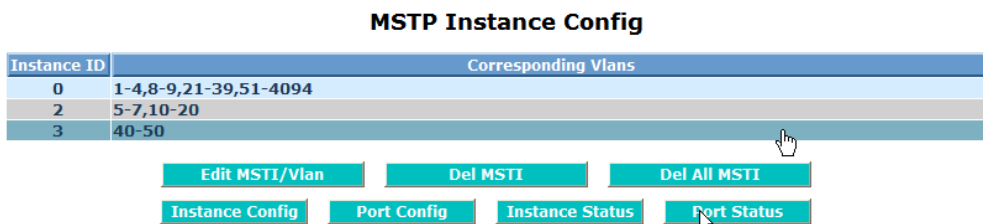


Fig. 3-123

Port Status of Instance 3

| Refresh | | | | | | | | | |
|---------|------------|------|-----------|----------|-------|------------|-----------|-----------------|----------------|
| Port No | Status | Role | Path Cost | Priority | Hello | Oper. Edge | Oper. P2P | Restricted Role | Restricted Tcn |
| 1 | DISCARDING | dsbl | 10 | 64 | 2/2 | V | V | | |
| 2 | DISCARDING | dsbl | 200000 | 128 | 2/2 | V | V | | |
| 3 | DISCARDING | dsbl | 200000 | 128 | 2/2 | V | V | | |
| 4 | DISCARDING | dsbl | 200000 | 128 | 2/2 | V | V | | |
| 5 | DISCARDING | dsbl | 200000 | 128 | 2/2 | V | V | | |
| 6 | DISCARDING | dsbl | 200000 | 128 | 2/2 | V | V | | |
| 7 | DISCARDING | dsbl | 200000 | 128 | 2/2 | V | V | | |
| 8 | DISCARDING | dsbl | 200000 | 128 | 2/2 | V | V | | |
| 9 | DISCARDING | dsbl | 200000 | 128 | 2/2 | V | V | | |
| 10 | DISCARDING | dsbl | 200000 | 128 | 2/2 | V | V | | |

Refresh

Fig. 3-124

Port No:

1-10

Status:

The forwarding status. Same definition as of the RSTP specification Possible values are “FORWARDING”, “LEARNING”, “DISCARDING”.

Role:

The role that a port plays in the spanning tree topology. Possible

values are “dsbl”(disable port) , “alt”(alternate port) , “bkup”(backup port) , “ROOT”(root port) , “DSGN”(designated port) , “MSTR”(master port). The last 3 are possible port roles for a port to transit to FORWARDING state

Path Cost:

Display currently resolved port path cost value for each port in a particular spanning tree instance.

Priority:

Display port priority value for each port in a particular spanning tree instance.

Hello:

per port Hello Time display. It takes the following form:

Current Hello Time/Hello Time Setting

Oper. Edge:

Whether or not a port is an Edge Port in reality.

Oper. P2P:

Whether or not a port is a Point-to-Point Port in reality.

Restricted Role:

Same as mentioned in “Port Config”

Restricted Tcn:

Same as mentioned in “Port Config”

3-16. Trunk

The Port Trunking Configuration is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipments to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

The switch supports two kinds of port trunking methods:

LACP:

Ports using Link Aggregation Control Protocol (according to IEEE 802.3ad specification) as their trunking method can choose their unique LACP GroupID (1~3) to form a logic “trunked port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “trunk group” (also called aggregator). LACP is safer than the other trunking method - static trunk.

The switch LACP does not support the followings:

- Link Aggregation across switches
- Aggregation with non-IEEE 802.3 MAC link
- Operating in half-duplex mode
- Aggregate the ports with different data rates

Static Trunk:

Ports using Static Trunk as their trunk method can choose their unique Static GroupID (also 1~3, this Static groupID can be the same with another LACP groupID) to form a logic “trunked port”. The benefit of using Static Trunk method is that a port can immediately become a member of a trunk group without any handshaking with its peer port. This is also a disadvantage because the peer ports of your static trunk group may not know that they should be aggregate together to form a “logic trunked port”. Using Static Trunk on both end of a link is strongly recommended. Please also note that low speed links will stay in “not ready” state when using static trunk to aggregate with high speed links.

As to system restrictions about the port aggregation function on the switch, In the management point of view, the switch supports maximum 3 trunk groups for LACP and additional 4 trunk groups for Static Trunk. But in the system capability view, only 4 “real trunked” groups are supported. An LACP trunk group with more than one ready member-ports is a “real trunked” group. An LACP trunk group with only one or less than one ready member-ports is not a “real trunked” group. Any Static trunk group is a “real trunked” group.

3-16-1. Port

Function name:

Port Setting/Status

Function description:

Port setting/status is used to configure the trunk property of each and every port in the switch system.

Trunk Port Setting/Status

| Trunk Port Setting | | | | Trunk Port Status | |
|--------------------|--------|-------|-------------|-------------------|--------|
| Port | Method | Group | Active LACP | Aggtr | Status |
| 1 | LACP ▾ | 1 ▾ | Active ▾ | 1 | --- |
| 2 | LACP ▾ | 1 ▾ | Active ▾ | 2 | --- |
| 3 | None ▾ | 0 ▾ | Active ▾ | 3 | --- |
| 4 | None ▾ | 0 ▾ | Active ▾ | 4 | --- |
| 5 | None ▾ | 0 ▾ | Active ▾ | 5 | --- |
| 6 | None ▾ | 0 ▾ | Active ▾ | 6 | --- |
| 7 | None ▾ | 0 ▾ | Active ▾ | 7 | --- |
| 8 | None ▾ | 0 ▾ | Active ▾ | 8 | --- |
| 9 | None ▾ | 0 ▾ | Active ▾ | 9 | Ready |
| 10 | None ▾ | 0 ▾ | Active ▾ | 10 | --- |

Apply/Refresh

Fig. 3-125

Parameter description:

Method:

This determines the method a port uses to aggregate with other ports.

None:

A port does not want to aggregate with any other port should choose this default setting.

LACP:

A port use LACP as its trunk method to get aggregated with other ports.

Static:

A port use Static Trunk as its trunk method to get aggregated with other ports.

Group:

Ports choosing the same trunking method other than “None” must be assigned a unique Group number (i.e. Group ID, valid value is from 1 to 4) in order to declare that they wish to aggregate with each other.

Active LACP:

This field is only referenced when a port’s trunking method is LACP.

Active:

An Active LACP port begins to send LACPDU to its link partner right after the LACP protocol entity started to take control of this port.

Passive:

A Passive LACP port will not actively send LACPDU out before it receives an LACPDU from its link partner.

Aggtr:

Aggtr is an abbreviation of “aggregator”. Every port is also an aggregator, and its own aggregator ID is the same as its own Port No. We can regard an aggregator as a representative of a trunking group. Ports with same Group ID and using same trunking method will have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest Port No. within the trunking group.

Status:

This field represents the trunking status of a port which uses a trunking method other than “None”. It also represents the management link status of a port which uses the “None” trunking method. “---” means “not ready”

3-16-2. Aggregator View

Function name:

Aggregator View

Function description:

To display the current port trunking information from the aggregator point of view.

| Aggregator View | | | |
|-----------------|--------|--------------|-------------|
| Aggregator | Method | Member Ports | Ready Ports |
| 1 | None | 1 | |
| 2 | None | 2 | |
| 3 | None | 3 | 3 |
| 4 | None | 4 | |
| 5 | None | 5 | |
| 6 | None | 6 | |
| 7 | None | 7 | |
| 8 | None | 8 | |
| 9 | None | 9 | 9 |
| 10 | None | 10 | |

Refresh

LACP Detail

Fig. 3-126

Parameter description:

Aggregator:

It shows the aggregator ID (from 1 to 10) of every port. In fact, every port is also an aggregator, and its own aggregator ID is the same as its own Port No..

Method:

Show the method a port uses to aggregate with other ports.

Member Ports:

Show all member ports of an aggregator (port).

Ready Ports:

Show only the ready member ports within an aggregator (port).

LACP Detail (LACP Aggregator Detailed Information)

Show the detailed information of the LACP trunking group.

Step: To select an existed entry, then click **<LACP Detail>** button

Aggregator View

| Aggregator | Method | Member Ports | Ready Ports |
|------------|--------|--------------|-------------|
| 1 | LACP | 1 | |
| 2 | LACP | 2 | |
| 3 | Static | 3, 5 | |
| 4 | None | 4 | |
| 5 | Static | | |
| 6 | None | 6 | |
| 7 | None | 7 | |
| 8 | None | 8 | |
| 9 | None | 9 | 9 |
| 10 | None | 10 | |

Refresh

LACP Detail

Fig. 3-127

Aggregator 2 Information

| Actor | | | Partner | |
|-----------------|-------------------|--------------|-----------------|-------------------|
| System Priority | MAC Address | | System Priority | MAC Address |
| 32768 | 00-40-c7-33-00-d1 | | 32768 | 00-00-00-00-00-00 |
| Port | Key | Trunk Status | Port | Key |
| 2 | 258 | --- | 2 | 0 |

Fig. 3-128

Actor:

The switch you are watching on.

Partner:

The peer system from this aggregator's view.

System Priority:

Show the System Priority part of a system ID.

MAC Address:

Show the MAC Address part of a system ID.

Port:

Show the port number part of an LACP port ID.

Key:

Show the key value of the aggregator. The key value is determined by the LACP protocol entity and can't be set through management.

Trunk Status:

Show the trunk status of a single member port. "---" means "not ready"

3-16-3. LACP System Config

Function name:

LACP System Configuration

Function description:

It is used to set the priority part of the LACP system ID. LACP will only aggregate together the ports whose peer link partners are all on a single system. Each system supports LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising a 48-bit MAC Address and 16-bit priority value.

LACP System Configuration

System Priority 32768 (1~65535)

Hash Method DA and SA

Note: This hash method applies to both LACP and static trunk.

Apply

Fig. 3-129

Parameter description:

System Priority:

The System Priority can be set by the user. Its range is from 1 to 65535.
Default: 32768.

LACP Hash Method:

DA+SA, DA and SA are three Hash methods offered for the Link Aggregation of the switch. Packets will decide the path to transmit according to the mode of Hash you choose.

Default: DA and SA

3-17. 802.1x Configuration

IEEE 802.1x port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through an IEEE 802.1x-enabled port without authentication. If a user wishes to touch the network through a port under IEEE 802.1x control, he (she) must firstly input his (her) account name for authentication and waits for gaining authorization before sending or receiving any packets from an IEEE 802.1x-enabled port.

Before the devices or end stations can access the network resources through the ports under IEEE 802.1x control, the devices or end stations connected to a controlled port send the authentication request to the authenticator, the authenticator pass the request to the authentication server to authenticate and verify, and the server tell the authenticator if the request get the grant of authorization for the ports.

According to IEEE 802.1x, there are three components implemented. They are Authenticator, Supplicant and Authentication server shown in Fig. 3-130.

Supplicant:

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE request to it.

Authenticator:

An entity facilitates the authentication of the supplicant entity. It controls the state of the port, authorized or unauthorized, according to the result of authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once start re-authenticating the supplicant, the controlled port keeps in the authorized state until re-authentication fails.

A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass the packets when the authenticator PAE is authorized, and otherwise, an uncontrolled port will unconditionally pass the packets with PAE group MAC address, which has the value of 01-80-c2-00-00-03 and will not be forwarded by MAC bridge, at any time.

Authentication server:

A device provides authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorized to access the network resource.

The overview of operation flow for the Fig. 3-130 is quite simple. When Supplicant PAE issues a request to Authenticator PAE, Authenticator and Supplicant exchanges authentication message. Then, Authenticator passes the request to RADIUS server to verify. Finally, RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the message to authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only touch the authenticator to perform authentication message exchange or access the network from the uncontrolled port.

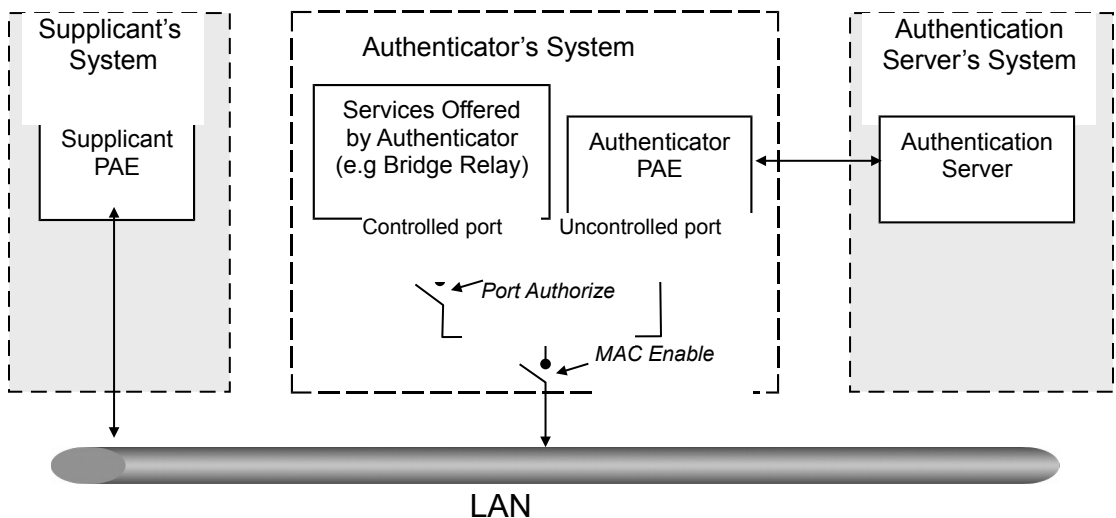


Fig. 3-130

In the Fig. 3-110, this is the typical configuration, a single supplicant, an authenticator and an authentication server. B and C is in the internal network, D is Authentication server running RADIUS, switch at the central location acts Authenticator connecting to PC A and A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C, first, it must exchange the authentication message with the authenticator on the port it connected via EAPOL packet. The authenticator transfers the supplicant's credentials to Authentication server for verification. If success, the authentication server will notice the authenticator the grant. PC A, then, is allowed to access B and C via the switch. If there are two switches directly connected together instead of single one, for the link connecting two switches, it may have to act two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.

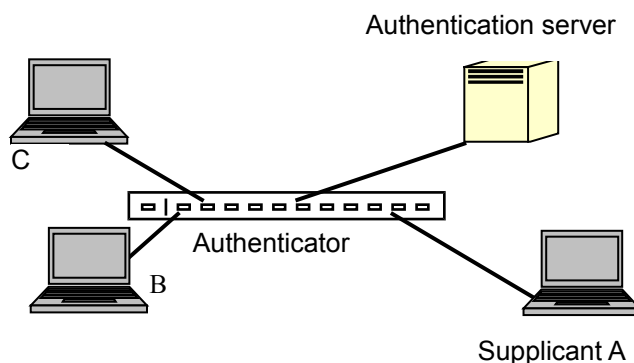


Fig. 3-131

The Fig. 3-131 shows the procedure of 802.1x authentication. There are steps for the login based on 802.1x port access control management. The protocol used in the right side is EAPOL and the left side is EAP.

1. At the initial stage, the supplicant A is unauthenticated and a port on switch acting as an authenticator is in unauthorized state. So the access is blocked in this stage.
2. Initiating a session. Either authenticator or supplicant can initiate the message exchange. If supplicant initiates the process, it sends EAPOL-start packet to the authenticator PAE and authenticator will immediately respond EAP-Request/Identity packet.
3. The authenticator always periodically sends EAP-Request/Identity to the supplicant for requesting the identity it wants to be authenticated.
4. If the authenticator doesn't send EAP-Request/Identity, the supplicant will initiate EAPOL-Start the process by sending to the authenticator.
5. And next, the Supplicant replies an EAP-Response/Identity to the authenticator. The authenticator will embed the user ID into Radius-Access-Request command and send it to the authentication server for confirming its identity.
6. After receiving the Radius-Access-Request, the authentication server sends Radius-Access-Challenge to the supplicant for asking for inputting user password via the authenticator PAE.
7. The supplicant will convert user password into the credential information, perhaps, in MD5 format and replies an EAP-Response with this credential information as well as the specified authentication algorithm (MD5 or OTP) to Authentication server via the authenticator PAE. As per the value of the type field in message PDU, the authentication server knows which algorithm should be applied to authenticate the credential information, EAP-MD5

(Message Digest 5) or EAP-OTP (One Time Password) or other else algorithm. If user ID and password is correct, the authentication server will send a Radius-Access-Accept to the authenticator. If not correct, the authentication server will send a Radius-Access-Reject.

8. When the authenticator PAE receives a Radius-Access-Accept, it will send an EAP-Success to the supplicant. At this time, the supplicant is authorized and the port connected to the supplicant and under 802.1x control is in the authorized state. The supplicant and other devices connected to this port can access the network. If the authenticator receives a Radius-Access-Reject, it will send an EAP-Failure to the supplicant. This means the supplicant is failed to authenticate. The port it connected is in the unauthorized state, the supplicant and the devices connected to this port won't be allowed to access the network.
9. When the supplicant issue an EAP-Logoff message to Authentication server, the port you are using is set to be unauthorized.

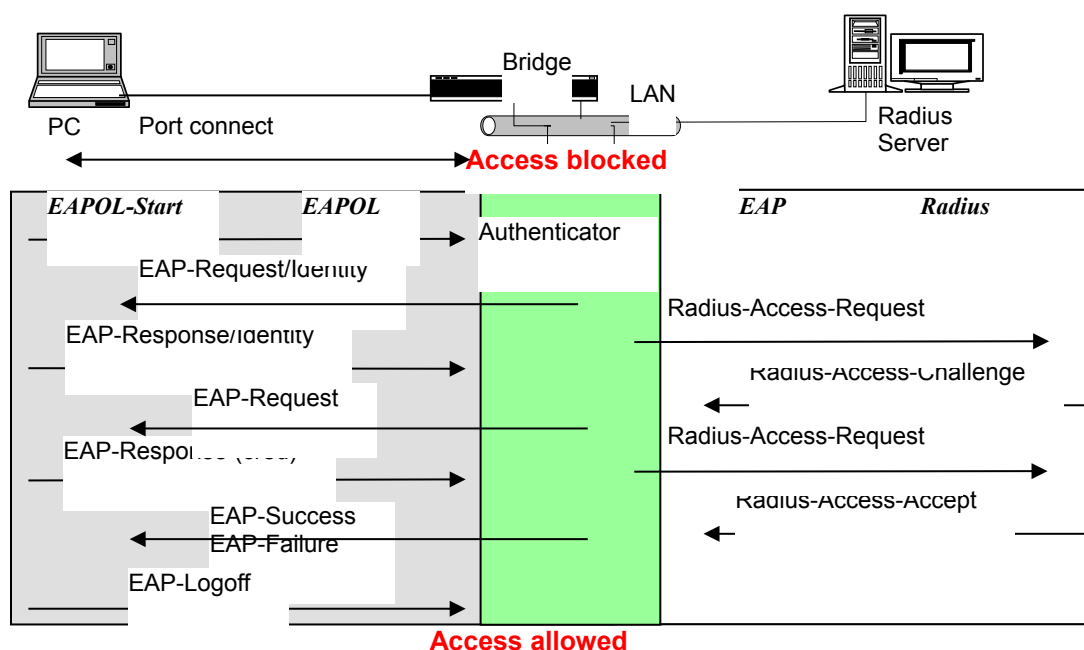


Fig. 3-132

Only MultiHost 802.1X is the type of authentication supported in the switch. In this mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

IEEE 802.1x Port-based Network Access Control function supported by the switch is little bit complex, for it just support basic Multihost mode, which can distinguish the device's MAC address and its VID. The following table is the summary of the combination of the authentication status and the port status versus the status of port mode, set in 802.1x Port mode, port control state, set in 802.1x port setting. Here Entry Authorized means MAC entry is authorized.

| Port Mode | Port Control | Authentication | Port Status |
|-----------|-------------------|----------------|-------------------|
| Disable | Don't Care | Don't Care | Port Uncontrolled |
| Multihost | Auto | Successful | Port Authorized |
| Multihost | Auto | Failure | Port Unauthorized |
| Multihost | ForceUnauthorized | Don't Care | Port Unauthorized |
| Multihost | ForceAuthorized | Don't Care | Port Authorized |

Table 3-3

3-17-1. State

Function name:

802.1x State Setting

Function description:

This function is used to configure the global parameters for RADIUS authentication in IEEE 802.1x port security application.

802.1X State Setting

| | |
|--------------------------|--|
| Radius Server 1 | <input type="text" value="192.168.1.1"/> |
| Port Number(1~65535) | <input type="text" value="1812"/> |
| Radius Server 2 | <input type="text" value="192.168.1.1"/> |
| Port Number(1~65535) | <input type="text" value="1812"/> |
| Secret Key | <input type="text" value="Radius"/> |
| Accounting Service | <input type="button" value="Enable"/> |
| Accounting Server 1 | <input type="text" value="192.168.1.1"/> |
| Accounting Port(1~65535) | <input type="text" value="1813"/> |
| Accounting Server 2 | <input type="text" value="192.168.1.1"/> |
| Accounting Port(1~65535) | <input type="text" value="1813"/> |
| Secret Key | <input type="text" value="Radius"/> |

Fig.3-133

Parameter description:

Radius Server:

RADIUS server IP address for authentication.

Default: 192.168.1.1

Port Number:

The port number to communicate with RADIUS server for the authentication service. The valid value ranges 1-65535.

Default port number is 1812.

Accounting Port:

The port number to communicate with Accounting server for the authentication service. The valid value ranges 1-65535.

Default port number is 1813.

Secret Key:

The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9.

Default: Radius

3-17-2. Mode

Function name:

802.1x Mode Setting

Function description:

Set the operation mode of 802.1X for each port. In this device, it supports only Multi-host operation mode.

802.1X Mode Setting

| Port | 802.1X Mode |
|------|-----------------|
| 1 | Disable |
| 2 | Disable |
| 3 | Normal |
| 4 | Advanced 802.1X |
| 5 | Disable |
| 6 | Disable |
| 7 | Disable |
| 8 | Disable |
| 9 | Disable |
| 10 | Disable |

Apply

Fig. 3-134

Parameter description:

Port Number:

Indicate which port is selected to configure the 802.1x operation mode.

802.1x Mode:

802.1x operation mode. There are two options, including Disable and Multi-host mode. Default is Disable.

■ Disable

It will have the chosen port acting as a plain port, that is no 802.1x port access control works on the port.

■ Normal

In normal mode, for the devices connected to this port, once a supplicant is authorized, the devices connected to this port can access the network resource through this port.

■ Advanced 802.1x

In Advanced 802.1x mode, for the devices connected to this port, all supplicant are need to authenticate.

3-17-3. Security

Function name:

Port Security Management

Function description:

Shows each port status. In Multihost mode, it shows the port number and its status, authorized or unauthorized.

Port Security Management

| Port | Mode | Status |
|------|-----------------|------------------------|
| 1 | Normal | Unauthorized |
| 2 | Advanced 802.1X | Authorized Entries : 0 |
| 3 | disable | |
| 4 | disable | |
| 5 | disable | |
| 6 | disable | |
| 7 | disable | |
| 8 | disable | |
| 9 | disable | |
| 10 | disable | |

Param. Setting

Fig. 3-135

Parameter description:

Port:

The port number to be chosen to show its 802.1X Port Status. The valid number is Port 1 – 10.

Mode:

When selecting Disable mode for a port in the function 802.1X Port Mode Configuration, the port is in the uncontrolled port state and does not apply 802.1X authenticator on it. Any node attached on this port can access the network without the admittance of 802.1X authenticator.

Status:

The current 802.1X status of the port.

Param. Setting:

The function is used to configure the parameters for each port in 802.1X port security application.

Step 1: To select a port entry, then click **<Param. Setting>** button

Step 2: To select Port Control and input reAuthMax, txPeriod, quiet Period...etc.(if necessary), then click **<Apply>** button

Port Security Management

| Port | Mode | Status |
|------|-----------------|------------------------|
| 1 | Normal | Unauthorized |
| 2 | Advanced 802.1X | Authorized Entries : 0 |
| 3 | disable | |
| 4 | disable | |
| 5 | disable | |
| 6 | disable | |
| 7 | disable | |
| 8 | disable | |
| 9 | disable | |
| 10 | disable | |

Param. Setting

Fig. 3-136

Port Parameter Setting

| | |
|-------------------------|------|
| Port | 2 |
| Port Control | Auto |
| reAuthMax(1-10) | 2 |
| txPeriod(1-65535 s) | 30 |
| Quiet Period(0-65535 s) | 60 |
| reAuthEnabled | ON |
| reAuthPeriod(1-65535 s) | 120 |
| max. Request(1-10) | 2 |
| suppTimeout(1-255 s) | 30 |
| serverTimeout(1-255 s) | 30 |

Apply

Fig. 3-137

Port:

It is the port number to be selected for configuring its associated 802.1X parameters which are Port control, reAuthMax, txPeriod, Quiet Period, reAuthEnabled, reAuthPeriod, max. Request, suppTimeout, serverTimeout and Controlled direction.

Port Control:

This is used to set the operation mode of authorization. There are three type of operation mode supported, ForceUnauthorized, ForceAuthorized, Auto.

- ForceUnauthorized:

The controlled port is forced to hold in the unauthorized state.

- ForceAuthorized:

The controlled port is forced to hold in the authorized state.

- Auto:

The controlled port is set to be in authorized state or unauthorized state depends on the result of the authentication exchange between the authentication server and the supplicant.

Default: Auto

reAuthMax(1-10):

The number of authentication attempt that is permitted before the port becomes unauthorized.

Default: 2

txPeriod(1-65535 s):

A time period to transmitted EAPOL PDU between the authenticator and the supplicant.

Default: 30

Quiet Period(0-65535 s):

A period of time during which we will not attempt to access the supplicant.

Default: 60 seconds

reAuthEnabled:

Choose whether regular authentication will take place in this port.

Default: ON

reAuthPeriod(1-65535 s):

A non-zero number seconds between the periodic re-authentication of the supplicant.

Default: 120

max. Request(1-10):

The maximum of number times that the authenticator will retransmit an EAP Request to the supplicant before it times out the authentication session. The valid range: 1 – 10.

Default: 2 times

suppTimeout(1-255 s):

A timeout condition in the exchange between the authenticator and the supplicant. The valid range: 1 –255.

Default: 30 seconds.

serverTimeout(1-255 s):

A timeout condition in the exchange between the authenticator and the authentication server. The valid range: 1 –255.

Default: 30 seconds

3-18. TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol which provides access control for the switch via one or more centralized servers. It provides separate authentication, authorization and accounting services. TACACS+ utilizes [TCP](#) port 49. It consists of three separate protocols, which can, if desired, be implemented on separate servers.

3-18-1. State

Function name:

TACACS+ Setting

Function description:

The switch supports the TACACS+ is facilitated through AAA and can be enabled only through AAA commands which detailed accounting information and flexible administrative control over authentication and authorization processes. Providing to set TACACS+ Server IP address and Secret Key.

TACACS+ Setting

| | | |
|------------|--------------------------------------|--------------------|
| Server 1 | <input type="text" value="0.0.0.0"/> | 0.0.0.0 is Disable |
| Server 2 | <input type="text" value="0.0.0.0"/> | |
| Secret Key | <input type="text" value="TACACS"/> | |

Apply

Fig. 3-138

Parameter description:

Server 1:

Server 1 IP address for authentication.

Default: 0.0.0.0

Server 2:

Server 2 IP address for authentication.

Default: 0.0.0.0

Secret Key:

The secret key between authentication server and authenticator. It is a string with the length 1 – 31 characters. The character string may contain upper case, lower case and 0-9. It is character sense.

Default: TACACS

3-18-2. Authentication

Function name:

Authentication Configuration

Function description:

The switch supports including Console, Telnet and Web authentication method via TACACS+ server.

Authentication Configuration

| Authentication | Login Primary | Login Secondary |
|----------------|---------------|-----------------|
| Console | Local ▼ | None ▼ |
| Telnet | Local ▼ | None ▼ |
| Web | Local ▼ | None ▼ |

| | |
|----------------------|---------|
| Authentication retry | 3 (1-3) |
|----------------------|---------|

Apply

Fig. 3-139

Parameter description:

Console:

To set Console authentication method with Login primary or Login secondary.

Default: Primary is "Local" and Secondary is "None"

Telnet:

To set Telnet authentication method with Login primary or Login secondary.

Default: Primary is "Local" and Secondary is "None"

Web:

To set Web authentication method with Login primary or Login secondary.

Default: Primary is "Local" and Secondary is "None"

Authentication retry:

To set the Authentication retry for all three login authentication methods.

Range: 1-3 and default is 3

3-18-3. Authorization

Function name:

Authorization Configuration

Function description:

The switch supports TACACS+ server Authorization method with “State” and “Fallback to Local Authorization “.

Authorization

| | |
|---------------------------------|-----------|
| State | Disable ▼ |
| Fallback to Local Authorization | Disable ▼ |

Apply

Fig. 3-140

Parameter description:

State:

To enable or disable the State Authorization via TACACS+ Server.

Default: Disable

Fallback to Local Authorization:

To enable or disable the switch Fallback to Local Authorization.

Default: Disable

3-18-4. Accounting

Function name:

Accounting Configuration

Function description:

The switch supports TACACS+ server Accounting method with “Enable” and “Disable “ for manage login traffic accounting.

Accounting

| | |
|-------|-----------|
| State | Disable ▼ |
|-------|-----------|

Apply

Fig. 3-141

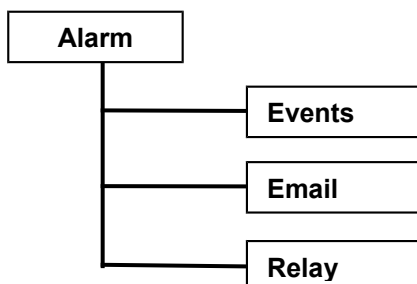
Parameter description:

State:

To enable or disable the accounting via TACACS+ Server.

Default: Disable

3-19. Alarm



3-19-1. Events

Function name:

Events Configuration

Function description:

The Events Configuration function is used to enable the switch to send out the events information while pre-defined trap events occurred. The switch offers 27 different trap events to users for switch management. The trap information can be sent out in two ways, including email and trap. The message will be sent while users tick (☐) the trap event individually on the web page shown as below.

Trap Events Configuration

Email Select/Unselect All ☐

Trap Select/Unselect All ☐

| Event | Email | Trap |
|-------------------------|--------------------------|-------------------------------------|
| Cold Start | ☐ | ☒ |
| Warm Start | ☐ | ☒ |
| Link Down | ☐ | ☒ |
| Link Up | ☐ | ☒ |
| Authentication Failure | ☐ | ☒ |
| User Login | ☐ | ☐ |
| User Logout | ☐ | ☐ |
| STP Topology Changed | ☐ | ☐ |
| STP Disabled | ☐ | ☐ |
| STP Enabled | ☐ | ☐ |
| LACP Disabled | ☐ | ☐ |
| LACP Enabled | ☐ | ☐ |
| LACP Member Added | ☐ | ☐ |
| LACP Port Failure | ☐ | ☐ |
| GVRP Disabled | ☐ | ☐ |
| GVRP Enabled | ☐ | ☐ |
| Port-based Vlan Enabled | ☐ | ☐ |
| Tag-based Vlan Enabled | ☐ | ☐ |
| Metro-mode Vlan Enabled | ☐ | ☐ |
| Module Inserted | ☐ | ☐ |
| Module Removed | ☐ | ☐ |
| Dual Media Swapped | ☐ | ☐ |
| Looping Detected | ☐ | ☐ |
| IP-MAC Binding Offered | ☐ | ☐ |
| IP-MAC Binding Released | ☐ | ☐ |
| ARP Inspection Detected | ☐ | ☐ |
| Power Monitor | ☐ | ☐ |

[Apply](#)

Parameter description:

Trap: Cold Start, Warm Start, Link Down, Link Up, Authentication Failure, User login, User logout

STP: STP Topology Changed, STP Disabled, STP Enabled

LACP: LACP Disabled, LACP Enabled, LACP Member Added, LACP Port Failure

GVRP: GVRP Disabled, GVRP Enabled

VLAN: Port-based VLAN Enabled, Tag-based VLAN Enabled, Metro-mode VLAN enabled

Module Swap: Module Inserted, Module Removed, Dual Media Swapped

IP MAC Binding: Offered, Released

Looping Detected, ARP Inspection Detected, Power Monitor

3-19-2. Email

Function name:

Email Configuration

Function description:

Alarm configuration is used to configure the persons who should receive the alarm message via email. An email address has to be set in the web page of alarm configuration (See Fig. 3-72). Then, user can read the trap information from the email. This function provides 6 email addresses at most. The 27 different trap events will be sent out to SNMP Manager when trap event occurs. After ticking trap events, you can fill in your desired email addresses. Then, please click **<Apply>** button to complete the alarm configuration. It will take effect in a few seconds.

Alarm Configuration

| | |
|-----------------|----------------------|
| Mail Server | <input type="text"/> |
| Username | <input type="text"/> |
| Password | <input type="text"/> |
| Sender | <input type="text"/> |
| Return-Path | <input type="text"/> |
| Email Address 1 | <input type="text"/> |
| Email Address 2 | <input type="text"/> |
| Email Address 3 | <input type="text"/> |
| Email Address 4 | <input type="text"/> |
| Email Address 5 | <input type="text"/> |
| Email Address 6 | <input type="text"/> |

Fig. 3-143

Parameter description:

Email:

Mail Server: the IP address of the server transferring your email.

Username: your username on the mail server.

Password: your password on the mail server.

Email Address 1 – 6: Email address that would like to receive the alarm message.

3-19-3. Relay

Function name:

Relay

Function description:

Provide “Power Monitoring” and “Port Monitoring” function. Users could set easily through UI “Select/Unselect all”.

Alarm Relay

| | |
|-------------------------|--|
| Power Monitoring | A. ☒ B. ☒ C. ☒ |
| Port Monitoring | 1. ☐ 2. ☐ 3. ☐ 4. ☐ 5. ☐ 6. ☐ 7. ☐ 8. ☐
9. ☒ 10. ☒ Port Select/Unselect All ☐ |

Fig. 3-144

Parameter description:

Power Monitoring:

A: Power A on terminal block.

B: Power B on terminal block.

C: Power C DC Jack.

Default : A, B, C

Port Monitoring:

Port 1~10.

Default : Port 9~10

Port Select / Unselect All : Click to select or unselect all.

3-20. Configuration

The switch supports three copies of configuration, including the default configuration, working configuration and user configuration for your configuration management. All of them are listed and described below respectively.

- **Default Configuration:**

This is Manufacturetech's setting and cannot be altered. In Web UI, two restore default functions are offered for the user to restore to the default setting of the switch. One is the function of "Restore Default Configuration included default IP address", the IP address will restore to default "192.168.1.1" as you use it. The other is the function of "Restore Default Configuration without changing current IP address", the IP address will keep the same one that you had saved before by performing this function.

- **Working Configuration:**

It is the configuration you are using currently and can be changed any time. The configurations you are using are saved into this configuration file. This is updated each time as you click **<Apply>** button.

- **User Configuration:**

It is the configuration file for the specified or backup purposes and can be updated while having confirmed the configuration. You can retrieve it by performing Restore User Configuration.

| Configuration | |
|-----------------|---|
| Save Start | Save as Start Configuration |
| Save User | Save as User Configuration |
| Restore Default | Restore Default Configuration including default ip address |
| Restore Default | Restore Default Configuration without changing current ip address |
| Restore User | Restore User Configuration |

Fig. 3-145

3-20-1. Save/Restore

Function name:

Save As Start Configuration

Function description:

Save the current configuration as a start configuration file in flash memory.

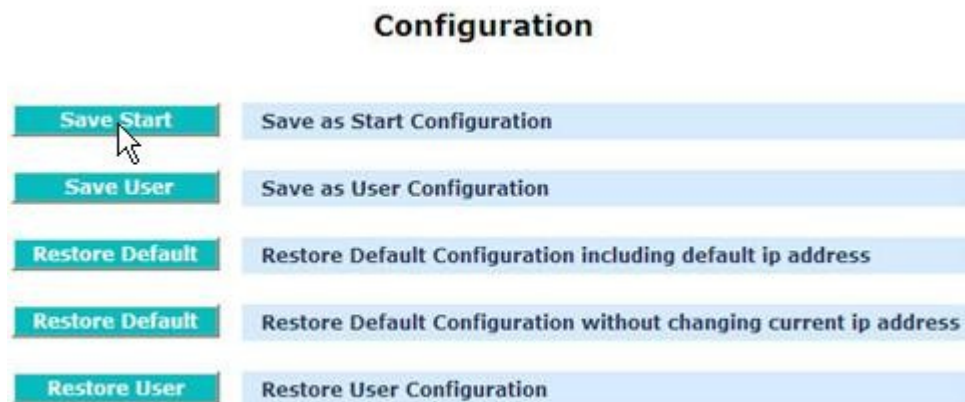


Fig. 3-146

Function name:

Save As User Configuration

Function description:

Save the current configuration as a user configuration file in flash memory.

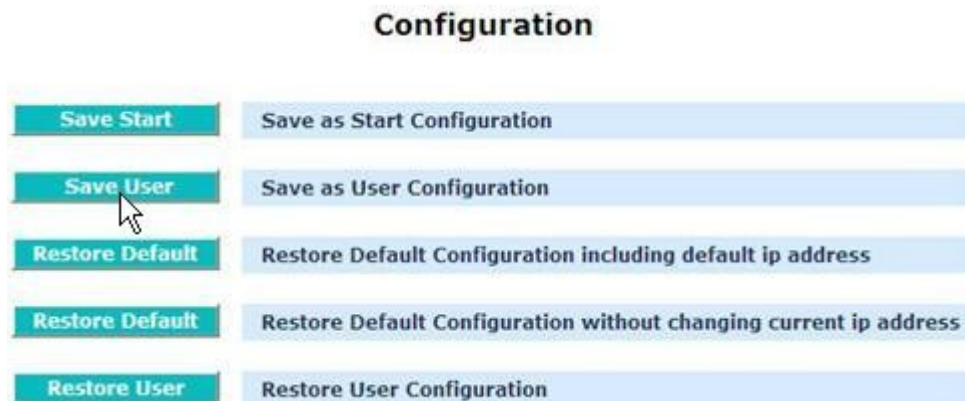


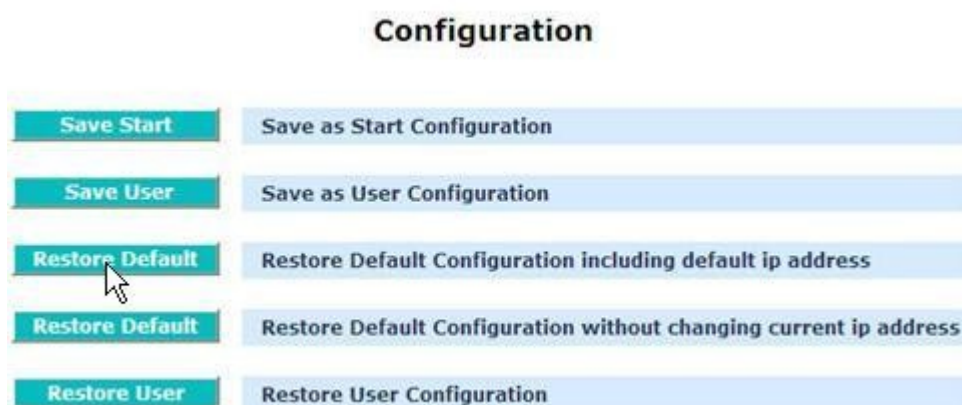
Fig. 3-147

Function name:

Restore Default Configuration (includes default IP address)

Function description:

Restore Default Configuration function can retrieve Manufacturetech's setting to replace the start configuration. And the IP address of the switch will also be restored to 192.168.1.1.



Restore Default Configuration Successfully



Fig. 3-148

Function name:

Restore Default Configuration (excludes current IP address)

Function description:

Restore Default Configuration function can retrieve Manufacturetech's setting to replace the start configuration. However, the switch's current IP address that the user set up will not be changed and will not be restored to 192.168.1.1 as well.



Restore Default Configuration Successfully

Reboot the system to take effect for the setting?

Reboot

Fig. 3-149

Function name:

Restore User Configuration

Function description:

Restore User Configuration function can retrieve the previous confirmed working configuration stored in the flash memory to update start configuration. When completing to restore the configuration, the system's start configuration is updated and will be changed its system settings after rebooting the system.

Configuration

| | |
|-----------------|---|
| Save Start | Save as Start Configuration |
| Save User | Save as User Configuration |
| Restore Default | Restore Default Configuration including default ip address |
| Restore Default | Restore Default Configuration without changing current ip address |
| Restore User | Restore User Configuration |

Restore User Configuration Successfully

Reboot the system to take effect for the setting?

Reboot

Fig. 3-150

3-20-2. Config File

Function name:

Config File

Function description:

With this function, user can back up or reload the config files of Save As Start or Save As User via TFTP.

Configure Export/Import File Path

| | |
|------------------|---|
| TFTP Server IP | 0.0.0.0 |
| Export File Path | <input type="text"/> |
| | <input type="button" value="Export Start"/> <input type="button" value="Export User-Conf"/> |
| Import File Path | <input type="text"/> |
| | <input type="button" value="Import Start"/> <input type="button" value="Import User-Conf"/> |

Fig. 3-151

Parameter description:

TFTP Server IP:

Display the TFTP Server. "0.0.0.0" will be shown if no TFTP server.

Export File Path:

Export Start:

Export Save As Start's config file stored in the flash.

Export User-Conf:

Export Save As User's config file stored in the flash.

Import File Path:

Import Start:

Import Save As Start's config file stored in the flash.

Import User-Conf:

Import Save As User's config file stored in the flash.

3-21. Security

3-21-1. Mirror

Function name:

Mirror Configuration

Function description:

Mirror Configuration is to monitor the traffic of the network. For example, we assume that Port A and Port B are Monitoring Port and Monitored Port respectively, thus, the traffic received by Port B will be copied to Port A for monitoring.

Mirror

| | | | | | | | | |
|------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Mode | Disable ▾ | | | | | | | |
| Monitoring Port | Port 1 ▾ | | | | | | | |
| Monitored Ingress Port | 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. |
| | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Monitored Egress Port | 1. | 2. | 3. | 4. | 5. | 6. | 7. | 8. |
| | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

Apply

Fig. 3-152

Parameter description:

Mode:

Enable or Disable Port Mirror function. Default is disable.

Monitoring Port:

Set up the port for monitoring. Valid port is Port 1~10 and default is port 1.

Monitored Ingress Port:

Set up the port for being monitored. It only monitor the packets received by the port you set up. Just tick the check box (☑) beside the port x and valid port is Port 1~10.

Monitored Egress Port:

Set up the port for being monitored. It only monitor the packets transmitted by the port you set up. Just tick the check box (☑) beside the port x and valid port is Port 1~10.

3-21-2. Isolated Group

Function name:

Isolated Group

Function description:

Isolated Group function can let the port be independent of other ports in the Isolated group, and the communication is also forbidden between these ports. But, the ports of the Isolated group are still able to communicate with the ports of the non-Isolated group. With this design, it will be helpful to the administrator to immediately find and solve the port that results in the occurrence of looping problems in the network.

Isolated Group

| | | | | | | | | | | |
|----------------|-----------------------------|------------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|-----------------------------|--|--|
| Mode | Disable ▾ | | | | | | | | | |
| Isolated Group | 1. ☐ | 2. ☐ | 3. ☐ | 4. ☐ | 5. ☐ | 6. ☐ | 7. ☐ | 8. ☐ | | |
| | 9. ☐ | 10. ☐ | | | | | | | | |

Fig. 3-153

Parameter description:

Mode:

Enable or Disable Isolated Group function. Default is disable

Isolated Group:

User can choose any port to be the member of this group. Just tick the check box (☑) beside the port x and valid port is Port 1~10. In this group, all of these member ports cannot forward packets with each other. Thus, the switch will not be capable of forwarding any packets in case all ports become the members of the Isolated group.

3-21-3. Arp Protect

Function name:

Arp Protect

Function description:

This function is used to prevent from ARP attack.

Arp Protect Setting

| | |
|--------------------------------------|-------|
| Packet Burst (0 or 1~200 Packets) | 160 |
| Rate per Second(0 or 64~25600 Bytes) | 10240 |

Apply

Note: 0 = No limit.

Fig. 3-154

Parameter description:

Packet Burst:

Available: 1~200 Packets, 0 for No limit

Default: 160

Rate per Second:

Available: 64~25600 Bytes, 0 for No limit

Default: 10240

3-22. Bandwidth

3-22-1. Ingress

Function name:

Ingress Bandwidth Setting

Function description:

Ingress Bandwidth Setting function is used to set up the limit of Ingress bandwidth for each port.

Ingress Bandwidth Control

FE Ports: 64 - 102400 (Kbps)

GE Ports: 1024 - 1024000 (Kbps)

| Port No | Rate(Kb) | Port No | Rate(Kb) |
|---------|----------|---------|----------|
| 1 | 102400 | 2 | 102400 |
| 3 | 102400 | 4 | 102400 |
| 5 | 102400 | 6 | 102400 |
| 7 | 102400 | 8 | 102400 |
| 9 | 1024000 | 10 | 1024000 |

Apply

Fig. 3-155

Parameter description:

Port No.:

Choose the port that you would like this function to work on it. Valid range of the port is 1~10.

Rate:

Set up the limit of Ingress bandwidth for the port you choose. Incoming traffic will be discarded if the rate exceeds the value you set up in Data Rate field. Pause frames are also generated if flow control is enabled. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~8 ranges from 64~102400 with minimum unit of 64 (64,128,192,...) and Port 9~10 ranges from 1024~1024000 with the minimum unit of 1024 (1024,2048,3072,...). Default value of Port 1~8 is 102400 and Port 9~10 is 1024000.

3-22-2. Egress

Function name:

Egress Bandwidth Setting

Function description:

Egress Bandwidth Setting function is used to set up the limit of Egress bandwidth for each port.

Egress Bandwidth Control

FE Ports: 64 - 102400 (Kbps)

GE Ports: 1024 - 1024000 (Kbps)

| Port No | Rate(Kb) | Port No | Rate(Kb) |
|---------|----------|---------|----------|
| 1 | 102400 | 2 | 102400 |
| 3 | 102400 | 4 | 102400 |
| 5 | 102400 | 6 | 102400 |
| 7 | 102400 | 8 | 102400 |
| 9 | 1024000 | 10 | 1024000 |

Apply

Fig. 3-156

Parameter description:

Port No.:

Choose the port that you would like this function to work on it. Valid range of the port is 1~10.

Rate:

Set up the limit of Egress bandwidth for the port you choose. Packet transmission will be delayed if the rate exceeds the value you set up in Data Rate field. Traffic may be lost if egress buffers run full. The format of the packet limits to unicast, broadcast and multicast. Valid value of Port 1~8 ranges from 64~102400 with the minimum unit of 64 (64,128,192,...) and Port 9~10 ranges from 1024~1024000 with the minimum unit of 1024 (1024,2048,3072,...). Default value of Port 1~8 is 102400 and Port 9~10 is 1024000.

3-22-3. Storm

Function name:

Storm Setting

Function description:

Bandwidth Management function is used to set up the limit of Ingress and Egress bandwidth for each port.

Storm Control

FE Ports: 64 - 102400 (Kbps)
GE Ports: 1024 - 1024000 (Kbps)

| Port | Type | Rate |
|------|---|---------|
| 1 | Disable  | 102400 |
| 2 | Disable  | 102400 |
| 3 | Disable  | 102400 |
| 4 | Disable  | 102400 |
| 5 | Disable  | 102400 |
| 6 | Disable  | 102400 |
| 7 | Disable  | 102400 |
| 8 | Disable  | 102400 |
| 9 | Disable  | 1024000 |
| 10 | Disable  | 1024000 |

BC for broadcast storm

UC for unicast storm

BC,UC for both broadcast and unicast storm

MC for multicast storm

BC,MC for both broadcast and multicast storm

UC,MC for both unicast and multicast storm

BC,UC,MC for broadcast, unicast and multicast storm



Fig. 3-157

Parameter description:

Storm Type:

Disable:

Disable the function of the bandwidth storm control.

BC (Broadcast Storm Control):

Enable the function of bandwidth storm control for broadcast packets.

UC (Unknown Unicast Storm Control):

Enable the function of bandwidth storm control for unknown unicast packets. These packets are the MAC address that had not completed the learning process yet.

BC, UC (Broadcast, Unknown Unicast Storm Control):

Enable the function of bandwidth storm control for broadcast and Unknown Unicast Storm packets in transmission

MC (Multicast Storm Control):

Enable the function of bandwidth storm control for multicast packets.

BC, MC (Broadcast, Multicast Storm Control):

Enable the function of bandwidth storm control for broadcast and multicast Storm packets in transmission.

UC, MC (Unknown Unicast, Multicast Storm Control):

Enable the function of bandwidth storm control for Unknown Unicast and multicast Storm packets in transmission.

BC, UC, MC (Broadcast, Unknown Unicast, Multicast Storm Control):

Enable the function of bandwidth storm control for all packets in transmission.

Rate :

Set up the limit of bandwidth for storm type you choose. Valid value of the storm rate ranges:

FE Ports: 64 - 102400 (Kbps)

GE Ports: 1024 - 1024000 (Kbps).

And only integer is acceptable. Default is 102400.

3-23. QoS

The switch supports 802.1p and DSCP priority control, WRR and Stric scheduling method.

3-23-1. Global

Function name:

QoS Global Setting

Function description:

When you want to use QoS function, please enable QoS Mode in advance. Then you can use MAC Priority, 802.1p Priority, IP TOS Priority, DiffServ DSCP Priority, or VIP Port functions and take effect. In this function, you can Enable QoS Mode. Choose any of Priority Control, such as 802.1p, TOS, DSCP. Moreover, you can select Scheduling Method of WRR (Weighted Round Robin) or Strict Priority. Next, you can arrange Weight values for queue 0 to queue 3.

QoS Global Config

| | |
|----------|-----------|
| QoS Mode | Disable ▼ |
|----------|-----------|

| Priority Control | |
|--------------------------|--------------------------|
| 802.1P | DSCP |
| ☐ | ☐ |

| | |
|-------------------|---------|
| Scheduling Method | 4 WRR ▼ |
|-------------------|---------|

| Weight (1-55) | | | |
|---------------|---------|---------|---------|
| Queue 0 | Queue 1 | Queue 2 | Queue 3 |
| 1 | 2 | 4 | 8 |

Apply

Fig. 3-158

Parameter description:

QoS Mode:

You can Enable QoS Mode and let QoS function become effective.
Default is Disable.

Priority Control:

Just tick the check box (☒) of 802.1P or DSCP Qos and click **<Apply>** button to be in operation.

Scheduling Method:

Including <4 WRR>, <1 Strict, 3 WRR>, <2 Strict, 2 WRR> and <4 Strict>. Default is <4 WRR>. After you choose any of Scheduling Method, please click **<Apply>** button to be in operation.

Weight (1~55):

Over here, you can make an arrangement to Weight values of Queue 0 to Queue 3. The range of Weight you can set is 1~55. In default, the weight of Queue 0 is 1, the weight of Queue 1 is 2, the weight of Queue 2 is 4, and the weight of Queue 3 is 8.

3-23-2. 802.1p

Function name:

802.1p Setting

Function description:

This function will affect the priority of VLAN tag. Based on the priority of VLAN tag, it can arrange 0~7 priorities, priorities can map to 4 queues of the switch (queue 0~3) and possess different bandwidth distribution according to your weight setting.

802.1p Priority Mapping

| Priority | Queue |
|----------|-------|
| 0 | 0 ▾ |
| 1 | 0 ▾ |
| 2 | 1 ▾ |
| 3 | 1 ▾ |
| 4 | 2 ▾ |
| 5 | 2 ▾ |
| 6 | 3 ▾ |
| 7 | 3 ▾ |

Apply

Fig. 3-159

Parameter description:

802.1p Priority Mapping:

Each Priority can select any of Queue 0 ~ Queue 3. In Default, Priority 0 is mapping to Queue 0, Priority 1 is mapping to Queue 0, Priority 2 is mapping to Queue 1, Priority 3 is mapping to Queue 1, Priority 4 is mapping to Queue 2, Priority 5 is mapping to Queue 2, Priority 6 is mapping to Queue 3, and Priority 7 is mapping to Queue 3.

3-23-3. DSCP

Function name:

DSCP Setting

Function description:

In the late 1990s, the IETF redefined the meaning of the 8-bit SERVICE TYPE field to accommodate a set of differentiated services (DS). Under the differentiated services interpretation, the first six bits comprise a codepoint, which is sometimes abbreviated DSCP, and the last two bits are left unused.

DSCP can form total 64 (0~63) kinds of Traffic Class based on the arrangement of 6-bit field in DSCP of the IP packet. In the switch, user is allowed to set up these 64 kinds of Class that belong to any of queue 0~3.

DSCP Priority Mapping

| Priority | Queue | Priority | Queue | Priority | Queue | Priority | Queue |
|----------|-------|----------|-------|----------|-------|----------|-------|
| 0 | 0 ▾ | 1 | 0 ▾ | 2 | 0 ▾ | 3 | 0 ▾ |
| 4 | 0 ▾ | 5 | 0 ▾ | 6 | 0 ▾ | 7 | 0 ▾ |
| 8 | 0 ▾ | 9 | 0 ▾ | 10 | 0 ▾ | 11 | 0 ▾ |
| 12 | 0 ▾ | 13 | 0 ▾ | 14 | 0 ▾ | 15 | 0 ▾ |
| 16 | 1 ▾ | 17 | 1 ▾ | 18 | 1 ▾ | 19 | 1 ▾ |
| 20 | 1 ▾ | 21 | 1 ▾ | 22 | 1 ▾ | 23 | 1 ▾ |
| 24 | 1 ▾ | 25 | 1 ▾ | 26 | 1 ▾ | 27 | 1 ▾ |
| 28 | 1 ▾ | 29 | 1 ▾ | 30 | 1 ▾ | 31 | 1 ▾ |
| 32 | 2 ▾ | 33 | 2 ▾ | 34 | 2 ▾ | 35 | 2 ▾ |
| 36 | 2 ▾ | 37 | 2 ▾ | 38 | 2 ▾ | 39 | 2 ▾ |
| 40 | 2 ▾ | 41 | 2 ▾ | 42 | 2 ▾ | 43 | 2 ▾ |
| 44 | 2 ▾ | 45 | 2 ▾ | 46 | 2 ▾ | 47 | 2 ▾ |
| 48 | 3 ▾ | 49 | 3 ▾ | 50 | 3 ▾ | 51 | 3 ▾ |
| 52 | 3 ▾ | 53 | 3 ▾ | 54 | 3 ▾ | 55 | 3 ▾ |
| 56 | 3 ▾ | 57 | 3 ▾ | 58 | 3 ▾ | 59 | 3 ▾ |
| 60 | 3 ▾ | 61 | 3 ▾ | 62 | 3 ▾ | 63 | 3 ▾ |

Apply

Fig. 3-160

Parameter description:

DSCP Priority Mapping:

64 kinds of priority traffic as mentioned above, user can set up any of Queue 0~3. In default, Priority 0~15 are mapping to Queue 0, Priority 16~31 are mapping to Queue 1, Priority 32~47 are mapping to Queue 2, Priority 48~63 are mapping to Queue 3.

3-24. ACL

The Cross-8/SP switch access control list (ACL) is probably the most commonly used object in the IOS. It is used for packet filtering but also for selecting types of traffic to be analyzed, forwarded, or influenced in some way.

The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

Note: The High-ACL List rule: When you set on the switch, it will apply the ACL rules with the top priority. The High-ACL rules will give the top priority against the other access control rules.

The Low-ACL List rule: When you set on the switch, it will apply the ACL rules which are lower than some specific packet filtering rules (e.g. MAC filtering, IP-MAC-Port Binding).

3-24-1. High-ACL List/Low-ACL List

Function name:

High-ACL List / Low-ACL List

Function description:

The switch ACL function support **up to 128 High Access Control List (High-ACL) and 256 Low Access Control List (Low-ACL List)**, using the shared 128 High ACEs and 256 Low ACEs for ingress classification. You can create an ACE and assign this ACE for each port with <Any> or assign this ACE for a policy or assign this ACE for a port. There are 7 priorities, each port can select one of policy, then decides which of the following actions would take according to the packet's IPv4, EtherType, ARP Protocol, MAC Parameters and VLAN parameters:

Current High-ACL List

Priority Up Priority Down

| No | Name | In-Band Counter | Out-Band Counter |
|--------|------|-----------------|------------------|
| (None) | | | |

Add Edit/Show Delete Clear Counter

Fig. 3-161

Parameter description:

Add:

To add new access control rule on switch. You must configure the parameters what described later when you add the new access control rule.

Step: To click **<Add>** button and input relative data, then click **<Apply>**

button.

ACL Configuration

| | |
|---------------------|--|
| ACL Name | Acc |
| Ingress Port Map | 1 ☒ 2 ☒ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐
9 ☐ 10 ☐ All ☐ |
| MAC DA/SA | |
| SMAC Filter | 00 - 00 - 00 - 00 - 00 - 00 |
| DMAC Filter | 00 - 00 - 00 - 00 - 00 - 00 |
| VLAN Tag | |
| Vlan Type | Any |
| Ethernet Type | |
| Frame Type | Any |
| IPv4 | |
| Protocol | Any |
| IPv4 TOS | Any |
| TTL Range | TTL for Any (Don't Care) |
| IPv4 DA | Any |
| IPv4 SA | Any |
| L4 Destination port | Any |
| L4 Source port | Any |

Action

| | |
|-------------------------------|-----------|
| In-Band | |
| Forward Decision | No change |
| Modify Packet-DSCP | Any |
| Out-Band | |
| Forward Decision | No change |
| Modify Packet-DSCP | Any |
| Modify Packet for In/Out-Band | |
| Modify Packet-802.1P | Any |
| Modify Packet-QOS | Any |

Rate Meter

| | |
|-----------|--------------|
| Bandwidth | 1024000 Kbps |
|-----------|--------------|

Apply

Fig. 3-162

ACL name:

To add a new ACL rule name that is composed of any letter (A-Z, a-z) and digit (0-9) with maximal 22 characters.

Ingress Port Map:

To evoke the ingress ports to join ACL rule. Port number is 1-10 or all.

MAC DA/SA:

To click **<MAC DA/SA>** and input the source and destination MAC.

VLAN Tag:

To click **<VLAN Tag>**, select Any or Tag-based VLAN and input Tag VID, Tag Priority if Tag-based VLAN selected.

ACL Configuration

| | |
|------------------|--|
| ACL Name | Acc |
| Ingress Port Map | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐
9 ☐ 10 ☐ All ☐ |
| MAC DA/SA | |
| VLAN Tag | |
| Vlan Type | Any <input type="button" value="v"/> |
| | Any |
| | Tag-based Vlan |
| Internet Type | |
| IPv4 | |

Fig. 3-163

ACL Configuration

| | |
|------------------|--|
| ACL Name | Acc |
| Ingress Port Map | 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐
9 ☐ 10 ☐ All ☐ |
| MAC DA/SA | |
| VLAN Tag | |
| Vlan Type | Tag-based Vlan <input type="button" value="v"/> |
| Tag VID | 1 |
| Tag Priority | 0 <input type="button" value="v"/> |
| Ethernet Type | |
| IPv4 | |

Fig. 3-164

Ethernet Type:

To click **<Ethernet Type>**, select Any, IPv4, ARP or Specific.

ACL Configuration

| | | |
|------------------|--|------|
| ACL Name | Acc | |
| Ingress Port Map | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8
☐ 9 ☐ 10 ☐ All | |
| MAC DA/SA | | |
| VLAN Tag | | |
| Ethernet Type | | |
| Frame Type | Any | IPv4 |
| | Any | |
| | IPv4 | |
| | ARP Specific | |

Fig. 3-165

IPv4:

To set IPv4 packet filter function with ACLs.

To click **<IPv4>** and select Protocol, IPv4 TOS, TTL Range, IPv4 DA, IPv4 SA, L4 Destination port and L4 Source port to select suitable item.

ACL Configuration

| | | |
|---------------------|--|--|
| ACL Name | Acc | |
| Ingress Port Map | ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8
☐ 9 ☐ 10 ☐ All | |
| MAC DA/SA | | |
| VLAN Tag | | |
| Ethernet Type | | |
| IPv4 | | |
| Protocol | Any | |
| IPv4 TOS | Any | |
| TTL Range | TTL for Any (Don't Care) | |
| IPv4 DA | Any | |
| IPv4 SA | Any | |
| L4 Destination port | Any | |
| L4 Source port | Any | |

Fig. 3-166

Protocol: Any, ICMP, UDP, TCP or Other.

IPv4 TOS: Any or Specific. To input TOS Value if Specific is selected.

| IPv4 | |
|---------------------|----------|
| Protocol | Any |
| IPv4 TOS | Specific |
| TOS Value | 0x 00 |
| TTL Range | TTL=0 |
| IPv4 DA | Any |
| IPv4 SA | Any |
| L4 Destination port | Any |
| L4 Source port | Any |

Fig. 3-167

TTL Range: TTL for Any(Don't Care), TTL=1, TTL=1-254 or TTL=255.

| IPv4 | |
|---------------------|--------------------------|
| Protocol | Any |
| IPv4 TOS | Any |
| TTL Range | TTL for Any (Don't Care) |
| IPv4 DA | TTL for Any (Don't Care) |
| IPv4 SA | TTL=1 |
| | TTL=2-254 |
| | TTL=255 |
| L4 Destination port | Any |
| L4 Source port | Any |

Fig. 3-168

IPv4 DA: Any, HOST or Network.

If HOST is selected: Input DA Value

If Network is selected: Input DA Value and DA Mask Value

IPv4 SA: Any, HOST or Network.

If HOST is selected: Input SA Value

If Network is selected: Input SA Value and SA Mask Value

| IPv4 | |
|---------------------|--------------------------|
| Protocol | Any |
| IPv4 TOS | Any |
| TTL Range | TTL for Any (Don't Care) |
| IPv4 DA | Any |
| IPv4 SA | Any |
| | HOST |
| | Network |
| L4 Destination port | Any |
| L4 Source port | Any |

Fig. 3-169

L4 Destination port:

Any or Specific.

If Specific is selected: Input Destination Port Value

L4 Source port:

Any or Specific.

If Specific is selected: Input Source Port Value

| IPv4 | |
|------------------------|-----------|
| Protocol | UDP |
| IPv4 TOS | Any |
| TTL Range | TTL=2-254 |
| IPv4 DA | Any |
| IPv4 SA | Any |
| L4 Destination port | Specific |
| Destination Port Value | 0 |
| L4 Source port | Specific |
| Source Port Value | 0 |

Fig. 3-170

In-Band / Out-Band:

Forward Decision:

To select “No change” , “ Use new forward map” , “ ORed with new map” or “ Explicit actions”.

(a) Use new forward map: When the packet is in-band/out-band then it will forward to new map.

(b) ORed with new map: When the packet is in-band/out-band then it will redirect forward to new map.

To select one item of Forward Map if (a) or (b) is selected.

Action

| In-Band | |
|-------------------------------|---------------------|
| Forward Decision | No change |
| Modify Packet-DSCP | No change |
| | Use new forward map |
| | ORed with new map |
| | Explicit actions |
| Forward Decision | No change |
| Modify Packet-DSCP | Any |
| Modify Packet for In/Out-Band | |
| Modify Packet-802.1P | Any |
| Modify Packet-QOS | Any |

Fig. 3-171

Action

| In-Band | |
|----------------------|-------------------|
| Forward Decision | ORed with new map |
| Forward Map | All Linked-Port |
| Modify Packet-DSCP | All Linked-Port |
| | Port 1 |
| | Port 2 |
| | Port 3 |
| Forward Decision | Port 4 |
| Modify Packet-DSCP | Port 5 |
| | Port 6 |
| | Port 7 |
| | Port 8 |
| | Port 9 |
| | Port 10 |
| Modify Packet-802.1P | |
| Modify Packet-QOS | Any |

Fig. 3-172

(c) Explicit actions: When the packet is in-band/out-band then it will forward with explicit action.

To select one item of Forward Map if (c) is selected.

Action

| In-Band | |
|-------------------------------|------------------------------------|
| Forward Decision | Explicit actions |
| Forward Map | As ARL map |
| Modify Packet-DSCP | As ARL map and copy to mirror port |
| | Drop |
| | Forward to mirror port |
| Forward Decision | No change |
| Modify Packet-DSCP | Any |
| Modify Packet for In/Out-Band | |
| Modify Packet-802.1P | Any |
| Modify Packet-QOS | Any |

Fig. 3-173

Modify Packet-DSCP: To select "Any" or "Specific."

To input DSCP Value if "Specific" is selected.

Action

| In-Band | |
|--------------------|---------------------|
| Forward Decision | Use new forward map |
| Forward Map | All Linked-Port |
| Modify Packet-DSCP | Specific |
| DSCP Value | 0 |

Fig. 3-174

Modify Packet for In/ Out-Band :

Modify Packet-802.1P:

To select "Any" or "Specific". To input 802.1p Value if "Specific" is selected.

Modify Packet-QoS:

To select "Any" or "Specific". To input QoS Value if "Specific" is selected.

| Modify Packet for In/Out-Band | |
|-------------------------------|------------|
| Modify Packet-802.1P | Specific ▼ |
| 802.1P Value | 0 |
| Modify Packet-QoS | Specific ▼ |
| QoS Value | 0 |

Fig. 3-175

Rate Meter:

To set rate meter function with the bandwidth parameter. The range is 64 to 1024000kbps.

Edit/Show:

To modify or monitor the access control configuration rule on switch.

Step 1: To select an existed entry.

Step 2: To click **<Edit/Show>** button and modify relative data, then click **<Apply>** button.

Delete:

To delete an existed access control configuration rule on switch.

Step: To select an existed entry, then click **<Delete>** button.

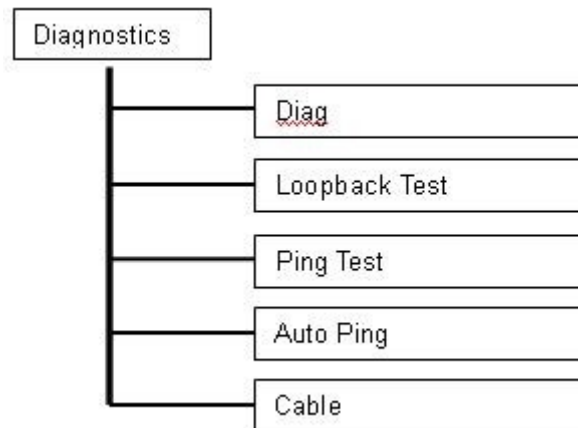
Clear Counter:

To clear in-band and out-band counter.

Step: To select an existed entry, then click **<Clear Counter>** button.

3-25. Diagnostics

Five functions, including Diagnostics, Loopback Test, Ping Test, Auto Ping and Cable are contained in this function folder for device self-diagnostics. Each of them will be described in detail orderly in the following sections.



3-25-1. Diag

Function name:

Diag

Function description:

Diagnostics function provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes EEPROM test, UART test, DRAM test and Flash test.

Diagnostics

| | |
|-------------|----|
| EEPROM Test | OK |
| UART Test | OK |
| DRAM Test | OK |
| Flash Test | OK |

Run

Fig. 3-176

Parameter description:

Run:

Execute function test.

3-25-2. Loopback

Function name:

Loopback Test

Function description:

In the Loopback Test function, there are two different loopback tests. One is Internal Loopback Test and the other is External Loopback Test. The former test function will not send the test signal outside the switch box. The test signal only wraps around in the switch box. As to the latter test function, it will send the test signal to its link partner. If you do not have them connected to active network devices, i.e. the ports are link down, the switch will report the port numbers failed. If they all are ok, it just shows OK.

Note: Whatever you choose Internal Loopback Test or External Loopback Test, these two functions will interfere with the normal system working, and all packets in sending and receiving also will stop temporarily.

Loopback Test

| Port No | Internal Loopback | External Loopback |
|---------|-------------------|-------------------|
| 1 | OK | Fail |
| 2 | OK | Fail |
| 3 | OK | OK |
| 4 | OK | Fail |
| 5 | OK | Fail |
| 6 | OK | Fail |
| 7 | OK | Fail |
| 8 | OK | Fail |
| 9 | OK | OK |
| 10 | OK | Fail |

Run Again

Fig. 3-177

Parameter description:

Run Again:

Execute Loopback Test again.

3-25-3. Ping Test

Function name:

Ping Test

Function description:

Ping Test function is a tool for detecting if the target device is alive or not through ICMP protocol which abounds with report messages. The switch provides Ping Test function to let you know that if the target device is available or not. You can simply fill in a known IP address and then click **<Ping>** button. After a few seconds later, the switch will report you the pinged device is alive or dead in the field of Ping Result.

Ping Test

| | |
|-----------------|-----------------------|
| IP Address | 192.168.2.12 |
| Default Gateway | 192.168.2.254 |
| Ping Result | 192.168.2.12 is alive |

Ping

Input an address to ping, ex. 192.168.1.1

Fig. 3-178

Parameter description:

IP Address:

An IP address with the version of IPv4, e.g. 192.168.1.1.

Default Gateway:

IP address of the default gateway.

For more details, please see the section of IP address in Chapter 2.

Ping Result:

“x.x.x.x is alive or dead” will be shown.

Ping:

To click **<Ping>** button to start “Ping Test”.

3-25-4. Auto Ping

Function name:

Auto Ping

Function description:

Auto Ping function is a tool for detecting if the target device is alive or not through ICMP which abounds with report messages. The switch provides auto Ping Test function to let you know that if the target device is available or not.

Auto Ping

| State | IP address | Interval | Times |
|-----------|------------|----------------|------------|
| Disable ▼ | | 20 (1~300 sec) | 10 (3~100) |

Apply

Fig. 3-179

Parameter description:

State:

To enable or disable Auto Ping function.

IP Address:

An IP address with the version of v4, e.g. 192.168.1.1.

Interval:

Range is 1 ~300 seconds.

Default: 20 seconds

Times:

Range is 3 ~100

Default: 10 times

3-25-5. Cable

Function name:

Cable

Function description:

Cable function is a tool for detecting if the cable per port status is OK or not. report messages.

Cable Diagnostic

Port to diagnose: Port 3 ▼

| | |
|--------|--------------------------------------|
| Status | Ok (2 pairs, deviation in 10 meters) |
| PAIR A | Ok, length 4 meters |
| PAIR B | Ok, length 4 meters |

Run

Fig. 3-180

Parameter description:

Status:

To show the length of tested port cable.

Pair A:

To show the length of Pair A.

Pair B:

To show the length of Pair B.

3-26. TFTP Server

Function name:

TFTP Server

Function description:

Set up IP address of TFTP server.



| TFTP Server | |
|-------------|---------|
| Server | 0.0.0.0 |

Apply

Fig. 3-181

Parameter description:

Specify the IP address where the TFTP server locates. Fill in the IP address of your TFTP server, then press **<Apply>** button to have the setting taken effect.

3-27. SysLog

The Syslog is a standard for [logging program messages](#) . It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as well a generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

Function name:

Syslog

Function description:

The Syslog allows you to configure the syslog server address and enable/disable messages sent to the syslog server from switch port.

Syslog

| | |
|---------------|-----------|
| Syslog | Disable ▾ |
| Syslog Server | 0.0.0.0 |
| Port | 514 |

Apply

Fig. 3-182

Parameter description:

Syslog:

Invoke the “Enable” to enable syslog function .

IP Address:

The IP address of the Syslog Server.

Port:

Filters the log to send syslog message with the selected port of PC host (or Syslog server , ex: 514).

3-28. Log

This function shows the log data. The switch provides system log data for users. There are 22 private trap logs, 5 public trap logs. The switch supports total 120 log entries. For more details on log items, please refer to the section of Alarm and SNMP.

Function name:

Log Data

Function description:

The Trap Log Data is displaying the log items including all SNMP Private Trap events, SNMP Public traps and user logs occurred in the system. In the report table, No., Time and Events are three fields contained in each trap record.

| Log Data | | |
|-------------|--------------------------|----------------------------------|
| TFTP Server | 0.0.0.0 | |
| Auto Upload | Disabled | |
| No | Time | Events |
| 1 | Wed Nov 12 14:05:36 2008 | Login [admin] |
| 2 | Wed Nov 12 14:00:11 2008 | Login [admin] |
| 3 | Wed Nov 12 13:58:54 2008 | Login [admin] |
| 4 | Wed Nov 12 13:33:01 2008 | Login [admin] |
| 5 | Wed Nov 12 13:31:47 2008 | Login [admin] |
| 6 | Wed Nov 12 13:15:18 2008 | LACP Enabled [Port 1 : Group: 1] |
| 7 | Wed Nov 12 12:54:38 2008 | Login [admin] |
| 8 | Wed Nov 12 12:31:50 2008 | Login [admin] |
| 9 | Wed Nov 12 11:34:17 2008 | Dual Media Swapped [Port 9] |
| 10 | Wed Nov 12 11:34:17 2008 | Module Inserted |
| 11 | Wed Nov 12 11:34:16 2008 | Link Up [Port 9] |
| 12 | Wed Nov 12 11:34:13 2008 | Dual Media Swapped [Port 9] |
| 13 | Wed Nov 12 11:34:13 2008 | Module Removed |
| 14 | Wed Nov 12 11:34:12 2008 | Link Down [Port 9] |
| 15 | Wed Nov 12 11:34:11 2008 | Link Up [Port 3] |
| 16 | Wed Nov 12 11:33:52 2008 | Dual Media Swapped [Port 9] |
| 17 | Wed Nov 12 11:33:52 2008 | Module Inserted |
| 18 | Wed Nov 12 11:33:51 2008 | Link Up [Port 9] |
| 19 | Wed Nov 12 11:33:31 2008 | Dual Media Swapped [Port 10] |
| 20 | Wed Nov 12 11:33:31 2008 | Module Removed |

Auto Upload Enable

Upload Log

Clear Log

Fig. 3-183

Parameter description:

TFTP Server:

Display the TFTP Server. "0.0.0.0" will be shown if no TFTP server.

Auto Upload:

Display the current status of Auto Upload(Enabled or Disabled).

No.:

Display the order number that the trap happened.

Time:

Display the time that the trap happened.

Events:

Display the trap event name.

Auto Upload Enable/Disable:

Enable or Disable Auto Upload function.

Upload Log:

Upload log data through TFTP.

Clear Log:

Clear log data.

3-29. Firmware Upgrade

Software upgrade tool is used to help upgrade the software function in order to fix or improve the function. The switch provides a TFTP client for software upgrade. This can be done through Ethernet.

Function name:

Firmware Upgrade

Function description:

The switch supports TFTP upgrade tool for upgrading software. If you assure to upgrade software to a newer version one, you must follow two procedures:

- 1.) Specifying the IP address where TFTP server locates. In this field, the IP address of your TFTP server should be filled in(According to **3-25 TFTP Server**).
- 2.) Specifying what the filename and where the file is. You must specify full path and filename.

Then, press **<Upgrade>** button if your download is not successful, the switch will also be back to “Software Upgrade”, and it will not upgrade the software as well.

When download is completed, the switch starts upgrading software. A reboot message will be prompted after completing upgrading software. At this time, you must reboot the switch to have new software worked.

Note: Software upgrade is hazardous if power is off. You must do it carefully.

Firmware Upgrade

| | |
|-------------------|---------|
| TFTP Server | 0.0.0.0 |
| Path and Filename | |

Upgrade

Fig. 3-184

Parameter description:

TFTP Server: A TFTP server stored the image file you want to upgrade.

Path and Filename: File path and filename stored the image file you want to upgrade.

3-30. Reboot

We offer you many ways to reboot the switch, including power up, hardware reset and software reset. You can press the RESET button in the front panel to reset the switch. After upgrading software, changing IP configuration or changing VLAN mode configuration, then you must reboot to have the new configuration taken effect. Here we are discussing is software reset for the “reboot” in the main menu.

Function name:

Reboot

Function description:

Reboot the switch. Reboot takes the same effect as the RESET button on the front panel of the switch. It will take around thirty (30) seconds to complete the system boot.

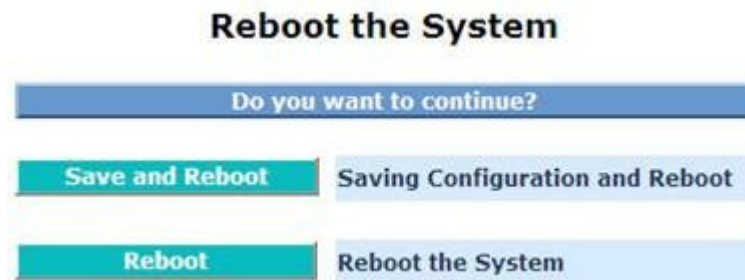


Fig. 3-185

Parameter description:

Save and Reboot:

Save the current settings as start configuration before rebooting the switch.

Reboot:

Reboot the system directly.

3-31. Logout

You can manually logout by performing Logout function. In the switch, it provides another way to logout. You can configure it to logout automatically.

Function name:

Logout

Function description:

The switch allows you to logout the system to prevent other users from the system without the permission. If you do not logout and exit the browser, the switch will automatically have you logout. Besides this manually logout and implicit logout, you can pull down the **<Auto Logout>** list at the left-top corner to explicitly ON/OFF this logout function.



Fig. 3-186

Parameter description:

Auto Logout:

Default is ON. If it is "ON", and no action and no key is stroke as well in any function screen more than 3 minutes, the switch will have you logout automatically.

4.Operation of CLI Management

4-1. CLI Management

Refer to Chapter 2 for basic installation. The following description is the brief of the network connection.

- Locate the correct serial cable which comes with the management switch.
- Attach the RJ-45 connector to serial port on the management device.
- Attach the other end(DB-9 female connector) of serial cable to an ASCII terminal emulator or PC COM port. For example, PC runs Microsoft Windows HyperTerminal utility.
- At "COM Port Properties" Menu, configure the parameters as below:

| | |
|---------------------|--------------|
| Baud rate | 57600 |
| Stop bits | 1 |
| Data bits | 8 |
| Parity | N |
| Flow control | none |

Login .4-1-1

The command-line interface (CLI) is a text-based interface. User can access the CLI through either a direct serial connection to the device or a Telnet session. The default accounts and authorization of the managed switch are listed as Table 4-1:

| Account | Password (Default) | Password Change | Create , Modify & Delete Account | Set | Read |
|----------|--------------------|------------------------|----------------------------------|-----|------|
| admin | admin | Yes | Yes | Yes | Yes |
| operator | operator | Yes
(Only operator) | No | Yes | Yes |
| guest | guest | Yes
(Only guest) | No | No | Yes |

Table 4-1

After you login successfully, the prompt will be shown as Fig. 4-1.

```
Managed Switch - IFEL2P-SW8C01# Managed Switch - IFEL2P-SW8C01#
Login: admin Login: operator
Password: Password:
IFEL2P-SW8C01# IFEL2P-SW8C01#
Managed Switch - IFEL2P-SW8C01#
Login: guest
Password:
IFEL2P-SW8C01$
```

Fig. 4-1

Commands of CLI .4-2

Input “?” or “help” after the prompt, then all commands will be listed in the screen. All commands can be divided into two categories, including global commands and local commands. Global commands can be used wherever the mode you are. They are “exit”, “end”, “help”, “history”, “logout”, “save start”, “save user”, “restore default” and “restore user”. For more details, please refer to Section 4-2-1.

Command instructions reside in the corresponding modes are local commands. The same command with the same command name may occur but perform totally different function in different modes. For example, “show” in IP mode performs displaying the IP information; however, it performs displaying the system information in system mode. For more details, please refer to Section 4-2-2.

Managed Switch – Cross-8/SP

Login : Admin

Password : 1234

Cross-8/SP#?

| | |
|----------------|------------------------------------|
| 802.1X | Enter into 802.1X mode |
| account | Enter into account mode |
| acl | Enter into acl mode |
| alarm | Enter into alarm mode |
| autologout | Change autologout time |
| bandwidth | Enter into bandwidth mode |
| config-file | Enter into config file mode |
| dhcp-boot | Enter into DHCP-boot mode |
| dhcp-snooping | Enter into DHCP snooping mode |
| dhcprelay | Enter into DHCP relay mode |
| diag | Enter into diag mode |
| firmware | Enter into firmware mode |
| gvrp | Enter into gvrp mode |
| hostname | Change hostname |
| ip | Enter into ip mode |
| ip-mac-bind | Enter into IP-MAC binding mode |
| lldp | Enter into LLDP mode |
| log | Enter into log mode |
| loop-detection | Enter into Loop-Detection(LD) mode |
| mac-table | Enter into mac table mode |
| management | Enter into management mode |
| mstp | Enter into mstp mode |
| multicast | Enter into multicast mode |

| | |
|---------------------------------|--|
| port | Enter into port mode |
| qos | Enter into qos mode |
| r-ring | Enter into ring mode |
| reboot | Reboot the system |
| security | Enter into security mode |
| snmp | Enter into snmp mode |
| stp | Enter into stp mode |
| syslog | Enter into syslog mode |
| system | Enter into system mode |
| tftp | Enter into tftp mode |
| time | Enter into time mode |
| trunk | Enter into trunk mode |
| vlan | Enter into vlan mode |
| vs | Enter into virtual stack mode |
| -----<< Global commands >>----- | |
| end | Back to the top mode |
| exit | Back to the previous mode |
| help | Show available commands |
| history | Show a list of previously run commands |
| logout | Logout the system |
| restore default | Restore default config |
| restore user | Restore user config |
| save start | Save as start config |
| save user | Save as user config |
| Cross-8/SP# | |

Fig. 4-2

Global Commands of CLI .4-2-1

end

Syntax:

end

Description:

Back to the top mode.

When you enter this command, your current position would move to the top mode. If you use this command in the top mode, you are still in the position of the top mode.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01# alarm
IFEL2P-SW8C01(alarm)# events
IFEL2P-SW8C01(alarm-events)# end
IFEL2P-SW8C01#
```

exit

Syntax:

exit

Description:

Back to the previous mode.

When you enter this command, your current position would move back to the previous mode. If you use this command in the top mode, you are still in the position of the top mode.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01# alarm
IFEL2P-SW8C01(alarm)# events
IFEL2P-SW8C01(alarm-events)#exit
IFEL2P-SW8C01(alarm)#
```

help

Syntax:

help

Description:

To show available commands.

Some commands are the combination of more than two words. When you enter this command, the CLI would show the complete commands. Besides, the command would help you classify the commands between the local commands and the global ones.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01# ip
```

```
IFEL2P-SW8C01(ip)# help
```

```
-----<< Local commands >>-----
```

| | |
|--------------|---|
| disable dhcp | Disable DHCP |
| enable dhcp | Enable DHCP, and set dns auto or manual |
| set dns | Set dns |
| set ip | Set ip and gateway |
| show | Show IP Configuration |

```
-----<< Global commands >>-----
```

| | |
|-----------------|--|
| end | Back to the top mode |
| exit | Back to the previous mode |
| help | Show available commands |
| history | Show a list of previously run commands |
| logout | Logout the system |
| restore default | Restore default config |
| restore user | Restore user config |
| save start | Save as start config |
| save user | Save as user config |

```
IFEL2P-SW8C01(ip)#
```

history

Syntax:

history [#]

Description:

To show a list of previous commands that you had ever run. When you enter this command, the CLI would show a list of commands which you had typed before. The CLI supports up to 256 records. If no argument is typed, the CLI would list total records up to 256. If optional argument is given, the CLI would only show the last numbers of records, given by the argument.

Argument:

[#]: show last number of history records. (optional)

Possible value:

[#]: 1, 2, 3,, 256

Example:

```
IFEL2P-SW8C01(ip)# history
```

```
Command history:
```

```
0. ?
```

```
1. trunk
```

```
2. exit
```

```
3. IFEL2P-SW8C01# trunk
```

```
4. IFEL2P-SW8C01(trunk)# exit
```

```
5. IFEL2P-SW8C01#
```

```
6. trunk
```

```
7. exit
```

```
8. alarm
```

```
9. events
```

```
10. end
```

```
11. ip
```

```
12. help
```

```
13. history
```

```
IFEL2P-SW8C01(ip)# history 3
```

```
Command history:
```

```
12. help
```

```
13. history
```

```
14. history 3
```

```
IFEL2P-SW8C01(ip)#
```

logout

Syntax:

logout

Description:

When you enter this command via Telnet connection, you would logout the system and disconnect. If you connect the system through direct serial port with RS-232 cable, you would logout the system and be back to the initial login prompt when you run this command.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01# logout
Managed Switch – IFEL2P-SW8C01
```

Login:

restore default

Syntax:

restore default

Description:

When you use this function in CLI, the system will show you the information “Do you want to restore the default IP address?(y/n)”. If you choose Y or y, the IP address will restore to default “192.168.1.1”. If you choose N or n, the IP address will keep the same one that you had saved before.

If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; otherwise, it would be back to the CLI system. After restoring default configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would reset to factory default.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01# restore default
Do you want to restore the default ip address?(y/n)
Restoring ...
Restore default configuration successfully.
Do you want to reboot the system?(y/n)
```

restore user

Syntax:

restore user

Description:

To restore the startup configuration as user defined configuration. If restoring default successfully, the CLI would prompt if reboot immediately or not. If you press Y or y, the system would reboot immediately; others would back to the CLI system. After restoring user-defined configuration, all the changes in the startup configuration would be lost. After rebooting, the entire startup configuration would replace as user defined one.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01# restore user
Restoring ...
Restore user configuration successfully.
Do you want to reboot the system?(y/n)
```

save start

Syntax:

save start

Description:

To save the current configuration as the start one. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH. If you want the configuration still works after rebooting, save the configuration using the command 'save stat'.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01# save start
Saving start...
Save Successfully
```

```
IFEL2P-SW8C01#
```

save user

Syntax:

save user

Description:

To save the current configuration as the user-defined configuration. When you enter this command, the CLI would save your current configuration into the non-volatile FLASH as user-defined configuration.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01# save user
```

```
Saving user...
```

```
Save Successfully
```

```
IFEL2P-SW8C01#
```

Local Commands of CLI .4-2-2

■ 802.1x

set acct-server

Syntax:

```
set acct-server <accounting service> <ip> <port-number> <secret key> <ip2>
<port-number>
```

Description:

To set 802.1x accounting state.

Argument:

<accounting service>: 0: Disable 1: Enable

```
<ip><ip2> : IPv4, xxx.xxx.xxx.xxx
```

<port-number> : 1-65535

<secret key> :

Possible value:

<accounting service>: 0: Disable 1: Enable

```
<ip><ip2> : IPv4, xxx.xxx.xxx.xxx
```

<port-number> : 1-65535

<secret key> : Length from 1 to 31 characters

Example:

```
IFEL2P-SW8C01(802.1x)#set acct-server 192.168.1.248 1360 Topsecret
192.168.1.249 1361
```

```
IFEL2P-SW8C01(802.1x)#show state
```

```

# RADIUS_SERVER_IP=$(cat /dev/urandom | fold -w 15 | tr -dc '0-9.' | fold -w 1 | tr -d '\n' | fold -w 15 | paste | sed 's/.$//')
Radius Server 1 : 192.168.1.1

```

Port Number : 1812

Radius Server 2 : 192.168.1.1

Port Number : 1812

Secret Key : Enable

Accounting Service: Enable

Accounting Server 1: 192.168.1.248

Accounting Port : 1360

Accounting Server 2: 192.168.1.249

Accounting Port : 1361

Secret Key : Topsecret

set max-request

Syntax:

```
set max-request <port-range> <times>
```

Description:

The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.

Argument:

<port range>: syntax 1,5-7, available from 1 to 10

<times>: max. times, range 1-10

Possible value:

<port range> : 1 to 10

<times> : 1-10, default is 2

Example:

```
IFEL2P-SW8C01(802.1x)# set max-request 2 2
```

Publication date: May., 2011

ccxxviii

Revision B1

set mode

Syntax:

set mode <port-range> <mode>

Description:

To set up the 802.1X authentication mode of each port.

Argument:

<port range> : syntax 1,5-7, available from 1 to 10

<mode> : set up 802.1x mode

Possible value:

<port range> : 1 to 10

<mode>: 0: Disable

1: Normal

2: Advanced 802.1x

Example:

IFEL2P-SW8C01(802.1x)# set mode 2 1

set port-control

Syntax:

set port-control <port-range> <authorized>

Description:

To set up 802.1X status of each port.

Argument:

<port range> : syntax 1,5-7, available from 1 to 10

<authorized> : set up the status of each port

0:ForceUnauthorized

1:ForceAuthorized

2:Auto

Possible value:

<port range> : 1 to 10

<authorized> : 0,1 or 2

Example:

IFEL2P-SW8C01(802.1x)# set port-control 2 2

set quiet-period

Syntax:

set quiet-period <port-range> <sec>

Description:

A timer used by the Authenticator state machine to define periods of time during when it will not attempt to acquire a Supplicant.

Argument:

<port range> : syntax 1,5-7, available from 1 to 10

<sec> : timer, range 0-65535

Possible value:

<port range> : 1 to 10

<sec> : 0-65535, default is 60

Example:

IFEL2P-SW8C01(802.1x)# set quiet-period 2 30

set reAuthEnabled

Syntax:

set reAuthEnabled <port-range> <ebl>

Description:

A constant that define whether regular reauthentication will take place on this port.

Argument:

<port range> : syntax 1,5-7, available from 1 to 10

<ebl> :

0:"OFF" to disable reauthentication

1:"ON" to enable reauthentication

Possible value:

<port range> : 1 to 10

<ebl> : 0 or 1, default is 1

Example:

IFEL2P-SW8C01(802.1x)# set reAuthEnabled 2 1

set reAuthMax

Syntax:

set reAuthMax <port-range> <max>

Description:

The number of reauthentication attempts that are permitted before the port becomes Unauthorized.

Argument:

<port range> : syntax 1,5-7, available from 1 to 10

<max> : max. value , range 1-10

Possible value:

<port range> : 1 to 10

<max> : 1-10, default is 2

Example:

IFEL2P-SW8C01(802.1x)# set reAuthMax 2 2

set reAuthPeriod

Syntax:

set reAuthPeriod <port-range> <sec>

Description:

A constant that defines a nonzero number of seconds between periodic reauthentication of the supplicant.

Argument:

<port range> : syntax 1,5-7, available from 1 to 10

<sec> : timer, range 1-65535

Possible value:

<port range> : 1 to 10

<sec> : 1-65535, default is 120

Example:

IFEL2P-SW8C01(802.1x)# set reAuthPeriod 2 3600

set server

Syntax:

set server <ip> <port-number> <secret key> <ip2> <port-number>

Description:

To configure the settings related with 802.1X Radius Server.

Argument:

<ip><ip2> : the IP address of Radius Server, and the IP format is xxx.xxx.xxx.xxx

<port-number> : the service port of Radius Server(Authorization port),
range 1~65535

<secret-key> : set up the value of secret-key, and the length of secret-key is
from 1 to 31

Possible value:

<port-number> : 1~65535, default 1812

Example:

```
IFEL2P-SW8C01(802.1x)# set server 192.168.1.115 1812 WinRadius  
192.168.1.116 1812
```

set serverTimeout

Syntax:

set serverTimeout <port-range> <sec>

Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Argument:

<port range> : syntax 1,5-7, available from 1 to 10

<sec> : timer, range 1-255

Possible value:

<port range> : 1 to 10

<sec> : 1-255

Example:

```
IFEL2P-SW8C01(802.1x)# set serverTimeout 2 30
```

set suppTimeout

Syntax:

set suppTimeout <port-range> <sec>

Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Argument:

<port range> : syntax 1,5-7, available from 1 to 10

<sec> : timer, range 1-255

Possible value:

<port range> : 1 to 10

<sec> : 1-255

Example:

IFEL2P-SW8C01(802.1x)# set suppTimeout 2 30

set txPeriod

Syntax:

set txPeriod <port-range> <sec>

Description:

A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted.

Argument:

<port range> : syntax 1,5-7, available from 1 to 10

<sec> : timer, range 1-65535

Possible value:

<port range> : 1 to 10

<sec> : 1-65535

Example:

IFEL2P-SW8C01(802.1x)# set txPeriod 2 30

show mode

Syntax:

show mode

Description:

To display the mode of each port.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(802.1x)# show mode

```
Port    Mode
=====
1       Disable
2       Normal
3       Disable
4       Disable
5       Disable
6       Disable
      :
```

show parameter

Syntax:

show parameter

Description:

To display the parameter settings of each port.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(802.1x)# show parameter

```
port 1) port control : Auto
      reAuthMax      : 2
      txPeriod       : 30
      Quiet Period   : 60
      reAuthEnabled  : ON
      reAuthPeriod   : 120
      max. Request   : 2
      suppTimeout    : 30
      serverTimeout  : 30
      :
      :
      :
```

show security

Syntax:

show security

Description:

To display the authentication status of each port.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(802.1x)# show security

```
Port   Mode   Status
=====
1      Disable
2      Normal  Unauthorized
3      Disable
4      Disable
5      Disable
6      Disable
      :
      :
```

:

show state

Syntax:

show state

Description:

To display the Radius server configuration.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(802.1x)# show state

Radius Server 1: 192.168.1.1

Port Number : 1812

Radius Server 2: 192.168.1.1

Port Number : 1812

Secret Key : Radius

Accounting Service : Enable

Accounting Server 1 : 192.168.1.1

Accounting Port : 1813

Accounting Server 2 : 192.168.1.1

Accounting Port : 1813

Secret Key : Radius

■ account

add guest

Syntax:

add guest <name>

Description:

To create a new guest user. When you create a new guest user, you must type in password and confirm password.

Argument:

<name> : new account name

Possible value:

<name> : a string must be at least 5 characters and smaller than 48 characters

"0~9", "a~z", "A~Z", "=", "-", "~", "!", "@", "\$", "^", "*", "(", ")", "{", "}",
"[", "]", "/", "<", ">", "?", ".", ",", and "|"

Example:

IFEL2P-SW8C01(account)# add guest aaaaa

Password:

Confirm Password:

IFEL2P-SW8C01(account)#

add operator

Syntax:

add operator <name>

Description:

To create a new operator user. When you create a new guest user, you must type in password and confirm password.

Argument:

<name> : new account name

Possible value:

<name> : a string must be at least 5 characters and smaller than 48 characters

"0~9", "a~z", "A~Z", "=", "-", "~", "!", "@", "\$", "^", "*", "(", ")", "{", "}",
"[", "]", "/", "<", ">", "?", ".", ",", and "|"

Example:

IFEL2P-SW8C01(account)# add operator aaaaa

Password:

Confirm Password:

IFEL2P-SW8C01(account)#

del

Syntax:

del <name>

Description:

To delete an existing account.

Argument:

<name> : existing user account

Possible value:

<name> : existing user account

Example:

IFEL2P-SW8C01(account)# del aaaaa

Account aaaaa deleted

modify account

Syntax:

modify account <name> <target_name>

Description:

To change the username of an existing account.

Argument:

<name> : existing user account

<target_name> : replacing user account

Possible value:

<name>: the length is from 5 to 47 characters.

<target_name>: the length is from 5 to 47 characters.

Example:

IFEL2P-SW8C01(account)# modify account aaaaa bbbbbb

IFEL2P-SW8C01(account)#

modify password

Syntax:

modify password <type> [username]

Description:

To change the password of an existing account.

Argument:

<type> : 0 for modify other account, 1 for itself

[username] : user account whose password to be changed

Possible value:

<type> : 0 for modify other account, 1 for itself

[username] : the length is from 5 to 47 characters.

Example:

IFEL2P-SW8C01(account)#modify password 0 aaaaa

Modify password for user : aaaaa

New password :

Confirm password :

Password changed successfully

show

Syntax:

show

Description:

To show user account, including “No.” “Account Name” and “Authorization”.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(account)# show

| No. | Account Name | Authorization |
|-----|--------------|---------------|
| 1 | admin | Administrator |
| 2 | operator | Operator |
| 3 | guest | Guest |

■ acl

high-list

Syntax:

high-list

Description:

To enter into acl high-list mode.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(acl)# high-list

IFEL2P-SW8C01(acl-high-list)#

low-list

Syntax:

low-list

Description:

To enter into acl low-list mode.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(acl)# low-list

IFEL2P-SW8C01(acl-low-list)#

clear-counter

Syntax:

clear-counter <name>

Description:

To clear the acl counter

Argument:

<name> : acl entry name

Possible value:

<name> : acl entry name

Example:

IFEL2P-SW8C01(acl-high-list)#clear-counter entry1

del

Syntax:

del <name>

Description:

To delete an acl entry

Argument:

<name>

Possible value:

<name> : acl entry name

Example:

IFEL2P-SW8C01(acl-high-list)#del entry1

set act-8021p

Syntax:

Set act-8021p <name> <ebl> <1p>

Description:

To set acl action for 802.1p field modification

Argument:

<name> : acl entry name

<ebl> : change 802.1p field

<1p> : new 802.1p field value

Possible value:

<name> : acl entry name

<ebl> : 0: don't care 802.1p field value

1: change 802.1p field value

<1p> : new 802.1p field value, from 0 to 7

Example:

IFEL2P-SW8C01(acl-high-list)# set act-8021p entry1 1 2

set act-in-dscp

Syntax:

set act-in-dscp <name> <ebl> <dscp>

Description:

To set acl action for in-band DSCP field modification

Argument:

<name>: acl entry name

<ebl> : 0: don't care DSCP field value

1: change DSCP field value

<dscp> : new DSCP field value from 0 to 63

Possible value:

<name>: acl entry name

<ebl> : 0: don't care DSCP field value

1: change DSCP field value

<dscp> : new DSCP field value from 0 to 63

Example:

IFEL2P-SW8C01(acl-high-list)#set act-in-dscp entry1 1 6

set act-in-forward

Syntax:

set act-in-forward <name> <decision> <fwd_map>

Description:

To set acl action for in-band forward decision

Argument:

<name>: acl entry name

<decision> : forward decision for in-band

<fwd_map> : New forward map, its meaning vary on <decision>

Possible value:

<name>: acl entry name

<decision> :

0: based on ARL forward map with no change

1: use <fwd_map> as final forward map

2: ARL forward map is ORed with <fwd_map> to get the final forward map
 3: Explicit actions, which defines with <fwd_map>
 <fwd_map> :
 when <decision> is 0, fwd_map is 0 for no change
 when <decision> is 1, fwd_map is defined as port, value: 1 to port 10, and 0 as
 flood to all linked-up ports
 when <decision> is 2, fwd_map is defined as port, value: 1 to port 10, and 0 as
 flood to all linked-up ports
 when <decision> is 3, fwd_map is defined as the following:
 0: As ARL forward map
 1: As ARL map a

Example:

IFEL2P-SW8C01(acl-high-list)#set act-in forward entry1 0 0

set act-out-dscp

Syntax:

set act-out-dscp <name> <ebl> <dscp>

Description:

To set acl action for out-band DSCP field modification

Argument:

<name>: acl entry name

<ebl> : change DSCP field

<dscp> : new DSCP field value, from 0 to 63

Possible value:

<name>: acl entry name

<ebl> :

0: don't care DSCP field value

1: change DSCP field value

<dscp> : new DSCP field value, from 0 to 63

Example:

IFEL2P-SW8C01(acl-high-list)# set act-out-dscp entry1 0 6

set act-out-forward

Syntax:

set act-out-forward <name> <decision> <fwd_map>

Description:

To set acl action for out-band forward decision

Argument:

<name>: acl entry name

<decision> : forward decision for out-band

<fwd_map> : new forward map, its meaning vary on <decision>

Possible value:

<name>: acl entry name

<decision> :

0: based on ARL forward map with no change

1: use <fwd_map> as final forward map

2: ARL forward map is ORed with <fwd_map> to get the final forward map

3: explicit actions, which defines with <fwd_map>

<fwd_map> : new DSCP field value, from 0 to 63

when <decision> is 0, fwd_map is 0 for no change

when <decision> is 1, fwd_map is defined as port, value:

1 to port 10, and 0 as flood to all linked-up ports

when <decision> is 2, fwd_map is defined as port, value:
1 to port 10, and 0 as flood to all linked-up ports
when <decision> is 3, fwd_map is defined as the following:
0: as ARL forward map
1: as ARL map and copy to mirror port
2: drop
3: forward to mirror port

Example:

```
IFEL2P-SW8C01(acl-high-list)#set act-out-forward entry1 0 0
```

set act-qos

Syntax:

```
set act-qos <name> <ebl> <qos>
```

Description:

To set acl action for qos

Argument:

<name> : acl entry name

<ebl> : change priority

<qos> : new priority, from 0 to 3

Possible value:

<name> : acl entry name

<ebl> : change priority

0: don't care qos field value

1: change packet priority

<qos> : new priority, from 0 to 3

Example:

```
IFEL2P-SW8C01(acl-high-list)#set act-qos entry1 0 0
```

set ether-type

Syntax:

```
set ether-type <name> <ether>
```

Description:

To set acl ethernet type

Argument:

<name> : acl entry name

<ether> : ethernet type

Possible value:

<name> : acl entry name

<ether> : ethernet type, format: 0806 (in hexadecimal format)

IPv4 for 0800, ARP for 0806

set ingress-port

Syntax:

```
set ingress-port <name> <range>
```

Description:

To set acl ingress port map

Argument:

<name> : acl entry name

<range> : syntax: 1,5-7, available from 1 to 10

Possible value:

<name> : acl entry name

<range> : syntax: 1,5-7, available from 1 to 10

set ip-da**Syntax:**

set ip-da <name> <ip> <mask>

Description:

To set acl ipv4 destination address

Argument:

<name> : acl entry name

<ip> : ip destination address

<mask> : ip address mask

Possible value:

<name> : acl entry name

<ip> : ip destination address

<mask> : ip address mask

set ip-l4-destination-port**Syntax:**

set ip-l4-destination-port <name> <port>

Description:

To set acl IPv4 L4 destination port

Argument:

<name> : acl entry name

<port> : IPv4 L4 destination port, from 0 to 65535

Possible value:

<name> : acl entry name

<port> : IPv4 L4 destination port, from 0 to 65535

set ip-l4-source-port**Syntax:**

set ip-l4-source-port <name> <port>

Description:

To set acl IPv4 L4 source port

Argument:

<name> : acl entry name

<port> : IPv4 L4 source port, from 0 to 65535

Possible value:

<name> : acl entry name

<port> : IPv4 L4 source port, from 0 to 65535

set ip-protocol**Syntax:**

set ip-protocol <name> <proto>

Description:

To set acl ipv4 protocol

Argument:

<name> : acl entry name

<proto> : IPv4 protocol, from 0 to 255

Possible value:

<name> : acl entry name

<proto> : IPv4 protocol, from 0 to 255

ICMP for 1, UDP for 17, TCP for 6

set ip-sa

Syntax:

set ip-sa <name> <ip> <mask>

Description:

To set acl ipv4 source address

Argument:

<name> : acl entry name

<ip> : ip source address

<mask> : ip address mask

Possible value:

<name> : acl entry name

<ip> : ip source address

<mask> : ip address mask

set ip-tos

Syntax:

set ip-tos <name> <tos>

Description:

To set acl ipv4 TOS

Argument:

<name> : acl entry name

<ip> : IPv4 TOS field, from 00 to ff (in hexadecimal format)

Possible value:

<name> : acl entry name

<ip> : IPv4 TOS field, from 00 to ff (in hexadecimal format)

set ip-ttl

Syntax:

set ip-ttl <name> <ttl>

Description:

To set acl ipv4 TTL Range

Argument:

<name> : acl entry name

<ttl> : IPv4 TTL range

Possible value:

<name> : acl entry name

<ttl> :

0: TTL for Any (Don't care)

1: TTL = 1

2: TTL = 2-254

3: TTL = 255IPv4 TOS field, from 00 to ff (in hexadecimal format)

set mac-da

Syntax:

set mac-da <name> <mac>

Description:

To set acl MAC destination address

Argument:

<name> : acl entry name

<mac> : mac address, format: 01-02-03-04-05-06

Possible value:

<name> : acl entry name

<mac> : mac address, format: 01-02-03-04-05-06

set mac-sa**Syntax:**

set mac-sa <name> <mac>

Description:

To set acl MAC source address

Argument:

<name> : acl entry name

<mac> : mac address, format: 01-02-03-04-05-06

Possible value:

<name> : acl entry name

<mac> : mac address, format: 01-02-03-04-05-06

set meter**Syntax:**

set meter <name> <rate>

Description:

To set acl rate meter

Argument:

<name> : acl entry name

<rate> : bandwidth for this acl entry, from 64Kbps to 1024000Kbps

Possible value:

<name> : acl entry name

<rate> : bandwidth for this acl entry, from 64Kbps to 1024000Kbps

set vlan**Syntax:**

set vlan <name> <ebl> <vid> <prio>

Description:

To set acl VLAN

Argument:

<name> : acl entry name

<ebl> : change VLAN field

<vid> : VLAN ID

<prio> : priority

Possible value:

<name> : acl entry name

<ebl> : change VLAN field

0: don't care VLAN value

1: apply VLAN value

<vid> : VLAN ID, from 1 to 4094, 0 for priority tag

<prio> : priority, from 0 to 7

show detail

Syntax:

show detail <name>

Description:

To show detail acl entry information

Argument:

<name> : acl entry name

Possible value:

<name> : acl entry name

show simple

Syntax:

show simple <name>

Description:

To show simple acl entry list

Argument:

<name> : acl entry name

Possible value:

<name> : acl entry name

swap

Syntax:

swap <entry_name_1> <entry_name_2>

Description:

Swap the priority of these two acl entries

Argument:

<entry_name_1> : acl entry name

<entry_name_2> : acl entry name

Possible value:

<entry_name_1> : acl entry name

<entry_name_2> : acl entry name

■ alarm

<<email>>

del mail-address

Syntax:

del mail-address <#>

Description:

To remove the e-mail address.

Argument:

<#>: email address number, range: 1 to 6

Possible value:

<#>: 1 to 6

Example:

IFEL2P-SW8C01(alarm-email)# del mail-address 2

del return-path

Syntax:

del return-path

Description:

To delete the return path.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(alarm-email)# del return-path

del sender

Syntax:

del sender

Description:

To delete the e-mail sender.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(alarm-email)# del sender

del server-user

Syntax:

del server-user

Description:

To delete the server, user account and password.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(alarm-email)# del server-user

set mail-address

Syntax:

set mail-address <#> <mail address>

Description:

To set the email address.

Argument:

<#> : email address number, range: 1 to 6

<mail address> : email address

Possible value:

<#>: 1 to 6

Example:

IFEL2P-SW8C01(alarm-email)# set mail-address 1 abc@mail.abc.com

set return-path

Syntax:

set return-path <path>

Description:

To set the email return path.

Argument:

<path> : email address

Possible value:

<path> :

set sender

Syntax:

set sender <sender name>

Description:

To set the email sender.

Argument:

<sender name> :

Possible value:

<sender name> :

Example:

IFEL2P-SW8C01(alarm-email)# set sender GoodGuy

IFEL2P-SW8C01(alarm-email)# show

Mail Server :

Username :

Password : *****

Sender : GoodGuy

Return-Path :

Email Address 1: abc@yahoo.com.tw

Email Address 2:

Email Address 3:

Email Address 4:

Email Address 5:

Email Address 6:

set server

Syntax:

set server <ip>

Description:

To set the IP address of the email server.

Argument:

<ip>:email server ip address or domain name

Possible value:

<ip>:IPv4

Example:

IFEL2P-SW8C01(alarm-email)# set server 192.168.1.6

set user

Syntax:

set user <username>

Description:

To set the account of the email server.

Argument:

<username>: email server account

Possible value:

<username>: email server account

Example:

IFEL2P-SW8C01(alarm-email)# set user admin

show

Syntax:

show

Description:

To show the e-mail configuration.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(alarm-email)# show

Mail Server : 192.168.1.6

Username : admin

Password : *****

Email Address 1: abc@mail.abc.com

Email Address 2:

Email Address 3:

Email Address 4:

Email Address 5:

Email Address 6:

<<events>>

del all

Syntax:

del all <range>

Description:

To delete selected trap event.

Argument:

<range>:syntax 1,5-7

Possible value:

<range>: 1~27

Example:

IFEL2P-SW8C01(alarm-events)# del all 1-3

del email

Syntax:

del email <range>

Description:

To delete event sent by email.

Argument:

<range>:syntax 1,5-7

Possible value:

<range>: 1~27

Example:

IFEL2P-SW8C01(alarm-events)# del email 1-3

del trap

Syntax:

del trap <range>

Description:

To disable the trap of the events.

Argument:

<range>:del the range of trap, syntax 1,5-7

Possible value:

<range>: 1~27

Example:

IFEL2P-SW8C01(alarm-events)# del trap 1-3

set all

Syntax:

set all <range>

Description:

To set trap of events.

Argument:

<range>: syntax 1,5-7

Possible value:

<range>: 1~27

Example:

IFEL2P-SW8C01(alarm-events)# set all 1-27

set email

Syntax:

set email <range>

Description:

To set events sent by email.

Argument:

<range>: set the range of email, syntax 1,5-7

Possible value:

<range>: 1~27

Example:

IFEL2P-SW8C01(alarm-events)# set email 1-5

set trap

Syntax:

set trap <range>

Description:

To set events sent by trap.

Argument:

<range>: set the range of trap, syntax 1,5-7

Possible value:

<range>: 1~27

Example:

IFEL2P-SW8C01(alarm-events)# set trap 1-5

show

Syntax:

show

Description:

To display the configuration of alarm event.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(alarm-events)# show

| Events | Email | Trap |
|--------------------------|-------|------|
| 1 Cold Start | v | v |
| 2 Warm Start | v | v |
| 3 Link Down | v | v |
| 4 Link Up | v | v |
| 5 Authentication Failure | v | v |
| 6 User Login | | |
| 7 User Logout | | |
| 8 STP Topology Changed | | |
| 9 STP Disabled | | |
| 10 STP Enabled | | |
| 11 LACP Disabled | | |
| 12 LACP Enabled | | |

13 LACP Member Added
14 LACP Port Failure
15 GVRP Disabled
16 GVRP Enabled
17 Port-based Vlan Enabled
18 Tag-based Vlan Enabled
19 Metro-mode Vlan Enabled
20 Module Inserted
21 Module Removed
22 Dual Media Swapped
23 Looping Detected
24 IP-MAC Binding Offered
25 IP-MAC Binding Released
26 ARP Inspection detected
27 Power Monitor

<<relay>>

set relay monitoring

Syntax:

set relay monitoring <range>

Description:

To set alarm relay monitoring function. Including “Power Monitoring” and “Port Monitoring”.

Argument:

<range>: syntax 1,5-7

Possible value:

<range>: 1~10 : Port 1 ~ Port 10

11~13 : Power A, Power B and Power C(DC Jack)

Example:

IFEL2P-SW8C01(alarm)#relay

IFEL2P-SW8C01(alarm-relay)#set relay monitoring 1-12

■ autologout

autologout

Syntax:

autologout <time>

Description:

To set up the timer of autologout.

Argument:

<time>: range 1 to 3600 seconds, 0 for autologout off.

Possible value:

<time>: 0,1-3600

Example:

IFEL2P-SW8C01# autologout 3600

Set autologout time to 3600 seconds

■ bandwidth

set egress

Syntax:

set egress <range> <rate>

Description:

To set up the egress-rate of the port.

Argument:

<range>:syntax 1,5-7, available from 1 to 10

<rate>: 64-1024000(Kbps).

port 1-8: 64-102400(Kbps)

port 9-10: 64-1024000(Kbps)

Possible value:

<range>:syntax 1,5-7, available from 1 to 10

<rate>: 64-1024000(Kbps).

port 1-8: 64-102400(Kbps)

port 9-10: 64-1024000(Kbps)

Example:

IFEL2P-SW8C01(bandwidth)# set egress 1-6 299

set ingress

Syntax:

set ingress <range> <rate>

Description:

To set up the ingress-rate of the ports.

Argument:

<range>:syntax 1,5-7, available from 1 to 10

<rate>: 64-1024000(Kbps)
port 1-8: 64-102400(Kbps)
port 9-10: 64-1024000(Kbps)

Possible value:

<range>: 1 to 10
<rate>: 64-1024000(Kbps)
port 1-8: 64-102400(Kbps)
port 9-10: 64-1024000(Kbps)

Example:

IFEL2P-SW8C01(bandwidth)# set ingress 1-6 100

set storm**Syntax:**

set storm <range> <type> <rate>

Description:

To set up the storm control.

Argument:

<range>:syntax: 1,3-5, available from 1 to 10

<type>:
0 - Disable
1 - BC for broadcast storm
2 - UC for unicast storm
3 - BC,UC for both broadcast and unicast storm
4 - MC for multicast storm
5 - BC,MC for both broadcast and multicast storm
6 - UC,MC for both unicast and multicast storm
7 - BC,UC,MC for broadcast, unicast and multicast storm
<rate>: 64-1024000(Kbps)
port 1-8: 64-102400(Kbps)
port 9-10: 64-1024000(Kbps)

Possible value:

<range>:syntax: 1,3-5, available from 1 to 10
<type>:
0 - Disable
1 - BC for broadcast storm
2 - UC for unicast storm
3 - BC,UC for both broadcast and unicast storm
4 - MC for multicast storm
5 - BC,MC for both broadcast and multicast storm
6 - UC,MC for both unicast and multicast storm
7 - BC,UC,MC for broadcast, unicast and multicast storm
<rate>: 64-1024000(Kbps)
port 1-8: 64-102400(Kbps)
port 9-10: 64-1024000(Kbps)

Example:

IFEL2P-SW8C01(bandwidth)# set storm 2 2 300

show**Syntax:**

show

Description:

To display all current settings of the bandwidth.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(bandwidth)# show

| Port | Ingress Rate(Kb) | Egress Rate(Kb) | Storm Type | Storm Rate(Kb) |
|-------|------------------|-----------------|------------|----------------|
| ===== | | | | |
| 1 | 102400 | 102400 | Disable | 102400 |
| 2 | 102400 | 102400 | Disable | 102400 |
| 3 | 102400 | 102400 | Disable | 102400 |
| | : | | | |
| | : | | | |
| 7 | 102400 | 102400 | Disable | 102400 |
| 8 | 102400 | 102400 | Disable | 102400 |
| 9 | 1024000 | 1024000 | Disable | 1024000 |
| 10 | 1024000 | 1024000 | Disable | 1024000 |

■ config-file

export start

Syntax:

export start

Description:

To run the export start function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(config-file)# export start
Export successful._

export user-conf

Syntax:

export user-conf

Description:

To run the export user-conf function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(config-file)# export user-conf
Export successful.

import start

Syntax:

import start

Description:

To run the import start function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(config-file)# import start
Import successful.

import user-conf

Syntax:

import user-conf

Description:

To run the import user-conf function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(config-file)# import user-conf
Import successful.

set export-path

Syntax:

set export-path <filepath>

Description:

To set up the file path and filename that user would like to export.

Argument:

<filepath>:filepath and filename

Possible value:

<filepath>:filepath and filename

Example:

IFEL2P-SW8C01(config-file)# set export-path log/21511.txt_

set import-path

Syntax:

set import-path <filepath>

Description:

To set up the filepath and filename that user would like to import.

Argument:

<filepath>:filepath and filename

Possible value:

<filepath>:filepath and filename

Example:

IFEL2P-SW8C01(config-file)# set import-path log/21511.txt_

show

Syntax:

show

Description:

To display the information of the config file.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(config-file)# show
TFTP Server IP Address: 192.168.3.111
Export Path and Filename: log/21511.txt
Import Path and Filename: log/21511.txt
```

■ **dhcp-boot**

set

Syntax:

set <sec>

Description:

To set up the delay time for DHCP Boot.

Argument:

<sec>:range syntax: 0, 1-30. The value "0" is to disable dhcp-boot delay

Possible value:

<sec>:0-30

Example:

```
IFEL2P-SW8C01(dhcp-boot)# set 30
```

show

Syntax:

show

Description:

To display the status of DHCP Boot.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(dhcp-boot)# show
DHCP Boot : Enable
Second    : 30
IFEL2P-SW8C01(dhcp-boot)#
```

■ dhcp-snooping

clear counter

Syntax:

clear counter

Description:

To clear DHCP counters.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(dhcp-snooping)# clear counter

clear lease

Syntax:

clear lease

Description:

To clear all DHCP leases.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(dhcp- snooping)#clear lease

del

Syntax:

del <tr_vid>

Description:

To delete trust group.

Argument:

<tr_vid>

Possible value:

<tr_vid>:trust VID, 1-4094

Example:

IFEL2P-SW8C01(dhcp-snooping)# del 2

disable

Syntax:

disable

Description:

To disable DHCP snooping.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(dhcp-snooping)# disable

enable

Syntax:

enable

Description:

To enable DHCP snooping.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(dhcp-snooping)# enable

set client-counter

Syntax:

set client-count <range> <limit>

Description:

To set per port client count

Argument:

<range>

<limit>

Possible value:

<range>:syntax: 1,5-7, available from 1 to 10

<limit>:from 1 to 512, 0 for disable

Example:

IFEL2P-SW8C01(dhcp-snooping)# set client-count 2 20

set default-group

Syntax:

set default-group <sr_vid> <sport_range> <ip> <option> <act>

Description:

To set default group

Argument:

<sr_vid>

<sport_range>

<ip>

<option>

<act>

Possible value:

<sr_vid>:server VID, 1-4094

<sport_range>:server port with range format, max port 2 ports, 0 for disabled

<ip>:allowed DHCP server IP, set 0.0.0.0 as disabled

<option>:option 82 state, 1 for enable, 0 for disable

<act>:Action when receiving DHCP packets which already contain option 82

0: Replace

1: Keep

2: Drop

Example:

IFEL2P-SW8C01(dhcp-snooping)# set default-group 2 1 192.168.1.248 1 1

set trust-group

Syntax:

set trust-group <tr_vid> <sr_vid> <sport_range> <sip> <option> <act>

Description:

To set default group

Argument:

<tr_vid>

<sr_vid>

<sport_range>

<sip>

<option>

<act>

Possible value:

<tr_vid>:Trust VID, 1-4094

<sr_vid>:Server VID, 1-4094

<sport_range>:Server port with range format, max port 2 ports

<sip>:allowed DHCP server IP

set 0.0.0.0 as disabled

<option>:option 82 state, 1 for enable, 0 for disable

<act>:Action when receiving DHCP packets which already contain option 82

0: Replace

1: Keep

2: Drop

Example:

IFEL2P-SW8C01(dhcp-snooping)# set trust-group 2 1 1 192.168.1.248 1 1

show config

Syntax:

show config

Description:

To show DHCP snooping configuration.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(dhcp-snooping)# show config

DHCP Snooping Config:

=====

State : Enable

Port 1 Client Count :128

Port 2 Client Count :128

Port 3 Client Count :128

Port 4 Client Count :128

Port 5 Client Count :128

Port 6 Client Count :128

Port 7 Client Count :128

Port 8 Client Count :128

Port 9 Client Count :128

Port10 Client Count :128

show counter

Syntax:

show counter

Description:

To show DHCP snooping counter.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(dhcp-snooping)# show counter

DHCP Snooping counters:

```
=====
```

| Port | Discovery | Offer | Request | Decline | Ack | Nack | Release | Inform |
|-------|-----------|-------|---------|---------|-------|-------|---------|--------|
| ===== | ===== | ===== | ===== | ===== | ===== | ===== | ===== | ===== |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Show default-group

Syntax:

show default-group

Description:

To show default group.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(dhcp-snooping)# show default-group

DHCP Default Group Config:

```
=====
```

```
Server VID : 1
Server IP  : 0.0.0.0
Server Port : (none)
Option 82  : Disable
Action     : Keep
```

show lease

Syntax:

show lease

Description:

To show DHCP snooping lease.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(dhcp-snooping)# show lease

Latest DHCP Snooping lease count : 0

show trust-group

Syntax:

show trust-group

Description:

To show trust group.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(dhcp-snooping)# show trust-group

■ dhcprelay

disable

Syntax:

disable

Description:

To disable DHCP relay.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(dhcprelay)# disable
```

```
IFEL2P-SW8C01(dhcprelay)# show config
```

```
DHCP Relay is disabled
```

enable

Syntax:

enable

Description:

To enable DHCP relay.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(dhcprelay)# enable
```

```
IFEL2P-SW8C01(dhcprelay)# show config
```

```
DHCP Relay Configuration:
```

```
    DHCP Relay Status   : Enabled
```

```
    DHCP LifeTime [5]   : 5
```

```
    DHCP Relay Agent Information Option82 State : Disabled
```

```
    DHCP Relay Agent Information Option82 Policy: Keep
```

```
    Server IP : 0.0.0.0
```

```
    Server Port : (none)
```

set lifetime

Syntax:

```
set lifetime <time>
```

Description:

To set lifetime.

Argument:

<time>

Possible value:

<time>: from 1 to 10 seconds

Example:

```
IFEL2P-SW8C01(dhcprelay)# set lifetime 10
```

set port-sip

Syntax:

set port-sip <sport_range> <sip>

Description:

To set DHCP server port and IP.

Argument:

<sport_range>:

<sip>:

Possible value:

<sport_range>: server port with range format, max port 2 ports

<sip>: allowed DHCP server IP, set 0.0.0.0 as disabled

Example:

IFEL2P-SW8C01(dhcprelay)# set port-ip 2 0.0.0.0

set state

Syntax:

set state <option> <act>

Description:

To set DHCP-relay option82 state.

Argument:

<option>:

<act>:

Possible value:

<option>: option 82 state, 1 for enable, 0 for disable

<act>: allowed DHCP server IP, set 0.0.0.0 as disabled

Example:

IFEL2P-SW8C01(dhcprelay)#

show config

Syntax:

show config

Description:

To show DHCP-relay configuration.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(dhcprelay)#show config

DHCP Relay Configuration:

DHCP Relay Status : Enabled

DHCP LifeTime [5] : 10

DHCP Relay Agent Information Option82 State : Disabled

DHCP Relay Agent Information Option82 Policy: Keep

Server IP : 0.0.0.0

Server Port : 1,

■ diag

autoping

Syntax:

autoping

Description:

Enter into autoping mode

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(diag)#autoping

IFEL2P-SW8C01(diag-autoping)#

disable

Syntax:

disable

Description:

Disable autoping function

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(diag-autoping)#disable

IFEL2P-SW8C01(diag-autoping)#show

Auto Ping State : Disabled

enable

Syntax:

enable

Description:

Enable autoping function

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(diag-autoping)#enable

IFEL2P-SW8C01(diag-autoping)#show

Auto Ping State : Enabled

IP Address :

Interval(sec) : 20

Times : 10

set

Syntax:

set <IP address> <interval> <times>

Description:

Setting autoping function

Argument:

<IP address>

<interval>

<times>

Possible value:

<IP address> : IPv4 format

<interval> : 1~300 (sec)

<times> : 3~100

Example:

```
IFEL2P-SW8C01(diag-autoping)#set 192.168.1.248 10 6
```

```
IFEL2P-SW8C01(diag-autoping)#show
```

```
Auto Ping State : Enabled
```

```
IP Address      : 192.168.1.248
```

```
Interval(sec)   : 10
```

```
Times           : 6
```

show

Syntax:

show

Description:

To show auto ping state

Argument:

None

Possible value:

None

Example:

```
IFEL2P-SW8C01(diag-autoping)#show
```

```
Auto Ping State : Disabled
```

cable

Syntax:

Cable <port>

Description:

Cable diagnostic

Argument:

<port>

Possible value:

<port>: ports to be diagnosed its cable, available from 1 to 8

Example:

```
IFEL2P-SW8C01(diag)#cable 8
```

```
Port 8 cable OK(0 pairs)
```

diag

Syntax:

diag

Description:

Diag is used to test whether EEPROM, UART, DRAM and Flash is normal or not.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(diag)# diag

EEPROM Test : OK

UART Test : OK

DRAM Test : OK

Flash Test : OK

loopback

Syntax:

loopback

Description:

For Internal/External Loopback Test.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(diag)# loopback

Internal Loopback Test : OK

External Loopback Test : Port 1 2 3 4 5 6 7 8 10 Fail

ping

Syntax:

ping <ip>

Description:

To confirm that whether the remote end-station or switch itself is alive or not.

Argument:

<ip> : IP address or domain name

Possible value:

IP address, e.g. 192.168.2.65 or domain name, e.g. tw.yahoo.com

Example:

IFEL2P-SW8C01(diag)# ping 192.168.1.115

Gateway : 192.168.1.253

192.168.1.115 is alive.

■ firmware

set upgrade-path

Syntax:

set upgrade-path <filepath>

Description:

To set upgrade file path and name

Argument:

<filepath>: upgrade file path and name

Possible value:

<filepath>: upgrade file path and name

Example:

IFEL2P-SW8C01(firmware)# set upgrade-path IPES2410_v2.05.img

show

Syntax:

show

Description:

To display the information of TFTP server and upgrade-path and file name.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(firmware)# show

TFTP Server IP Address: 192.168.3.111

Path and Filename : IPES2410_v2.05.img

upgrade

Syntax:

upgrade

Description:

To run the software upgrade function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(firmware)# upgrade

Upgrading firmware ...

■ gvrp

disable

Syntax:

disable

Description:

To disable the gvrp function

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(gvrp)# disable

enable

Syntax:

enable

Description:

To enable the gvrp function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(gvrp)# enable

group

Syntax:

group <group number>

Description:

To enter any of gvrp group for changing gvrp group setting. You can change the applicant or registrar mode of existing gvrp group per port.

Argument:

<group number>: enter which gvrp group you had created, using value is vid.

Available range: 1 to 4094

Possible value:

<group number>: 1 to 4094

Example:

IFEL2P-SW8C01(gvrp)# show group

GVRP group information

Current Dynamic Group Number: 1

VID Member Port

2

5

```
IFEL2P-SW8C01(gvrp)# group 2
IFEL2P-SW8C01(gvrp-group-2)# set applicant 1-6 non-participant
```

```
IFEL2P-SW8C01(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant      Registrar
```

```
-----
1  Non-Participant Normal
2  Non-Participant Normal
3  Non-Participant Normal
4  Non-Participant Normal
5  Non-Participant Normal
6  Non-Participant Normal
7  Normal              Normal
      :
      :
9  Normal              Normal
10 Normal              Normal
```

```
IFEL2P-SW8C01(gvrp-group-2)# set registrar 1-6 fixed
```

```
IFEL2P-SW8C01(gvrp-group-2)# show
GVRP group VID: 2
Port Applicant      Registrar
```

```
-----
1  Non-Participant Fixed
2  Non-Participant Fixed
3  Non-Participant Fixed
4  Non-Participant Fixed
5  Non-Participant Fixed
6  Non-Participant Fixed
7  Normal              Normal
8  Normal              Normal
9  Normal              Normal
10 Normal              Normal
```

set applicant

Syntax:

set applicant <range> <normal|non-participant>

Description:

To set default applicant mode for each port.

Argument:

<range>: port range, syntax 1,5-7, available from 1 to 10

<normal>: set applicant as normal mode

<non-participant>: set applicant as non-participant mode

Possible value:

<range>: 1 to 10

<normal|non-participant>: normal or non-participant

Example:

IFEL2P-SW8C01(gvrp)# set applicant 1-8 non-participant

set registrar

Syntax:

set registrar <range> <normal|fixed|forbidden>

Description:

To set default registrar mode for each port.

Argument:

<range>: port range, syntax 1,5-7, available from 1 to 10

<normal>: set registrar as normal mode

<fixed>: set registrar as fixed mode

<forbidden>: set registrar as forbidden mode

Possible value:

<range>: 1 to 10

<normal|fixed|forbidden>: normal or fixed or forbidden

Example:

IFEL2P-SW8C01(gvrp)# set registrar 1-5 fixed

set restricted

Syntax:

set restricted <range> <enable|disable>

Description:

To set the restricted mode for each port.

Argument:

<range>: port range, syntax 1,5-7, available from 1 to 10

<enable>: set restricted as enabled

<disable>: set restricted as disabled

Possible value:

<range>: 1 to 10

<enable|disable>: enable or disable

Example:

```
IFEL2P-SW8C01(gvrp)# set restricted 1-10 enable
```

```
IFEL2P-SW8C01(gvrp)# show config
```

```
GVRP state: Enable
```

```
Port Join Time Leave Time LeaveAll Time Applicant Registrar Restricted
```

| | | | | | | |
|----|----|----|------|--------|--------|--------|
| 1 | 20 | 60 | 1000 | Normal | Normal | Enable |
| 2 | 20 | 60 | 1000 | Normal | Normal | Enable |
| 3 | 20 | 60 | 1000 | Normal | Normal | Enable |
| 4 | 20 | 60 | 1000 | Normal | Normal | Enable |
| 5 | 20 | 60 | 1000 | Normal | Normal | Enable |
| 6 | 20 | 60 | 1000 | Normal | Normal | Enable |
| 7 | 20 | 60 | 1000 | Normal | Normal | Enable |
| 8 | 20 | 60 | 1000 | Normal | Normal | Enable |
| 9 | 20 | 60 | 1000 | Normal | Normal | Enable |
| 10 | 20 | 60 | 1000 | Normal | Normal | Enable |

set timer**Syntax:**

```
set timer <range> <join> <leave> <leaveall>
```

Description:

To set gvrp join time, leave time, and leaveall time for each port.

Argument:

<range> : port range, syntax 1,5-7, available from 1 to 10

<join>: join timer, available from 20 to 100

<leave>: leave timer, available from 60 to 300

<leaveall>: leaveall timer, available from 1000 to 5000

Leave Time must equal double Join Time at least.

Possible value:

<range> : 1 to 10

<join>: 20 to 100

<leave>: 60 to 300

<leaveall>: 1000 to 5000

Example:

```
IFEL2P-SW8C01(gvrp)# set timer 2-8 25 80 2000
```

show config**Syntax:**

```
show config
```

Description:

To display the gvrp configuration.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(gvrp)# show config
```

GVRP state: Disable

| Port | Join Time | Leave Time | LeaveAll Time | Applicant | Registrar | Restricted |
|------|-----------|------------|---------------|-----------|-----------|------------|
| 1 | 20 | 60 | 1000 | Normal | Normal | Disable |
| 2 | 20 | 60 | 1000 | Normal | Normal | Disable |
| 3 | 20 | 60 | 1000 | Normal | Normal | Disable |
| 4 | 20 | 60 | 1000 | Normal | Normal | Disable |
| | | : | | | | |
| | | : | | | | |
| | | : | | | | |
| 9 | 20 | 60 | 1000 | Normal | Normal | Disable |
| 10 | 20 | 60 | 1000 | Normal | Normal | Disable |

show counter

Syntax:

show counter <port>

Description:

To show gvrp counter of the port.

Argument:

<port>: port number, available from 1 to 10

Possible value:

<port>: 1 to 10

Example:

IFEL2P-SW8C01(gvrp)# show counter 2

GVRP Counter port: 2

| Counter Name | Received | Transmitted |
|--------------|----------|-------------|
|--------------|----------|-------------|

| | | |
|----------------------|---|------|
| Total GVRP Packets | 0 | 0 |
| Invalid GVRP Packets | 0 | ---- |
| LeaveAll message | 0 | 0 |
| JoinEmpty message | 0 | 0 |
| JoinIn message | 0 | 0 |
| LeaveEmpty message | 0 | 0 |
| Empty message | 0 | 0 |

show group

Syntax:

show group

Description:

To show the gvrp group.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(gvrp)# show group

GVRP group information

Current Dynamic Group Number: 0

| VID | Member Port |
|-----|-------------|
|-----|-------------|

■ hostname

hostname

Syntax:

hostname <name>

Description:

To set up the hostname of the switch.

Argument:

<name>: hostname, max. 40 characters.

Possible value:

<name>: hostname, max. 40 characters.

Example:

```
IFEL2P-SW8C01# hostname Company
Company#ip
Company(ip)#
```

■ IP

disable dhcp

Syntax:

disable dhcp

Description:

To disable the DHCP function of the system.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(ip)# disable dhcp
DHCP is already stopped.
```

enable dhcp

Syntax:

enable dhcp <manual|auto>

Description:

To enable the system DHCP function and set DNS server via manual or auto mode.

Argument:

<manual|auto> : set DNS by using manual or auto mode.

Possible value:

<manual|auto> : manual or auto

Example:

```
IFEL2P-SW8C01(ip)# enable dhcp manual
```

set dns

Syntax:

set dns <ip>

Description:

To set the IP address of DNS server.

Argument:

<ip> : dns ip address

Possible value:

<ip> : 168.95.1.1

Example:

IFEL2P-SW8C01(ip)# set dns 168.95.1.1

set ip

Syntax:

set ip <ip> <mask> <gateway>

Description:

To set the system IP address, subnet mask and gateway.

Argument:

<ip> : ip address

<mask> : subnet mask

<gateway> : default gateway

Possible value:

<ip> : 192.168.1.1 or others

<mask> : 255.255.255.0 or others

<gateway> : 192.168.1.253 or others

Example:

IFEL2P-SW8C01(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253

show

Syntax:

show

Description:

To display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(ip)# show
DHCP           : Disable
IP Address      : 192.168.1.1
Current IP Address : 192.168.1.1
Subnet mask     : 255.255.255.0
Gateway        : 192.168.1.253
DNS Setting     : Manual
DNS Server      : 192.95.1.1
```

■ ip-mac-bind

add

Syntax:

add <name> <mac> <ip> <port_range> <method>

Description:

To set the system IP address, subnet mask and gateway.

Argument:

<name>:entry name

<mac>:mac address

<ip> : ip address

<port_range> : range syntax: 1,5-7, available from 1 to 10

<method> : binding method

Possible value:

<name>:entry name

<mac>:mac address

<ip> : ip address

<port_range> : range syntax: 1,5-7, available from 1 to 10

<method> : binding method

0: IP and MAC

1: IP only

2: MAC only

Example:

IFEL2P-SW8C01(ip-mac-bind)# add entry1 00-40-c7-3f-00-d2 192.168.1.200 2 0

del ip

Syntax:

del ip <ip>

Description:

To delete by IP.

Argument:

<ip>: IP address

Possible value:

<ip>: IP address

Example:

IFEL2P-SW8C01(ip-mac-bind)# del ip 192.168.1.200

del mac

Syntax:

del mac <mac>

Description:

To delete by MAC.

Argument:

<mac>: MAC address

Possible value:

<mac>: MAC address

Example:

IFEL2P-SW8C01(ip-mac-bind)# del mac 00-40-c7-3f-00-d2

del name

Syntax:

del name <name>

Description:

To delete by name.

Argument:

<name>: entry name

Possible value:

<name>: entry name

Example:

IFEL2P-SW8C01(ip-mac-bind)# del name entry1

disable

Syntax:

disable

Description:

To disable IP-MAC Binding.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(ip-mac-bind)# disable

enable

Syntax:

enable

Description:

To enable IP-MAC Binding.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(ip-mac-bind)# enable

show list

Syntax:

show list

Description:

To show binding list.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(ip-mac-bind)# show list

Current user count: 0

show status

Syntax:

show status

Description:

To show IP-MAC binding status.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(ip-mac-bind)# show status

IP-MAC-Binding Status : Enable

Binding Port : 1 2 3 4 5 6 7 8 9 10

■ **lldp**

set clear

Syntax:

set clear

Description:

To clear counter

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(lldp)# set clear

set mode

Syntax:

set mode <range> <mode>

Description:

To set LLDP mode

Argument:

<range>:syntax: 1,5-7

<mode>:set LLDP state

Possible value:

<range>:available from 1 to 10

<mode>:set LLDP state

disabled = 0

tx and rx = 1

tx only = 2

rx only = 3

Example:

IFEL2P-SW8C01(lldp)# set mode 2 1

set notification

Syntax:

set notification <range> <notification>

Description:

To enable/disable LLDP notification

Argument:

<range>:syntax: 1,5-7

<notification>:enable/disable LLDP notification

Possible value:

<range>:syntax: 1,5-7, available from 1 to 10

<notification>:enable/disable LLDP notification

enable = 1

disable = 2

Example:

IFEL2P-SW8C01(lldp)# set notification 1-10 1

set notificationinterval

Syntax:

set notificationinterval <time>

Description:

To set notification interval

Argument:

<time>:

Possible value:

<time>:from 5 to 3600 seconds

Example:

IFEL2P-SW8C01(lldp)# set notificationinterval 200

set reInitDelay

Syntax:

set reInitDelay <time>

Description:

To set reinit delay

Argument:

<time>:

Possible value:

<time>:from 1 to 10 seconds

Example:

IFEL2P-SW8C01(lldp)# set reInitDelay 2

set tlv

Syntax:

set tlv <#> <#> <#> <#> <#> <#>

Description:

To disable/enable LLDP tlv

Argument:

Port Description: bit 0

System Name: bit 1

System Description: bit 2
System Capabilities: bit 3
Management Address: bit 4
port range syntax : 1,5-7, available from 1 to 10
Possible value:
Port Description: bit 0
System Name: bit 1
System Description: bit 2
System Capabilities: bit 3
Management Address: bit 4
port range syntax : 1,5-7, available from 1 to 10

set txDelay

Syntax:

set txDelay <time>

Description:

To set Tx Delay

Argument:

<time>:

Possible value:

<time>: from 1 to 8192 second(s)

Example:

IFEL2P-SW8C01(lldp)# set txDelay 200

set txHold

Syntax:

set txHold <time>

Description:

To set Tx Hold

Argument:

<time>:

Possible value:

<time>: from 2 to 10 second(s)

Example:

IFEL2P-SW8C01(lldp)# set txHold 3

set txIntervl

Syntax:

set txInterval <time>

Description:

To set Tx interval

Argument:

<time>:

Possible value:

<time>: from 5 to 32768 second(s)

Example:

IFEL2P-SW8C01(lldp)# set txInterval 60

show Local-device

Syntax:

show Local-device

Description:

To show LLDP local device

Argument:

None

Possible value:

None

Example:

```
IFEL2P-SW8C01(Ifdp)# show Local-device
LLDP Local Devices Information
```

Chassis Type : MAC-address

Chassis Id : 00-40-c7-3f-00-d2

System name : IFEL2P-SW8C01

System Description :

System Capabilities : bridge

System Capabilities : bridge

Management Address :

Type : ipv4

Address : 192.168.1.1

LLDP Port Information

| Port | PortType | PortId | PortDesc |
|------|----------|--------|----------|
| 1 | local | 1 | Port #1 |
| 2 | local | 2 | Port #2 |
| 3 | local | 3 | Port #3 |
| 4 | local | 4 | Port #4 |
| 5 | local | 5 | Port #5 |
| 6 | local | 6 | Port #6 |

...(q to quit)

show Local-info

Syntax:

show Local-info <port>

Description:

To show LLDP local information

Argument:

<port>

Possible value:

<port> :1,5-7 , available from 1 to 10

Example:

```
IFEL2P-SW8C01(Ifdp)# show Local-info 2
```

LLDP Local Port Information Detail

Port :2

PortType :local

PortId :2
PortDesc :Port #2

show Neighbor

Syntax:

show Neighbor <port>

Description:

To show LLDP remote entry

Argument:

<port>

Possible value:

<port> :syntax 1,5-7 , available from 1 to 10

Example:

IFEL2P-SW8C01(lldp)# show Neighbor 2

show config

Syntax:

show config

Description:

To show LLDP configuration

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(lldp)# show config
LLDP Global Configuration

LLDP Transmit Interval [30] : 30
LLDP Hold time Multiplier [4] : 4
LLDP Delay Interval [2] : 2
LLDP Reinit Interval [2] : 2
LLDP Notification Interval [5] : 5

LLDP Port Configuration

Port AdminStatus NotificationEnabled

| | | |
|----|---------|-------|
| 1 | Disable | False |
| 2 | Disable | False |
| 3 | Disable | False |
| 4 | Disable | False |
| 5 | Disable | False |
| 6 | Disable | False |
| 7 | Disable | False |
| 8 | Disable | False |
| 9 | Disable | False |
| 10 | Disable | False |

show detail-counter

Syntax:

show detail-counter <port>

Description:

To show LLDP per port counter

Argument:

<port>

Possible value:

<port>: syntax 1,5-7 , available from 1 to 10

Example:

IFEL2P-SW8C01(lldp)# show detail-counter 2

show port-config

Syntax:

show port-config <port>

Description:

To show LLDP per port configuration

Argument:

<port>

Possible value:

<port>: syntax 1,5-7 , available from 1 to 10

Example:

IFEL2P-SW8C01(lldp)# show port-config 2

show remote-device

Syntax:

show remote-device

Description:

To show LLDP remote device

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(lldp)# show remote-device

show stats

Syntax:

show stats

Description:

To show LLDP counter

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(lldp)# show stats
LLDP Device Statistics

Neighbor Entries List Last Updated : 0 Days 1 Hours 31 Mins 4 Secs
 New Neighbor Entries Count : 0
 Neighbor Entries Deleted Count : 0
 Neighbor Entries Dropped Count : 0
 Neighbor Entries AgeOut Count : 0

LLDP Port Statistics

| | Tx | Rx | Rx | Rx | TLV | TLV | |
|------|--------|--------|--------|----------|----------|---------|------|
| Port | Frames | Frames | Errors | Discards | Discards | Unknown | Aged |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

■ log

clear

Syntax:

clear

Description:

To clear the log data.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(log)# clear

disable auto-upload

Syntax:

disable auto-upload

Description:

To disable the auto-upload function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(log)# disable auto-upload

enable auto-upload

Syntax:

enable auto-upload

Description:

To enable the auto-upload function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(log)# enable auto-upload

show

Syntax:

show

Description:

To show a list of trap log events. When any of log events happens, it will be recorded and using show command in log function to query. Up to 120 log records are supported.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(log)# show

Tftp Server : 0.0.0.0

Auto Upload : Disable

- 1) Wed Apr 13 12:13:27 2005 Link Up [Port 1]
- 2) Wed Apr 13 12:13:26 2005 Link Down [Port 1]
- 3) Wed Apr 13 11:58:31 2005 Login [admin]
- 4) Wed Apr 13 11:19:45 2005 Login [admin]
- 5) Wed Apr 13 11:19:37 2005 Logout [admin]

upload

Syntax:

Upload

Description:

To upload log data through tftp.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(log)# upload

■ loop-detection

disable action

Syntax:

disable action

Description:

To disable the locked-port action when loop occurs

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(loop-detection)# disable action

disable port

Syntax:

disable port <range>

Description:

To disable Loop Detection by port

Argument:

<range>

Possible value:

<range>:syntax 1,5-7 , available from 1 to 10

Example:

IFEL2P-SW8C01(loop-detection)# disable port 2

enable action

Syntax:

enable action

Description:

To enable the locked-port action when loop occurs

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(loop-detection)# enable action

enable port

Syntax:

enable port

Description:

To enable Loop Detection by port

Argument:

<range>:

Possible value:

<range>:syntax 1,5-7 , available from 1 to 10

Example:

IFEL2P-SW8C01(loop-detection)# enable port 2

resume port

Syntax:

resume port <range>

Description:

To remove locked-port

Argument:

<range>:syntax 1,5-7

Possible value:

<range> : available from 1 to 10

Example:

IFEL2P-SW8C01(loop-detection)# resume port 1

show

Syntax:

show

Description:

To display loop-detection status

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(loop-detection)# show

Locked port action: Disable

Port Loop-detection Current-status

| | | |
|----|---------|----------|
| 1 | Disable | Unlocked |
| 2 | Disable | Unlocked |
| 3 | Disable | Unlocked |
| 4 | Disable | Unlocked |
| 5 | Disable | Unlocked |
| 6 | Disable | Unlocked |
| 7 | Disable | Unlocked |
| 8 | Disable | Unlocked |
| 9 | Disable | Unlocked |
| 10 | Disable | Unlocked |

■ mac-table

<<alias>>

del

Syntax:

del <mac>

Description:

To delete the mac alias entry.

Argument:

<mac> : mac address

Possible value:

<mac> : mac address , format: 00-02-03-af-05-06

Example:

IFEL2P-SW8C01#mac-table

IFEL2P-SW8C01(mac-table)#alias

IFEL2P-SW8C01(mac-table-alias)# del 00-44-33-44-55-44

set

Syntax:

set <mac> <alias>

Description:

To set up the mac alias entry.

Argument:

<mac> : mac address, format: 00-02-03-04-05-06

<alias> : mac alias name, max. 15 characters

Possible value:

<mac> : mac address

<alias> : max. 15 characters

Example:

IFEL2P-SW8C01(mac-table-alias)# set 00-44-33-44-55-44 www

show

Syntax:

show

Description:

To show the mac alias entry.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(mac-table-alias)# show

MAC Alias List

| MAC Address | Alias |
|-------------|-------|
|-------------|-------|

- | | | |
|----|-------------------|-----|
| 1) | 00-02-03-04-05-06 | aaa |
| 2) | 00-33-03-04-05-06 | ccc |

<<information>>

search

Syntax:

search <port> <mac> <vid>

Description:

To search the relative mac information in mac table.

Argument:

<port> : set up the range of the ports to search for,

syntax 1,5-7, available form 1 to 10

<mac> : mac address, format: 01-02-03-04-05-06, '?' can be used

<vid> : vlan id, from 1 to 4094; '?' as don't care, 0 as untagged

Possible value:

<port> : 1 to 10

<mac> : mac address, format: 01-02-03-04-05-06, '?' can be used

<vid> : 0, 1 ~4094

Example:

IFEL2P-SW8C01(mac-table-information)# search 1-10 ??-??-??-??-??-?? ?

MAC Table List

| Alias | MAC Address | Port | VID | State |
|-------|-------------|------|-----|-------|
|-------|-------------|------|-----|-------|

| | | | |
|-------------------|---|---|---------|
| 00-40-c7-88-00-06 | 1 | 0 | Dynamic |
|-------------------|---|---|---------|

IFEL2P-SW8C01(mac-table-information)#

show

Syntax:

show

Description:

To display all mac table information.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(mac-table-information)# show

MAC Table List

| Alias | MAC Address | Port | VID | State |
|-------|-------------|------|-----|-------|
|-------|-------------|------|-----|-------|

| | | | | |
|--------|-------------------|---|---|-------------------|
| ABC | 00-40-c7-d6-00-01 | 1 | 2 | Static Forwarding |
| ABC123 | 00-40-c7-d6-00-02 | 1 | 3 | Static Filtering |

<<maintain>>

flush

Syntax:

flush

Description:

To flush the MAC table

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(mac-table-maintain)# flush

set aging

Syntax:

set aging <time>

Description:

To set mac table aging out time.

Argument:

<time>:MAC table age out time

Possible value:

<time>:MAC table age out time between 10 and 1000000 seconds
set time to 0 as disable age out time

Example:

IFEL2P-SW8C01(mac-table-maintain)# set aging 100

set learning

Syntax:

set learning <port> <num>

Description:

To set mac table learning.

Argument:

<port>:syntax: 1,5-7

<num>: MAC address numbers which can be dynamically learned

Possible value:

<port>:1 to 10

<num>:0 to 8191; 0 for learning disabled

Example:

IFEL2P-SW8C01(mac-table-maintain)# set learning 3 0

show

Syntax:

show

Description:

To show the MAC table maintenance

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(mac-table-maintain)# show

<<port-security>>

disable**Syntax:**

disable <range>

Description:

To disable port security

Argument:

<range>:syntax 1,5-7

Possible value:

<range>:1 to 10

Example:

IFEL2P-SW8C01(mac-table-port-security)# disable 2

enable**Syntax:**

enable <range>

Description:

To enable port security

Argument:

<range>:syntax 1,5-7

Possible value:

<range>:1 to 10

Example:

IFEL2P-SW8C01(mac-table- port-security)# enable 1-10

port**Syntax:**

port <range>

Description:

To enter into per port static MAC mode

Argument:

<range>:syntax 1,5-7

Possible value:

<range>:1 to 26

Example:

IFEL2P-SW8C01(mac-table- port-security)# port 8

show**Syntax:**

show

Description:

To show port security

Argument:

None

Possible value:

None

Example:

```
IFEL2P-SW8C01(mac-table- port-security)# show  
<<static-mac>>
```

add**Syntax:**

```
add <mac> <vid> <rule> <port>
```

Description:

To set static MAC entry

Argument:

<mac>:mac address, format: 01-02-03-04-05-06

<vid>:VLAN ID

<rule>:forwarding rule

<port>:forwarded destination port

Possible value:

<mac>:mac address, format: 01-02-03-04-05-06

<vid>:1 to 4094

<rule>:forwarding rule; from 0 to 2

0:static;

1:drop destination address matches;

2:drop source address matches

<port>:from 1 to 10

Example:

```
IFEL2P-SW8C01(mac-table-static-mac)# add xx-xx-xx-xx-xx-xx 20 0 2
```

del**Syntax:**

```
del <mac>
```

Description:

To delete static MAC entry

Argument:

<mac>:mac address, format: 01-02-03-04-05-06

Possible value:

<mac>:mac address, format: 01-02-03-04-05-06

Example:

```
IFEL2P-SW8C01(mac-table-static-mac)# del xx-xx-xx-xx-xx-xx
```

show**Syntax:**

```
show
```

Description:

To show static MAC entry

Argument:

None

Possible value:

None

Example:

```
IFEL2P-SW8C01(mac-table-static-mac)# show
```

■ management

del

Syntax:

del <name>

Description:

To delete a management security entry.

Argument:

<name> : management security entry name

Possible value:

<name> : management security entry name

Example:

```
IFEL2P-SW8C01(management)# show
```

```
1):
```

```
Name      : Tom
```

```
VID       : Any
```

```
IP Range  : Any
```

```
Port      : Any
```

```
Access    : Http Telnet SNMP
```

```
Action    : Deny
```

```
IFEL2P-SW8C01(management)# del 1
```

```
IFEL2P-SW8C01(management)# show
```

Security rule list is empty now

set access

Syntax:

set access <name> <range>

Description:

To setup access type field of a management security entry.

Argument:

<name> : management security entry name

<range> : 0:Any, 1:Http, 2:Telnet, 3:SNMP

Possible value:

<name>:

<range> : 0-3

Example:

```
IFEL2P-SW8C01(management)#set access Tom 1-3
```

```
IFEL2P-SW8C01(management)#show
```

```
1):
```

```
Name      : Tom
```

```
VID       : Any
```

```
IP Range  : Any
```

```
Port      : Any
```

```
Access    : Http Telnet SNMP
```

```
Action    : Deny
```

set action

Syntax:

set action <name> <act>

Description:

To setup action field of a management security entry.

Argument:

<name> : management security entry name

<act> : 0:Deny 1:Accept

Possible value:

<act> : 0 or 1

Example:

IFEL2P-SW8C01(management)#set action Tom 1

IFEL2P-SW8C01(management)#show

1):

Name : Tom

VID : Any

IP Range : Any

Port : Any

Access : Http Telnet SNMP

Action : Accept

set ip

Syntax:

set ip <name> <ip1> <ip2>

Description:

To setup ip field of a management security entry.

Argument:

<name> : management security entry name

<ip1> : start ip address

<ip2> : end ip address

Possible value:

None

Example:

IFEL2P-SW8C01(management)#set ip Tom 192.168.1.1 192.168.1.20

IFEL2P-SW8C01(management)#show

1):

Name : Tom

VID : Any

IP Range : 192.168.1.1-192.168.1.20

Port : Any

Access : Http Telnet SNMP

Action : Accept

set port

Syntax:

set port <name> <range>

Description:

To setup port field of a management security entry.

Argument:

<name> : management security entry name

<range> : available from 0-10, 0 for any

Possible value:

<range> : 0-10

Example:

IFEL2P-SW8C01(management)#set port Tom 1-3

IFEL2P-SW8C01(management)#show

1):

Name : Tom

VID : Any

IP Range : 192.168.1.1-192.168.1.20

Port : 1 2 3

Access : Http Telnet SNMP

Action : Accept

set vid

Syntax:

set vid <name> <vid>

Description:

To setup vid field of a management security entry.

Argument:

<name> : management security entry name

<vid> : available from 0-4094, 0 for any

Possible value:

<range> : 0-4094

Example:

IFEL2P-SW8C01(management)#set vid Tom 2

IFEL2P-SW8C01(management)#show

1):

Name : Tom

VID : 2

IP Range : 192.168.1.1-192.168.1.20

Port : 1 2 3

Access : Http Telnet SNMP

Action : Accept

show

Syntax:

show

Description:

To show the specific management policy record.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(management)# show

1):

Name : Tom

VID : 2

IP Range : 192.168.1.1-192.168.1.20

Port : 1 2 3

Access : Http Telnet SNMP

Action : Accept

■ **mstp**

del-msti

Syntax:

del-msti <instance-id|all>

Description:

To delete an MST instance or all MST instances.

Argument:

<instance-id> : MSTI id

<instance-all>: to delete all configured MSTIs

Possible value:

<instance-id> : 1 to 4094

<instance-all>: to delete all configured MSTIs

Example:

IFEL2P-SW8C01(mstp)# del-msti all

disable

Syntax:

disable

Description:

To disable MSTP.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(mstp)# disable

enable

Syntax:

enable

Description:

To enable MSTP.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(mstp)# enable

MSTP started

migrate-check**Syntax:**

migrate-check <port range>

Description:

To execute migrate check on (a) port(s)

Argument:

<port range> : syntax: 1,5-7

Possible value:

<port range> : available from 1 to 10

Example:

IFEL2P-SW8C01(mstp)# migrate-check 2

set config**Syntax:**

set config <Max Age><Forward Delay><Max Hops>

Description:

To set max age,forward delay,max hops

Argument:

<Max Age>:available from 6 to 40. Recommended value is 20

<Forward Delay>:available from 4 to 30. Recommended value is 15

<Max Hops>:available from 6 to 40. Recommended value is 20

Possible value:

<Max Age>:available from 6 to 40. Recommended value is 20

<Forward Delay>:available from 4 to 30. Recommended value is 15

<Max Hops>:available from 6 to 40. Recommended value is 20

Note: 2*(Forward Delay -1) >= Max Age

Example:

IFEL2P-SW8C01(mstp)# set config 20 15 20

set msti-vlan**Syntax:**

set msti-vlan <instance-id><vid-string>

Description:

To map Vlan ID(s) to an MSTI

Argument:

<instance-id>:MSTI id

<vid-string>:vid-string syntax example: 2,5-7,100-200

Possible value:

<instance-id>:1 to 4094

<vid-string>:vid-string syntax example: 2,5-7,100-200
available from 1 to 4094

Example:

```
IFEL2P-SW8C01(mstp)# set msti-vlan 200 100
```

set p-cost

Syntax:

```
set p-cost <instance_id> <port range> <path cost>
```

Description:

To set port path cost per instance

Argument:

<instance_id> :MSTI id

<port range>:syntax: 1,5-7, available from 1 to 10

<path cost>:0, 1-200000000. The value zero means auto status

Possible value:

<instance_id>: MSTI id

<port range>:syntax: 1,5-7, available from 1 to 10

<path cost>:0, 1-200000000. The value zero means auto status

Example:

```
IFEL2P-SW8C01(mstp)# set p-cost 2 0
```

set p-edge

Syntax:

set p-edge <port range> <admin edge>

Description:

To set per port admin edge

Argument:

<port range> : syntax: 1,5-7, available from 1 to 10

<admin edge> : 0->non-edge port,1->edge port

Possible value:

<port range> : syntax: 1,5-7, available from 1 to 10

<admin edge> : 0->non-edge port,1->edge port

Example:

IFEL2P-SW8C01(mstp)# set p-edge 2 0

set p-hello

Syntax:

set p-hello <port range> <hello time>

Description:

To set per port hello time

Argument:

<port range> : syntax: 1,5-7, available from 1 to 10

<hello time> : only 1~2 are valid values

Possible value:

<port range> : syntax: 1,5-7, available from 1 to 10

<hello time> : only 1~2 are valid values

Example:

IFEL2P-SW8C01(mstp)# set p-hello 6 2

set p-p2p

Syntax:

set p-p2p <port range> <admin p2p>

Description:

To set per port admin p2p

Argument:

<port range> : syntax: 1,5-7, available from 1 to 10

<admin p2p> : Admin point to point, <auto|true|false>

Possible value:

<port range> : syntax: 1,5-7, available from 1 to 10

<admin p2p> : Admin point to point, <auto|true|false>

Example:

IFEL2P-SW8C01(mstp)# set p-p2p 6 auto

set p-priority

Syntax:

set p-priority <instance_id> <port range> <priority>

Description:

To Set port priority per instance

Argument:

<instance_id>: MSTI id

<port range> : syntax: 1,5-7, available from 1 to 10

<priority>:priority must be a multiple of 16, available from 0 to 240

Possible value:

<instance_id>: MSTI id

<port range> : syntax: 1,5-7, available from 1 to 10

<priority>:priority must be a multiple of 16, available from 0 to 240

Example:

IFEL2P-SW8C01(mstp)# set p-priority 20 3 32

set priority

Syntax:

set priority <instance-id><Instance Priority>

Description:

To set instance priority

Argument:

<instance_id>: 0->CIST;1-4094->MSTI

<Instance Priority>:must be a multiple of 4096,available from 0 to 61440

Possible value:

<instance_id>: 0->CIST;1-4094->MSTI

<Instance Priority>:must be a multiple of 4096,available from 0 to 61440

Example:

IFEL2P-SW8C01(mstp)# set priority 0 2000

set r-role

Syntax:

set r-role <port range> <restricted role>

Description:

To set per port restricted role

Argument:

<port range>:syntax: 1,5-7, available from 1 to 10

<restricted role>:0->>false,1->True

Possible value:

<port range>:syntax: 1,5-7, available from 1 to 10

<restricted role>:0->>false,1->True

Example:

IFEL2P-SW8C01(mstp)# set r-role 2 0

set r-tcn

Syntax:

set r-tcn <port range> <restricted tcn>

Description:

To set per port restricted tcn

Argument:

<port range>:syntax: 1,5-7, available from 1 to 10

<restricted tcn>:0->>false,1->True

Possible value:

<port range>:syntax: 1,5-7, available from 1 to 10

<restricted tcn>:0->>false,1->True

Example:

IFEL2P-SW8C01(mstp)# set r-tcn 2 0

set region-name

Syntax:

set region-name <string>

Description:

To set mstp region name(0~32 bytes)

Argument:

<string>:a null region name

Possible value:

<string>:a null region name
1-32

Example:

IFEL2P-SW8C01(mstp)# set region-name xxxxx

set revision-level

Syntax:

set revision-level <revision-level>

Description:

To set mstp revision-level(0~65535)

Argument:

<revision-level>:

Possible value:

<revision-level>:0 to 65535

Example:

IFEL2P-SW8C01(mstp)# set revision-level 1000

set version

Syntax:

set revision <stp|rstp|mstp>

Description:

To set force version

Argument:

<stp|rstp|mstp>:

Possible value:

<stp|rstp|mstp>:

Example:

IFEL2P-SW8C01(mstp)# set revision stp

show instance

Syntax:

show instance <instance-id>

Description:

To show instance status

Argument:

<instance-id>:

Possible value:

<instance-id>:0->CIST;1-4094->MSTI

Example:

IFEL2P-SW8C01(mstp)# show instance 0

show pconf

Syntax:

show pconf <instance-id>

Description:

To show port configuration

Argument:

<instance-id>:

Possible value:

<instance-id>:0->CIST;1-4094->MSTI

Example:

IFEL2P-SW8C01(mstp)# show pconf 0

show ports

Syntax:

show ports <instance-id>

Description:

To show port status

Argument:

<instance-id>:

Possible value:

<instance-id>:0->CIST;1-4094->MSTI

Example:

IFEL2P-SW8C01(mstp)# show ports 0

show region-info

Syntax:

show region-info

Description:

To show region configuration

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(mstp)# show region-info

show vlan-map

Syntax:

show vlan-map <instance-id>

Description:

To show vlan mapping of an instance

Argument:

<instance-id>:0->CIST;1-4094->MSTI

Possible value:

<instance-id>:0->CIST;1-4094->MSTI

Example:

IFEL2P-SW8C01(mstp)# show vlan-map 0

■ multicast

add group-filter

Syntax:

add group-filter <vid> <start> <end> <port>

Description:

To add group filter

Argument:

<vid>:VLAN ID

<start>:ip address format.

<end>:ip address format.

<port>:syntax: 1,5-7, from 1 to 10 value.

Possible value:

<vid>:from 1 to 4094 value.

<start>:ip address format.

<end>:ip address format.

<port>:syntax: 1,5-7, from 1 to 10 value.

Example:

IFEL2P-SW8C01(multicast)# add group-filter 20 192.168.1.1 192.168.1.10 1-3

add igmp-vlan

Syntax:

add igmp-vlan <vid>

Description:

To add IGMP VLAN

Argument:

<vid>:VLAN ID

Possible value:

<vid>:from 1 to 4094 value.

Example:

IFEL2P-SW8C01(multicast)# add igmp-vlan 20

delete group-filter

Syntax:

delete group-filter <vid> <index>

Description:

To delete group filter

Argument:

<vid>:VLAN ID

<index>:

Possible value:

<vid>:from 1 to 4094 value.

<index>:from 1 to 16

Example:

IFEL2P-SW8C01(multicast)# delete group-filter 20 20

delete igmp-vlan

Syntax:

delete igmp-vlan <vid>

Description:

To delete IGMP VLAN

Argument:

<vid>:VLAN ID

Possible value:

<vid>:from 1 to 4094 value.

Example:

IFEL2P-SW8C01(multicast)# delete igmp-vlan 20

edit group-filter

Syntax:

edit group-filter <vid> <index> <start> <end> <port>

Description:

To edit group filter

Argument:

<vid>:VLAN ID

<index>:1 to 16

<start>:ip address format.

<end>:ip address format.

<port>:syntax: 1,5-7, from 1 to 10 value.

Possible value:

<vid>:VLAN ID

<index>:1 to 16

<start>:ip address format.

<end>:ip address format.

<port>:syntax: 1,5-7, from 1 to 10 value.

Example:

IFEL2P-SW8C01(multicast)# edit group-filter 20 10 192.168.1.1 192.168.1.10 1-3

set acct-server

Syntax:

set acct-server <accounting service> <ip> <port-number> <secret key> <ip2>
<port-number>

Description:

To set 802.1x accounting state.

Argument:

<accounting service>: 0: Disable 1: Enable

<ip><ip2> : IPv4, xxx.xxx.xxx.xxx

<port-number> : 1-65535

<secret key> :

Possible value:

<accounting service>: 0: Disable 1: Enable

<ip><ip2> : IPv4, xxx.xxx.xxx.xxx

<port-number> : 1-65535

<secret key> : Length from 1 to 31 characters

Example:

IFEL2P-SW8C01(multicast)#set acct-server 192.168.1.248 1360 Topsecret

set gnlqry-parameter

Syntax:

set gnlqry <interval> <response> <timeout>

Description:

To set general query parameters

Argument:

<interval>: from 1 to 2000

<response>: from 1 to 10

<timeout>: from 1 to 30

Possible value:

<interval>: from 1 to 2000

<response>: from 1 to 10

<timeout>: from 1 to 30

Example:

IFEL2P-SW8C01(multicast)# set gnlqry 20 3 10

set group-limit

Syntax:

set group-limit <port> <limit>

Description:

To set multicast group limit

Argument:

<port> : syntax: 1,5-7, from 1 to 10

<limit> : from 0 to 256

Possible value:

<port> : syntax: 1,5-7, from 1 to 10

<limit> : from 0 to 256

Example:

IFEL2P-SW8C01(multicast)# set group-limit 2 10

set igmp-router

Syntax:

set igmp-router <port> <state>

Description:

To set IGMP router port

Argument:

<port> : syntax: 1,5-7, from 1 to 10

<state> : 0: none router

1: router

Possible value:

<port> : syntax: 1,5-7, from 1 to 10

<state> : 0: none router

1: router

Example:

IFEL2P-SW8C01(multicast)# set igmp-router 2 1

set igmpsnp-enable

Syntax:

set igmpsnp-enable <state>

Description:

To set IGMP snooping state

Argument:

<state> : 0: disable
 1: enable

Possible value:

<state> : 0: disable
 1: enable

Example:

IFEL2P-SW8C01(multicast)# set igmpsnp-enable 1

set mvr-enable

Syntax:

set mvr-enable <state> [<mvid>]

Description:

To set mvr state

Argument:

<state> : 0(disable), 1(enable).
[<mvid>]:from 1 to 4094 value. When set <state> to enable, the option is necessary.

Possible value:

<state> : 0(disable), 1(enable).
[<mvid>]:from 1 to 4094 value. When set <state> to enable, the option is necessary.

Example:

IFEL2P-SW8C01(multicast)# set mvr-enable 1 20

set mvr-tagging

Syntax:

set mvr-tagging <port> <state>

Description:

To set mvr tagging

Argument:

<port> : syntax: 1,5-7
<state>: 0(untag-out), 1(tag-out).

Possible value:

<port> : from 1 to 10
<state>: 0(untag-out), 1(tag-out).

Example:

IFEL2P-SW8C01(multicast)# set mvr-enable 1 20

set mvr-vid

Syntax:

set mvr-vid <vid>

Description:

To set mvr VLAN ID

Argument:

<vid> : VLAN ID

Possible value:

<vid> : from 1 to 10

Example:

IFEL2P-SW8C01(multicast)# set mvr-vid 1

set mvrserve-type

Syntax:

set mvrserve-type <port> <type>

Description:

To set mvr service type

Argument:

<port> : syntax: 1,5-7

<type>: 0(None), 1(Client), 2(Router).

Possible value:

<port> : from 1 to 10

<type>: 0(None), 1(Client), 2(Router).

Example:

IFEL2P-SW8C01(multicast)# set mvrserve-type 1 1

set rad-igmp-port

Syntax:

set mvrserve-type <port range> <mode>

Description:

To set radius IGMP enabled ports

Argument:

<port range> : syntax: 1,5-7

<mode>: 0(disable), 1(enable).

Possible value:

<port range> : from 1 to 10

<mode>: 0(disable), 1(enable).

Example:

IFEL2P-SW8C01(multicast)# set rad-igmp-port 1 1

set retry

Syntax:

set retry <value>

Description:

To set radius IGMP number of retry

Argument:

<value> : number of retry

Possible value:

<value> : from 0 to 10

Example:

IFEL2P-SW8C01(multicast)# set retry 1

set server

Syntax:

set server <ip> <port-number> <secret key> <ip2> <port-number>

Description:

To configure the settings related with 802.1X Radius Server.

Argument:

<ip><ip2> : the IP address of Radius Server, and the IP format is xxx.xxx.xxx.xxx
<port-number> : the service port of Radius Server(Authorization port),
range 1~65535
<secret-key> : set up the value of secret-key, and the length of secret-key is
from 1 to 31

Possible value:

<port-number> : 1~65535, default 1812

Example:

```
IFEL2P-SW8C01(multicast)# set server 192.168.1.115 1812 WinRadius  
192.168.1.116 1812
```

set specqry

Syntax:

```
set specqry <cnt> <response> <timeout>
```

Description:

To set specific query count

Argument:

<cnt>: from 1 to 10 value.

<response>: from 1 to 10 value.

<timeout>:from 1 to 30 value.

Possible value:

<cnt>: from 1 to 10 value.

<response>: from 1 to 10 value.

<timeout>:from 1 to 30 value.

Example:

```
IFEL2P-SW8C01(multicast)# set soecqry 2 2 10
```

set timeout

Syntax:

```
set timeout <value>
```

Description:

To set RADIUS IGMP timeout

Argument:

<value>:

Possible value:

<value>:2 to 60 seconds

Example:

```
IFEL2P-SW8C01(multicast)# set timeout 5
```

set unregfld-enable

Syntax:

```
set unregfld-enable <state>
```

Description:

To set unregister multicast flooding state

Argument:

<state>:0(disable), 1(enable)

Possible value:

<state>:0(disable), 1(enable)

Example:

```
IFEL2P-SW8C01(multicast)# set unregfld-enable 1
```

show group-filtering

Syntax:

show group-filtering <vid>

Description:

To show group filtering

Argument:

<vid>:VLAN ID

Possible value:

<vid>:1 to 4094

Example:

IFEL2P-SW8C01(multicast)# show group-filtering 20

show igmp-setting

Syntax:

show igmp-setting

Description:

To show IGMP setting

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(multicast)# show igmp-setting

IGMP Snooping : Enable
Unregister Multicast Flooding : Disable
General Query Interval : 125
General Query Max Response Time : 10
General Query Timeout : 11
Specific Query Count : 2
Specific Query Max Response Time : 1
Specific Query Timeout : 2

Port Multicast Group Limit IGMP Router

| | |
|----|-----|
| 1 | 256 |
| 2 | 256 |
| 3 | 256 |
| 4 | 256 |
| 5 | 256 |
| 6 | 256 |
| 7 | 256 |
| 8 | 256 |
| 9 | 256 |
| 10 | 256 |

show igmp-vlan

Syntax:

show igmp-vlan

Description:

To show IGMP VLAN

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(multicast)# show igmp-vlan

| Index | VID |
|-------|-----|
|-------|-----|

| | |
|---|----|
| 1 | 10 |
|---|----|

show multicast-status

Syntax:

show multicast-status

Description:

To show multicast status

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(multicast)# show multicast-status

No entry exist

show mvr-setting

Syntax:

show mvr-setting

Description:

To show MVR setting

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(multicast)# show mvr-setting

Multicast VLAN Registration : Enable

Multicast VLAN ID : 10

Port Service Type Tagging

| | |
|---|------|
| 1 | None |
| 2 | None |
| 3 | None |
| 4 | None |
| 5 | None |

| | | |
|----|--------|---|
| 6 | None | |
| 7 | None | |
| 8 | None | |
| 9 | None | |
| 10 | Router | v |

show rad-igmp

Syntax:

show rad-igmp

Description:

To show RADIUS IGMP Snooping configuration

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(multicast)# show rad-igmp

■ port

clear counter

Syntax:

clear counter

Description:

To clear all ports' counter (include simple and detail port counter) information.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(port)# clear counter

disable ge-fiber-power

Syntax:

disable ge-fiber-power <port>

Description:

To disable gigabit fiber port power

Argument:

<port>

Possible value:

<port> : 9 or 10

Example:

IFEL2P-SW8C01(port)# disable ge-fiber-power 10

disable power_saving

Syntax:

disable power_saving <range>

Description:

To disable port power saving

Argument:

<range> syntax 1,5-7

Possible value:

<range> : 1-10

Example:

IFEL2P-SW8C01(port)# disable power_saving 2

disable state

Syntax:

disable state <range>

Description:

To disable port state.

Argument:

<range>: syntax 1,5-7

Possible value:

<range>: 1-10

Example:

IFEL2P-SW8C01(port)# disable state 8

enable ge-fiber-power

Syntax:

enable ge-fiber-power <port>

Description:

To enable gigabit fiber port power.

Argument:

<port>

Possible value:

<port>: 9 or 10

Example:

IFEL2P-SW8C01(port)# enable ge-fiber-power 10

enable power_saving

Syntax:

enable state <range>

Description:

To enable port power saving.

Argument:

<range>: syntax 1,5-7

Possible value:

<range>: 1-10

Example:

IFEL2P-SW8C01(port)#

enable state

Syntax:

enable state <range>

Description:

To enable port state.

Argument:

<range>: syntax 1,5-7

Possible value:

<range>: 1-10

Example:

IFEL2P-SW8C01(port)# enable state 3-8

set description

Syntax:

set description <range> <description>

Description:

To enable port state.

Argument:

<range>: syntax 1,5-7

<description>: set its port description max. 47 characters

Possible value:

<range>: 1-10

Example:

IFEL2P-SW8C01(port)# set description 9 gigabitSFP

set flow-control

Syntax:

set flow-control <range> <symmetric | disable>

Description:

To set port flow control.

Argument:

<range>:port range, syntax 1,5-7, available from 1 to 10

<symmetric>: set its flow control as symmetric

<disable>: set its flow control as asymmetric

Possible value:

<range>: 1 to 10

<symmetric | disable>:symmetric or disable

Example:

IFEL2P-SW8C01(port)# set flow-control 3-6 symmetric

set speed-duplex

Syntax:

set speed-duplex <range> <auto> | [<10 |100 |1000> <half | full>]

Description:

To set up the speed and duplex of all ports.

Argument:

<range>:port range, syntax 1,5-7, available from 1 to 10

<port-speed>:

auto : set auto-negotiation mode

10 : set speed to 10M

100 : set speed to 100M

1000 : set speed to 1000M

<port-duplex> :

Half : set to half duplex

full : set to full duplex

Possible value:

<range>: 1 to 10

<port-speed> : auto, 10, 100, 1000

<port-duplex> : full, half

Example:

IFEL2P-SW8C01(port)# set speed-duplex 8 100 full

show conf

Syntax:

show conf

Description:

To display the each port's configuration about state, speed-duplex and flow control.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(port)# show conf

show description

Syntax:

show description

Description:

To display the port description

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(port)# show description

show detail-counter

Syntax:

show detail-counter <#>

Description:

To display the detailed counting number of each port's traffic.

Argument:

: port, available from 1 to 10

Possible value:

1-10

Example:

IFEL2P-SW8C01(port)# show detail-counter 6

show media

Syntax:

show media <port>

Description:

To display the module 9 or 10 information.

Argument:

<port>: available 9, 10

Possible value:

<port>: 9, 10

Example:

IFEL2P-SW8C01(port)# show media 9

Port 9 Fiber Media Information

Connector Type : SFP - LC
Fiber Type : Multi-mode (MM)
Tx Central Wavelength : 850
Baud Rate : 1G
Vendor OUI : 00:40:c7
Vendor Name : APAC Opto
Vendor PN : KM28-C3S-TC-N
Vendor Rev : 0000
Vendor SN : 5425010828

Date Code : 050530
 Temperature : none
 Vcc : none
 Mon1 (Bias) mA : none
 Mon2 (TX PWR) : none
 Mon3 (RX PWR) : none

show simple-counter

Syntax:

show simple-counter

Description:

To display the summary counting of each port's traffic.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(port)# show simple-counter

show status

Syntax:

show status

Description:

To display the port's current status.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(port)# show status

Port Media Link State Auto Nego. Speed/Duplex Rx Pause Tx Pause

| | | | | | | | |
|----|----|------|--------|--------|-----------|------|------|
| 1 | TP | Down | Enable | Enable | ----/---- | ---- | ---- |
| 2 | TP | Down | Enable | Enable | ----/---- | ---- | ---- |
| 3 | TP | Down | Enable | Enable | ----/---- | ---- | ---- |
| 4 | TP | Down | Enable | Enable | ----/---- | ---- | ---- |
| 5 | TP | Up | Enable | Enable | 100M/Full | ON | ON |
| 6 | TP | Down | Enable | Enable | ----/---- | ---- | ---- |
| 7 | TP | Down | Enable | Enable | ----/---- | ---- | ---- |
| | | | : | | | | |
| | | | : | | | | |
| | | | : | | | | |
| 9 | TP | Down | Enable | Enable | ----/---- | ---- | ---- |
| 10 | TP | Down | Enable | Enable | ----/---- | ---- | ---- |

■ qos

disable 1p

Syntax:

disable 1p

Description:

To disable 802.1p qos.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(qos)# disable 1p

disable dscp

Syntax:

disable dscp

Description:

To disable IP DSCP qos.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(qos)# disable dscp

disable qos

Syntax:

disable qos

Description:

To disable qos function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(qos)# disable qos

enable 1p

Syntax:

enable 1p

Description:

To enable 802.1p qos.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(qos)# enable 1p

enable dscp

Syntax:

enable dscp

Description:

To enable IP DSCP qos.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(qos)# enable dscp

enable qos

Syntax:

enable qos

Description:

To enable qos function.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(qos)# enable qos

set dscp

Syntax:

set dscp [<q0><priority>] [<q1><priority>] [<q2><priority>] [<q3><priority>]

Description:

To set IP DSCP qos weighting for 4 queues.

Argument:

<q>: queue level, q0: queue 0; q1: queue 1; q2: queue 2; q3: queue 3.

<priority>: priority level. One queue has been assigned 2 different priorities.

You don't need to use all of queue, but must assign queue in order.

Syntax: 1,2 or 2,5-7, available from 0 to 63.

Possible value:

<priority>: 0 to 63

Example:

IFEL2P-SW8C01(qos)# set dscp q0 2 q1 2 q2 2 q3 3

set pri-tag

Syntax:

set pri-tag [<q0><priority>] [<q1><priority>] [<q2><priority>] [<q3><priority>]

Description:

To set 802.1p qos weighting for 4 queues.

Argument:

<q>: queue level, q0: queue 0; q1: queue 1; q2: queue 2; q3: queue 3.

<priority>: priority level. One queue has been assigned 2 different priorities.

You don't need to use all of queues, but must assign queues in order.

Syntax: 1,2 or 2,5-7, available from 0 to 7.

Possible value:

<priority>: 0 to 7

Example:

```
IFEL2P-SW8C01(qos)# set pri-tag q0 0 q1 2 q3 4
```

set sche

Syntax:

set sche <method> <wrr_0> <wrr_1> <wrr_2> <wrr_3>

Description:

To set qos schedule and weight for 4 queues.

Argument:

<method>: priority scheduling method

<wrr_0 to 3>: weighted for every queue. Weighted range : 1-55.

Possible value:

<method>:

0: 4 WRR

1: 1 Strict + 3 WRR

2: 2 Strict + 2 WRR

3: 4 Strict

<wrr_0 to 3>: 1-55

Example:

```
IFEL2P-SW8C01(qos)# set sche 0 1 2 8 16
```

show dscp

Syntax:

show dscp

Description:

To Show qos DSCP priority mapping

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(qos)# show dscp
```

```
ip diffserv classification
```

```
=====
```

```
Global QoS mode: Enable QoS
```

```
Disable 802.1p Priority
```

```
Disable ip diffserv classification
```

Scheduling: 4 WRR method.
weight: wrr 0 = 1; wrr 1 = 2; wrr 2 = 4; wrr 3 = 8.
weighted range: 1~55.
P0~63: Priority 0~63.
Default mode: Queue0: P0~15; Queue1: P16~31; Queue2: P32~47; Queue3: P48~63.

| DiffServ | Queue | DiffServ | Queue | DiffServ | Queue | DiffServ | Queue |
|----------|-------|----------|-------|----------|-------|----------|-------|
| 0 | 0 | 1 | 0 | 2 | 0 | 3 | 0 |
| 4 | 0 | 5 | 0 | 6 | 0 | 7 | 0 |
| 8 | 0 | 9 | 0 | 10 | 0 | 11 | 0 |
| 12 | 0 | 13 | 0 | 14 | 0 | 15 | 0 |
| 16 | 1 | 17 | 1 | 18 | 1 | 19 | 1 |
| 20 | 1 | 21 | 1 | 22 | 1 | 23 | 1 |
| 24 | 1 | 25 | 1 | 26 | 1 | 27 | 1 |
| 28 | 1 | 29 | 1 | 30 | 1 | 31 | 1 |
| 32 | 2 | 33 | 2 | 34 | 2 | 35 | 2 |
| 36 | 2 | 37 | 2 | 38 | 2 | 39 | 2 |
| 40 | 2 | 41 | 2 | 42 | 2 | 43 | 2 |
| 44 | 2 | 45 | 2 | 46 | 2 | 47 | 2 |
| 48 | 3 | 49 | 3 | 50 | 3 | 51 | 3 |
| 52 | 3 | 53 | 3 | 54 | 3 | 55 | 3 |
| 56 | 3 | 57 | 3 | 58 | 3 | 59 | 3 |
| 60 | 3 | 61 | 3 | 62 | 3 | 63 | 3 |

show priority-tag

Syntax:

show priority-tag

Description:

To show qos 802.1p priority mapping

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(qos)# show priority-tag

802.1p priority

=====

Global QoS mode: Enable QoS

Enable 802.1p Priority

Disable ip diffserv classification

Scheduling: 4 WRR method.

weight: wrr 0 = 1; wrr 1 = 2; wrr 2 = 4; wrr 3 = 8.

weighted range: 1~55.

P0~7: Priority 0~7.

Default mode: Queue0: P0,P1; Queue1: P2,P3; Queue2: P4,P5; Queue3: P6,P7.

| | P0 | P1 | P2 | P3 | P4 | P5 | P6 | P7 |
|---------|----|----|----|----|----|----|----|----|
| ----- | | | | | | | | |
| Queue 0 | 0 | 0 | 1 | 1 | 2 | 2 | 3 | 3 |

■ r-ring

set ring state

Syntax:

Set state <role>

Description:

Set ring state.

Argument:

<role>

Possible value:

<role>: 0 for disable, 1 for master, 2 for member

Example:

IFEL2P-SW8C01(r-ring)# set state 1

Note:R-Ring function can't run with

1. LACP
2. STP/RSTP/MSTP
3. IEEE802.1X
4. Loop Detection
5. IGMP Snooping , IGMP Proxy

■ reboot

reboot

Syntax:

reboot

Description:

To reboot the system.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01# reboot

Read system parameters from IIC EEPROM...Done!

BIOS v1.12

BIOS(0)>

.....Now booting image...

Start: no need to update flash..

User: no need to update flash..

Managed Switch - IFEL2P-SW8C01

Login:

■ security

<<arp-protect>>

Syntax:

set <packet-burst> <rate-per-second>

Description:

To set arp protect

Argument:

<packet-burst>: 0 or 1-200 packets

<rate-per-second>: 0 or 64-25600 bytes

Possible value:

<packet-burst>: 0 or 1-200 packets

<rate-per-second>: 0 or 64-25600 bytes

Example:

IFEL2P-SW8C01(security)#arp-protect

IFEL2P-SW8C01(security-arp-protect)#set 20 64

IFEL2P-SW8C01(security-arp-protect)#show

Packet Burst: 20

Rate per Second: 64

<<isolated-group>>

set

Syntax:

set <port>

Description:

To set up the function of the isolated group.

Argument:

<port> : isolated port; range syntax: 1,5-7, available from 0 to 10
set 0 as disabled

Possible value:

<port>:0 to 10

Example:

IFEL2P-SW8C01(security)#isolated-group

IFEL2P-SW8C01(security-isolated-group)# set 2,3,4

show

Syntax:

show

Description:

To display the current setting status of isolated group.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(security-isolated-group)# show
Isolated group:
2 3 4

<<mirror>>

disable

Syntax:

disable

Description:

Disable mirror.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(security)#mirror

IFEL2P-SW8C01(security-mirror)# disable

enable

Syntax:

enable

Description:

Enable mirror.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(security)#mirror

IFEL2P-SW8C01(security-mirror)# enable

set

Syntax:

set <spy> <ingress> <egress>

Description:

To set mirror ingress/egress port

Argument:

<spy>:Monitoring port

<ingress>:monitored ingress port

<egress>: monitored egress port

Possible value:

<spy>:Monitoring port

<ingress>:range syntax: 1,5-7, available from 0 to 10

<egress>:range syntax: 1,5-7, available from 0 to 10

set ingress/egress to 0 as ingress/egress disabled

Example:

IFEL2P-SW8C01(security)#mirror

IFEL2P-SW8C01(security-mirror)#set 2 6 6

show**Syntax:**

show

Description:

To show current mirror port.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(security-mirror)# show

Mirror:

Monitoring Port :2

Monitored Ingress :6

Monitored Egress :6

■ snmp

del access

Syntax:

del access <group_name> <security_model> <security_level>

Description:

To delete SNMP access entry.

Argument:

<group_name>: max 32 characters

<security_model>: 1→v1, 2→v2c, 3→usm, 0→any

<security_level>: 1→NoAuthPriv, 2→AuthNoPriv, 3→AuthPriv

Possible value:

<group_name>: max 32 characters

<security_model>: 0-3

<security_level>: 1-3

Example:

IFEL2P-SW8C01(snmp)# del test1 2 2

del community

Syntax:

del community <community>

Description:

To delete SNMP community entry.

Argument:

<community>: max 32 characters

Possible value:

<community>: max 32 characters

Example:

IFEL2P-SW8C01(snmp)# del test1

del group

Syntax:

del group <security_model> <user_name>

Description:

To delete SNMP group entry.

Argument:

<security_model>: 1→v1, 2→v2c, 3→usm

<user_name>: max 32 characters

Possible value:

<security_model>: 1, 2, 3

<user_name>: max 32 characters

Example:

IFEL2P-SW8C01(snmp)# del 1 Tommy

del user

Syntax:

```
del user <name>
```

Description:

To delete SNMP user entry.

Argument:

<name>: max 32 characters

Possible value:

<name>: max 32 characters

Example:

IFEL2P-SW8C01(snmp)# del user Tommy

del view

Syntax:

```
del view <view name> <oid subtree>
```

Description:

To delete SNMP view entry.

Argument:

<view name>: max 32 characters

<oid subtree>: the OID defining the root of the subtree to add to the name view

Possible value:

<view name>: max 32 characters

<oid subtree>: the OID defining the root of the subtree to add to the name view

Example:

IFEL2P-SW8C01(snmp)# del view access KKKKK

set access

Syntax:

```
set access <group_name> <security_model> <security_level> <read_view_name>
        <write view name>
```

Description:

To set SNMP access entry.

Argument:

<group name>: max 32 characters

<security model>:1→v1, 2→v2c, 3→usm, 0→any

<security_level>: 1→NoAuthPriv, 2→AuthNoPriv, 3→AuthPriv
v1 and v2 security level = 1

`<read_view_name>`:The scope for a specified instance can read, none is reserved for empty.

`<write_view_name>`: The scope for a specified instance can write, none is reserved for empty.

Possible value:

<group name>: max 32 characters

<security model>:1→v1, 2→v2c, 3→usm, 0→any

<security_level>:1→NoAuthPriv, 2→AuthNoPriv, 3→AuthPriv
v1 and v2 security level = 1

<read_view_name>:The scope for a specified instance can read, none is reserved for empty.

<write_view_name>:The scope for a specified instance can write, none is reserved for empty.

set community

Syntax:

set community <Community> <user_name> <Source_IP> <Source Mask>

Description:

To set SNMP community entry.

Argument:

<Community>:syntax: aBc, max 32 characters

<user_name>:syntax: aBc, max 32 characters

<Source_IP>:SNMP access source ip

<Source Mask>:SNMP access source address mask

Possible value:

<Community>:max 32 characters

<user_name>:max 32 characters

<Source_IP>:xxx.xxx.xxx.xxx

<Source Mask>:xxx.xxx.xxx.xxx

set engine-id

Syntax:

set engine-id <id>

Description:

To set engine-id config.

Argument:

<id>:0-9,a-f,A-F, Min 5 Bytes, Max 32 Bytes, the fifth Byte can't input 00.

Possible value:

<id>:0-9,a-f,A-F

Example:

IFEL2P-SW8C01(snmp)# set engine-id 23se45ujop

set group

Syntax:

set group <user_name> <security_model> <group_name>

Description:

To set SNMP group entry.

Argument:

<user_name>: max 32 characters

<security_model>:1→v1, 2→v2c, 3→usm

<group_name>: max 32 characters

Possible value:

<user_name>: max 32 characters

<security_model>:1-3

<group_name>: max 32 characters

Example:

IFEL2P-SW8C01(snmp)# set group operator 2 good

set mode

Syntax:

set mode <enable | disable>

Description:

To set SNMP state.

Argument:

<enable>: SNMP is enabled

<disable >:SNMP is disabled

Possible value:

Enable or disable

Example:

```
IFEL2P-SW8C01(snmp)# set mode enable
```

```
IFEL2P-SW8C01(snmp)# show mode
```

SNMP mode is enabled

set trap

Syntax:

set trap <#> <state> <version> <ip> <port> <name> [<security> <auth> <authpass>
[<privpass>]]

Description:

To set trap IP, Port, Community---etc.

Argument:

<#>:trap number, 1-6

<state>:0:Disable, 1:Enable

<version>:1:SNMPv1,2:SNMPv2c,3:SNMPv3

<ip>:ip address or domain name

<port>:trap port(1-65535)

<name>:community/security name, max 32 characters

<security>:1:NoAuthNoPriv, 2:AuthNoPriv, 3:AuthPriv

<auth>:1:MD5, 2:SHA

<authpass>:authentication password, max 32 characters

<privpass>:privacy password, max 32 characters

Possible value:

<#>:1-6

<state>:0-1

<version>:1-3

<ip>:ip address or domain name

<port>:1-65535

<name>:community/security name, max 32 characters

<security>:1-3

<auth>:1-2

<authpass>:authentication password, max 32 characters

<privpass>:privacy password, max 32 characters

set user

Syntax:

set user <user_name> <security_level> [<auth><authpass><priv>[<privpass>]]

Description:

To set SNMP user entry.

Argument:

<user_name>:syntax:aBc, max 32 characters

<security_level>:1:NoAuthNoPriv, 2:AuthNoPriv, 3:AuthPriv

<auth>:1:MD5, 2:SHA

<authpass>:syntax:a9Bc,min 8 characters, max 32 characters

<priv>:1:DES

<privpass>:syntax aBc, min 8 characters, max 32 characters

Possible value:

<user_name>:syntax:aBc, max 32 characters

<security_level>:1:NoAuthNoPriv, 2:AuthNoPriv, 3:AuthPriv

<auth>:1:MD5, 2:SHA

<authpass>:syntax:a9Bc,min 8 characters, max 32 characters

<priv>:1:DES

<privpass>:syntax aBc, min 8 characters, max 32 characters

Example:

IFEL2P-SW8C01(snmp)# set user user 2

set view

Syntax:

set view <view_name> <view_type> <oid_subtree>

Description:

To set SNMP view entry.

Argument:

<view_name>:max 32 characters

<view_type>:1:included, 0:excluded

included:Indicate this view subtree should be included

excluded:Indicate this view subtree should be excluded

<oid_subtree>:The OID defining the root of subtree to add to the named view

Possible value:

<view_name>:max 32 characters

<view_type>:1:included, 0:excluded

included:Indicate this view subtree should be included

excluded:Indicate this view subtree should be excluded

<oid_subtree>:The OID defining the root of subtree to add to the named view

show access

Syntax:

show access

Description:

To show SNMP access entry.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(snmp)# show acces

No entry existed !

show community

Syntax:

show community

Description:

To show SNMP community entry.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(snmp)# show community

show engine-id

Syntax:

show engine-id

Description:

To show engine-id config.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(snmp)# show engine-id

Engine ID: 80001455030040C73300D1

Engine Boots: 5

show group

Syntax:

show group

Description:

To show SNMP group entry.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(snmp)# show group

show mode

Syntax:

show mode

Description:

To show SNMP state.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(snmp)# show mode
SNMP mode is enabled

show trap

Syntax:

show trap

Description:

To show trap IP, Port, Community---etc.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(snmp)# show trap

show user

Syntax:

show user

Description:

To show SNMPv3 user config.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(snmp)# show user

show view

Syntax:

show view

Description:

To show SNMP view entry.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(snmp)# show view

■ stp

MCheck

Syntax:

MCheck <range>

Description:

To force the port to transmit RST BPDUs.

Argument:

<range>: syntax 1,5-7, available from 1 to 10

Possible value:

<range>: 1 to 10

Example:

IFEL2P-SW8C01(stp)# Mcheck 1-8

disable

Syntax:

disable

Description:

To disable the function of STP.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(stp)# disable

enable

Syntax:

enable

Description:

To enable the function of STP.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(stp)# enable

set config

Syntax:

set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>

Description:

To set up the parameters of STP.

Argument:

<Bridge Priority>: priority must be a multiple of 4096, available from 0 to 61440.

<Hello Time>: available from 1 to 10.

<Max. Age>: available from 6 to 40.

<Forward Delay>: available from 4 to 30.

Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max. Age}$

$\text{Max. Age} \geq 2 * (\text{Hello Time} + 1)$

Possible value:

<Bridge Priority>: 0 to 61440.

<Hello Time>: 1 to 10.

<Max. Age>: 6 to 40.

<Forward Delay>: 4 to 30.

Example:

IFEL2P-SW8C01(stp)# set config 61440 2 20 15

set port

Syntax:

set port <range> <path cost> <priority> <edge_port> <admin p2p>

Description:

To set up the port information of STP.

Argument:

<range>: syntax 1,5-7, available from 1 to 10

<path cost>: 0, 1-200000000. The value zero means auto status

<priority>: priority must be a multiple of 16, available from 0 to 240

<edge_port>: Admin Edge Port, <0: Normal|1:Edge|2:Non STP>

<admin p2p>: Admin point to point, <auto|true|false>

Possible value:

<range> : 1 to 10 <path cost>: 0, 1-200000000.

<priority> : 0 to 240 <edge_port> : 0,1,2

<admin p2p>: auto / true / false

Example:

IFEL2P-SW8C01(stp)# set port 1-6 0 128 0 auto

set version

Syntax:

set version <stp|rstp>

Description:

To set up the version of STP.

Argument:

<stp|rstp>: stp / rstp

Possible value:

<stp|rstp>: stp / rstp

Example:

IFEL2P-SW8C01(stp)# set version rstp_

show config

Syntax:

show config

Description:

To display the STP configuration data.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(stp)# show config
STP State Configuration :
Spanning Tree Protocol : Enabled
Bridge Priority (0-61440): 61440
Hello Time (1-10 sec)   : 2
Max. Age (6-40 sec)     : 20
Forward Delay (4-30 sec): 15
Force Version           : RSTP
```

show port

Syntax:

show port

Description:

To display the port information of STP.

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(stp)# show port
Port Port  Status  Path Cost Priority Admin Edge Port Admin Point To Point
=====
  1 DISCARDING 200000 128          Normal      Auto
  2 DISCARDING 200000 128          Normal      Auto
  3 DISCARDING 200000 128          Normal      Auto
  4 DISCARDING 200000 128          Normal      Auto
  5 DISCARDING 200000 128          Normal      Auto
    :
    :
    :
  9 FORWARDING 20000 128          Normal      Auto
 10 FORWARDING 20000 128          Normal      Auto
```

show status

Syntax:

show status

Description:

To display the status of STP.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(stp)# show status

STP Status :

| | |
|--------------------------------------|---------------------|
| STP State | : Enabled |
| Bridge ID | : 00:40:C7:3F:00:D2 |
| Bridge Priority | : 32768 |
| Designated Root | : 00:40:C7:3F:00:D2 |
| Designated Priority | : 32768 |
| Root Port | : 0 |
| Root Path Cost | : 0 |
| Current Max. Age(sec) | : 20 |
| Current Forward Delay(sec) | : 15 |
| Hello Time(sec) | : 2 |
| STP Topology Change Count | : 0 |
| Time Since Last Topology Change(sec) | : 1269 |

■ syslog

disable

Syntax:

Diabie

Description:

To disable syslog function.

Argument:

<None>

Possible value:

<None>

Example:

IFEL2P-SW8C01(syslog)# diable

IFEL2P-SW8C01(syslog)#

enable

Syntax:

enable

Description:

To enable syslog function.

Argument:

<None>

Possible value:

<None>

Example:

IFEL2P-SW8C01(syslog)# enable

IFEL2P-SW8C01(syslog)#

set server

Syntax:

set server <ip> <port>

Description:

To set syslog Host IP and Port.

Argument:

<ip > : syslog server ip

<port> : trap port

Possible value:

<ip > : syslog server ip

<port> : trap port

Example:

IFEL2P-SW8C01 (syslog)# set server 192.168.22.0 8

IFEL2P-SW8C01 (syslog)#

IFEL2P-SW8C01 (syslog)# show

syslog : Enable

Syslog Host IP: 192.168.22.0 Port: 8

show

Syntax:

show

Description:

To show syslog server IP.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01 (syslog)# show

syslog : Enable

Syslog Host IP: 192.168.22.0 Port: 8

■ system

set contact

Syntax:

set contact <contact>

Description:

To set the contact description of the switch.

Argument:

<contact>: string length up to 40 characters.

Possible value:

<contact>: A, b, c, d, ... ,z and 1, 2, 3, etc.

Example:

IFEL2P-SW8C01(system)# set contact Taipei

set device-name

Syntax:

set device-name <device-name>

Description:

To set the device name description of the switch.

Argument:

<device-name>: string length up to 40 characters.

Possible value:

<device-name>: A, b, c, d, ... ,z and 1, 2, 3, etc.

Example:

IFEL2P-SW8C01(system)# set device-name CR-2600

set location

Syntax:

set location <location>

Description:

To set the location description of the switch.

Argument:

<location>: string length up to 40 characters

Possible value:

<location>: A, b, c, d, ... ,z and 1, 2, 3, etc.

Example:

IFEL2P-SW8C01(system)# set location Taipei

show

Syntax:

show

Description:

To display the basic information of the switch.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(system)# show

| | |
|-----------------------------|--|
| Model Name | : IFEL2P-SW8C01 |
| System Description | : Industrial 8-Port L2 Managed Fast Ethernet Switch
+ 2 TP/SFP Gigabit Dual Media |
| Location | : |
| Contact | : |
| Device Name | : IFEL2P-SW8C01 |
| System Up Time | : 0 Days 1 Hours 38 Mins 24 Secs |
| Current Time | : Fri Jan 01 04:26:30 2010 |
| BIOS Version | : v1.22 |
| Firmware Version | : v5.32 |
| Hardware-Mechanical Version | : v1.01-v1.01 |
| Serial Number | : 032C01000009 |
| Host IP Address | : 192.168.1.1 |
| Host MAC Address | : 00-40-c7-3f-00-d2 |
| Device Port | : UART * 1 TP *8 Fiber * 2 |
| RAM Size | : 32 M |
| Flash Size | : 4 M |
| CPU Load | : 15% |

■ tac-plus

disable accounting

Syntax:

disable accounting

Description:

To disable TACACS+ accounting.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(tac-plus)# disable accounting
Server disconnect !

disable authorization

Syntax:

disable authorization

Description:

To disable TACACS+ authorization

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(tac-plus)# disable authorization

disable fallback-author

Syntax:

disable fallback-author

Description:

To disable fallback to local authorization.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(tac-plus)# disable fallback-author

enable accounting

Syntax:

enable accounting

Description:

To enable TACACS+ accounting.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(tac-plus)# enable accounting
Server disconnect !

enable authorization**Syntax:**

enable authorization

Description:

To enable TACACS+ authorization

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(tac-plus)# enable authorization

enable fallback-author**Syntax:**

enable fallback-author

Description:

To enable fallback to local authorization.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(tac-plus)# enable fallback-author

set console-authentication**Syntax:**

set console-authentication <method 1> <method 2>

Description:

To set console authentication method.

Argument:

method: 0:Local

1:TACACS Authentication

2:None(for method 2 only)

Possible value:

method: 0-2

Example:

IFEL2P-SW8C01(tac-plus)# set console-authentication 0 2

set host**Syntax:**

set host <#> <ip>

Description:

To set TACACS+ Host IP

Argument:

<#>: host number, 1-2

Publication date: May., 2011

Revision B1

<ip>:xxx.xxx.xxx.xxx, 0.0.0.0 is disable

Possible value:

<#>: host number, 1-2

<ip>:xxx.xxx.xxx.xxx, 0.0.0.0 is disable

Example:

IFEL2P-SW8C01(tac-plus)# set host 1 192.168.1.2

set key

Syntax:

set key <secret_key>

Description:

To set TACACS+ key

Argument:

<secret_key>:1-31 characters

Possible value:

<secret_key>:1-31 characters

Example:

IFEL2P-SW8C01(tac-plus)# set key topsecret

set retry

Syntax:

set retry <retry>

Description:

To set retry times

Argument:

<retry>:1-3

Possible value:

<retry>:1-3

Example:

IFEL2P-SW8C01(tac-plus)# set retry 3

set telnet-authentication

Syntax:

set telnet-authentication <method 1> <method 2>

Description:

To set telnet-authentication method

Argument:

method: 0:Local

1:TACACS Authentication

2:None(for method 2 only)

Possible value:

method: 0:Local

1:TACACS Authentication

2:None(for method 2 only)

Example:

IFEL2P-SW8C01(tac-plus)# set telnet-authentication 0 2

set web-authentication

Syntax:

set web-authentication <method 1> <method 2>

Description:

To set web-authentication method

Argument:

method: 0:Local

1:TACACS Authentication

2:None(for method 2 only)

Possible value:

method: 0:Local

1:TACACS Authentication

2:None(for method 2 only)

Example:

IFEL2P-SW8C01(tac-plus)# set web-authentication 0 2

show authentication

Syntax:

show authentication

Description:

To show authentication config

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(tac-plus)# show authentication

Authentication retry : 3

| Authentication | Login
Primary | Login
Secondary |
|----------------|------------------|--------------------|
| Console | Local | None |
| Telnet | Local | None |
| Web | Local | None |

show tac-plus

Syntax:

show tac-plus

Description:

To show TACACS+ config

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(tac-plus)# show tac-plus

Authorization : Disable

Fallback to Local Authorization : Disable

Accounting : Disable

Secret Key: TACACS

| # | Server | IP |
|-------|---------|----|
| ----- | | |
| 1 | 0.0.0.0 | |
| 2 | 0.0.0.0 | |

■ tftp

set server

Syntax:

set server <ip>

Description:

To set up the IP address of tftp server.

Argument:

<ip>: the IP address of tftp server

Possible value:

<ip>: tftp server IP

Example:

IFEL2P-SW8C01(tftp)# set server 192.168.3.111

show

Syntax:

show

Description:

To display the information of tftp server.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(tftp)# show

Tftp Server : 192.168.3.111

■ time

set daylightsaving

Syntax:

set daylightsaving <hr> <MM/DD/HH> <mm/dd/hh>

Description:

To set up the daylight saving.

Argument:

<hr> : daylight saving hour, range: -5 to +5

<MM> : daylight saving start Month (01-12)

<DD> : daylight saving start Day (01-31)

<HH> : daylight saving start Hour (00-23)

<mm> : daylight saving end Month (01-12)

<dd> : daylight saving end Day (01-31)

<hh> : daylight saving end Hour (00-23)

Possible value:

<hr> : -5 to +5

<MM> : (01-12)

<DD> : (01-31)

<HH> : (00-23)

<mm> : (01-12)

<dd> : (01-31)

<hh> : (00-23)

Example:

IFEL2P-SW8C01(time)# set daylightsaving 3 11/11/01 11/12/01

set manual

Syntax:

set manual <YYYY/MM/DD> <hh:mm:ss>

Description:

To set up the current time manually.

Argument:

<YYYY> : Year (2000-2036)

<MM> : Month (01-12)

<DD> : Day (01-31)

<hh> : Hour (00-23)

<mm> : Minute (00-59)

<ss> : Second (00-59)

Possible value:

<YYYY> : (2000-2036)

<MM> : (01-12)

<DD> : (01-31)

<hh> : (00-23)

<mm> : (00-59)

<ss> : (00-59)

Example:

IFEL2P-SW8C01(time)# set manual 2009/11/30 16:18:50

set ntp

Syntax:

set ntp <ip> <timezone>

Description:

To set up the current time via NTP server.

Argument:

<ip>: ntp server ip address or domain name

<timezone>: time zone (GMT), range: -12 to +13

Possible value:

<timezone>: -12,-11...,0,1...,13

Example:

```
IFEL2P-SW8C01(time)# set ntp clock.via.net 8
```

```
Synchronizing...(1)
```

```
Synchronization success
```

show

Syntax:

show

Description:

To show the time configuration, including "Current Time", "NTP Server", "Timezone",

" Daylight Saving", " Daylight Saving Start" and "Daylight Saving End"

Argument:

None.

Possible value:

None.

Example:

```
IFEL2P-SW8C01(time)# show
```

```
Current Time      : Mon Nov. 30 16:16:22 2009
```

```
NTP Server       : 209.81.9.7
```

```
Timezone        : 8
```

```
Day light Saving : 4 Hours
```

```
Day light Saving Start : Mth: 2 Day: 20 Hour: 10
```

```
Day light Saving End  : Mth: 3 Day: 20 Hour: 10
```

```
IFEL2P-SW8C01(time)#
```

■ trunk

del trunk

Syntax:

del trunk <port-range>

Description:

To remove the trunk port.

Argument:

<port-range> : syntax 1,5-7, available from 1 to 10

Possible value:

<port-range> : 1 to 10

Example:

IFEL2P-SW8C01(trunk)# del trunk 1

set hash

Syntax:

set hash <method>

Description:

To set up trunk hash method.

Argument:

<method>: lacp hash method

<method>:hash method

0: DA and SA

1: SA

2: DA

3: IPv4 DIP

4: IPv4 SIP

5: DA, SA, IPv4 DIP and IPv4 SIP

note : This hash method applies to both LACP and static trunk.

Possible value:

<method>: from 0 to 5

Example:

IFEL2P-SW8C01(trunk)# set hash 2

set priority

Syntax:

set priority <range>

Description:

To set up the LACP system priority.

Argument:

<range>:available from 1 to 65535.

Possible value:

<range>:1 to 65535.

Example:

IFEL2P-SW8C01(trunk)# set priority 33333

set trunk

Syntax:

set trunk <port-range> <method> <group> <active LACP>

Description:

To set up the status of trunk, including the group number and mode of the trunk as well as LACP mode.

Argument:

<port-range> : syntax 1,5-7, available from 1 to 10

<method>: <static|lacp>

static : adopt the static link aggregation

lacp : adopt the dynamic link aggregation- link aggregation control protocol

<group>: 1-4

<active LACP>: <passive|active>

active : set the LACP to active mode

passive : set the LACP to passive mode

Possible value:

<port-range> : 1 to 10

<method>: static or lacp

<group>: 1-4

<active LACP>: active or passive

Example:

IFEL2P-SW8C01(trunk)# set trunk 2-5 lacp 1 active

show aggtr-view

Syntax:

show aggtr-view

Description:

To display the aggregator list.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(trunk)# show aggtr-view

Aggregator 1) Method: None
Member Ports: 1
Ready Ports:1

Aggregator 2) Method: LACP
Member Ports: 2
Ready Ports:
:
:
:
:

show lacp-config

Syntax:

show lacp-config

Description:

To show LACP configuration.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(trunk)# show lacp-config

LACP System Priority : 33333

Hash Method : DA

show lacp-detail

Syntax:

show lacp-detail <aggr>

Description:

To display the detailed information of the LACP trunk group.

Argument:

<aggr> : aggregator, available from 1 to 10

Possible value:

<aggr> : 1 to 10

Example:

IFEL2P-SW8C01(trunk)# show lacp-detail 2

show status

Syntax:

show status

Description:

To display the aggregator status and the settings of each port.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(trunk)# show status

Trunk Port Setting Trunk Port Status

| ----- | | | | | |
|-------|--------|-------|-------------|------------|--------|
| port | Method | Group | Active LACP | Aggregator | Status |
| ===== | | | | | |
| 1 | None | 0 | Active | 1 | Ready |
| 2 | LACP | 1 | Active | 2 | --- |
| 3 | LACP | 1 | Active | 3 | --- |
| 4 | LACP | 1 | Active | 4 | --- |
| 5 | LACP | 1 | Active | 5 | --- |
| 6 | None | 0 | Active | 6 | --- |
| 7 | None | 0 | Active | 7 | --- |
| 8 | None | 0 | Active | 8 | --- |
| 9 | None | 0 | Active | 9 | --- |
| 10 | None | 0 | Active | 10 | --- |

■ vlan

del port-group

Syntax:

del port-group <name>

Description:

To delete the port-based vlan group.

Argument:

<name>: port-vlan name

Possible value:

<name>: port-vlan name

Example:

IFEL2P-SW8C01(vlan)# del port-group vlan-2

del tag-group

Syntax:

del tag-group <vid>

Description:

To delete the tag-based vlan group.

Argument:

<vid>: vlan ID, available from 1 to 4094

Possible value:

<vid>: 1 to 4094

Example:

IFEL2P-SW8C01(vlan)# del tag-group 2

disable double-tag

Syntax:

disable double-tag

Description:

To disable double-tag.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vlan)# disable double-tag

disable drop-untag

Syntax:

disable drop-untag <port_range>

Description:

To disable drop-untag.

Argument:

<port_range>: which port(s) you want not to drop untagged frames. Syntax: 1,5-7, available from 1 to 10

Possible value:

<port_range>: 1 to 10

Example:

IFEL2P-SW8C01(vlan)# disable drop-untag 2,4,5-7

disable svl

Syntax:

disable svl

Description:

To enable Independent VLAN Learning.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vlan)# disable svl

disable symmetric

Syntax:

disable symmetric

Description:

Don't Drop frame from nonmember port

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vlan)# disable symmetric

enable double-tag

Syntax:

enable double-tag <SP-Tag_delimiter> <SP-Port_range>

Description:

To enable double-tag.

Argument:

<SP-Tag_delimiter>:Delimiter of SP Tagged frame.

<SP-Port_range>:syntax: 1,5-7

Possible value:

<SP-Tag_delimiter>:Delimiter of SP Tagged frame. 1: 0x88A8, 2:0x8100

<SP-Port_range>:syntax: 1,5-7, available from 1 to 10

Example:

IFEL2P-SW8C01(vlan)# enable double-tag 1 2

enable drop-untag

Syntax:

enable drop-untag <port_range>

Description:

To enable drop-untag.

Argument:

<port_range>: which port(s) you want to drop untagged frames.

Possible value:

<port_range>: Syntax: 1,5-7, available from 1 to 10

Example:

IFEL2P-SW8C01(vlan)# enable drop-untag 2,4,5-7

enable svl

Syntax:

enable svl

Description:

To enable Shared VLAN Learning.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vlan)# enable svl

enable symmetric

Syntax:

enable symmetric

Description:

To drop frames from the non-member port.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vlan)# enable symmetric

set mgt-vlan

Syntax:

set mgt-vlan <state> [vid]

Description:

To set management VLAN.

Argument:

<state>:

[vid]:VLAN ID

Possible value:

<state>:0 for disable, 1 for enable

[vid]:from 1 to 4094

Example:

IFEL2P-SW8C01(vlan)# set mgt-vlan 1 2

set mode

Syntax:

set mode <port|tag|metro|>

Description:

To switch vlan mode between port-based and tag-based modes.

Argument:

<port|tag|metro|> : port or tag or metro
tag: set tag-based vlan
port: set port-based vlan
metro: set metro mode vlan
#: up-link port type

Possible value:

<port|tag|metro|> : port or tag or metro
tag: set tag-based vlan
port: set port-based vlan
metro: set metro mode vlan
#: up-link port type
0: 9 port
1:10 port
2: 9 and 10 port

Example:

IFEL2P-SW8C01(vlan)# set mode tag

set port-group

Syntax:

set port-group <name> <range>

Description:

To add or edit a port-based vlan group.

Argument:

<name>: port-vlan name
<range>: vlan group members, syntax: 1,5-7, available from 1 to 10

Possible value:

<range>: 1 to 10

Example:

IFEL2P-SW8C01(vlan)# set port-group vlan-1 2-5,6-10

set pvid

Syntax:

set pvid <port_range> <pvid> <default_priority>

Description:

To set vlan PVID and port priority.

Argument:

<port_range>: which port(s) you want to set PVID(s). Syntax 1,5-7, available from 1 to 10

<pvid>: which PVID you want to set, available from 1 to 4094

<default_priority>: which priority you want to set, available from 0 to 7

Possible value:

<port_range>: 1 to 10

<pvid>: 1 to 4094

<default_priority>: 0 to 7

Example:

IFEL2P-SW8C01(vlan)# set pvid 3,5,6-8 5 6

set tag-group

Syntax:

set tag-group <vid> <name> <member_range> <untag_range> <#1> <#2>

Description:

To add or edit the tag-based vlan group.

Argument:

<vid>: vlan id, from 1 to 4094

<name>: tag-vlan group name

<member_range>: member port; syntax: 1,5-7, available from 1 to 10

<untag_range>: untagged out port; syntax: 1,5-7, available from 0 to 10
set untag_range to 0 as none of the ports are force untagged

<#1>:gvrp propagation setting. 0 for disable, 1 for enable

<#2>:vlan action setting. 0 : Not in service, 1: active

Possible value:

<vid>: 1 to 4094

<member_range>: 1 to 10

<untag_range>: 0 to 10

<#1>:0 or 1

<#2>:0 or 1

Example:

IFEL2P-SW8C01(vlan)# set tag-group 2 vlan-2 2-8 0 0 0

show config

Syntax:

show config

Description:

To display the current vlan mode, Symmetric vlan, SVL and Double tag states.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vlan)# show config

Current vlan mode : Tag-based vlan

Global setting:

Symmetric vlan : Disable (Asymmetric)

SVL : Disable (IVL)

Double tag : Disable

SP port : 9 10

show group

Syntax:

show group

Description:

To display vlan mode and vlan group.

Argument:

None

Possible value:

None

Example:

IFEL2P-SW8C01(vlan)# show group

Vlan mode is tag-based.

1) Name :default

VID :1

GVRP Propagation: Enable

Member:1 2 3 4 5 6 7 8 9 10

Untag : 1 2 3 4 5 6 7 8 9 10

Action : active

show pvid

Syntax:

show pvid

Description:

To display pvid, priority and drop untag result.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vlan)# show pvid

| Port | PVID | Priority | Drop | Untag |
|-------|------|----------|------|---------|
| ----- | | | | |
| 1 | 1 | 0 | | Disable |
| 2 | 1 | 0 | | Disable |
| 3 | 1 | 0 | | Disable |
| 4 | 1 | 0 | | Disable |
| 5 | 1 | 0 | | Disable |
| 6 | 1 | 0 | | Disable |
| 7 | 1 | 0 | | Disable |
| 8 | 1 | 0 | | Disable |
| 9 | 1 | 0 | | Disable |
| 10 | 1 | 0 | | Disable |

■ vs

disable

Syntax:

disable

Description:

To disable the virtual stack.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vs)# disable

enable

Syntax:

enable

Description:

To enable the virtual stack.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vs)# enable

set gid

Syntax:

set gid <gid>

Description:

To set the group id.

Argument:

<gid>: group ID

Possible value:

<gid>: a-z,A-Z,0-9

Example:

IFEL2P-SW8C01(vs)# set gid group1

set role

Syntax:

set role <master|slave>

Description:

To set role.

Argument:

<master|slave>: master: act as master, slave : act as slave

Possible value:

<master|slave>: master or slave

Example:

IFEL2P-SW8C01(vs)# set role master

show

Syntax:

show

Description:

To display the configuration of the virtual stack.

Argument:

None.

Possible value:

None.

Example:

IFEL2P-SW8C01(vs)# show

Virtual Stack Config:

State : Enable

Role : Master

Group ID : group1

5. Maintenance

5-1. Resolving No Link Condition

The possible causes for a no link LED status are as follows:

- The attached device is not powered on
- The cable may not be the correct type or is faulty
- The installed building premise cable is faulty
- The port may be faulty

5-2. Q&A

1. Computer A can connect to Computer B, but cannot connect to Computer C through the Managed Switch.
 - ✓ The network device of Computer C may fail to work. Please check the link/act status of Computer C on the LED indicator. Try another network device on this connection.
 - ✓ The network configuration of Computer C may be something wrong. Please verify the network configuration on Computer C.
2. The uplink connection function fails to work.
 - ✓ The connection ports on another must be connection ports. Please check if connection ports are used on that Managed Switch.
 - ✓ Please check the uplink setup of the Managed Switch to verify the uplink function is enabled.
3. The console interface cannot appear on the console port connection.
 - ✓ The COM port default parameters are [Baud Rate: 57600, Data Bits: 8, Parity Bits: None, Stop Bit: 1, Flow Control: None]. Please check the COM port property in the terminal program. And if the parameters are changed, please set the COM configuration to the new setting.
 - ✓ Check the RS-232 cable is connected well on the console port of the Managed Switch and COM port of the PC.
 - ✓ Check if the COM port of the PC is enabled.
4. How to configure the Managed Switch?
 - ✓ The "Hyperterm" is the terminal program in Win95/98/NT/XP. Users can also use any other terminal programs in Linux/Unix to configure the Managed Switch. Please refer to the user guide of that terminal program. But the COM port parameters (baud rate/ data bits/ parity bits/ flow control) must be the same as the setting of the console port of the Managed Switch.

Appendix A

Technical Specifications

Hardware Specifications

| Feature | Detailed Description |
|---------------------|--|
| Power Requirement | 24VDC(12~48 V) |
| Consumption | 12W |
| Ambient Temperature | -40° to 75°C |
| Humidity | 5% to 95% |
| Dimensions | 66(W)x152(H)x102(D) |
| Installation | DIN-Rail, Wall Mount |
| Alarm contact | Current carrying capacity 1A @ 24V |
| Certification | Comply with FCC Part 15 Class A & CE Mark Approval |
| Shock | IEC60068-2-27 |
| Freefall | IEC60068-2-32 |
| Vibration | IEC60068-2-6 |

Network Interface

| Category | Connector | Transmission | Max. Cable Length | Wavelength |
|-------------|-----------|------------------|-------------------|------------|
| 10-T/100-TX | RJ-45 | Full/Half Duplex | 100M | / |
| 1000Base-T | RJ-45 | Full Duplex | 100M | / |
| 100Base-X | SFP | Full Duplex | | |
| 1000Base-X | SFP | Full Duplex | | |

Dimension Diagram

Management Software Specifications

| | |
|---------------------------------|---|
| System Configuration | Auto-negotiation support on 10/100Base-TX ports, Web browser or console interface can set transmission speed (10/100Mbps) and operation mode (Full/Half duplex) on each port, enable/disable any port, set VLAN group, set Trunk Connection. |
| Management Agent | SNMP support; MIB II, Bridge MIB, RMON MIB |
| Spanning Tree Algorithm | IEEE 802.1D |
| VLAN Function | Port-Base / 802.1Q-Tagged, allowed up to 256 active VLANs in one switch. |
| Trunk Function | Ports trunk connections allowed |
| IGMP | IP Multicast Filtering by passively snooping on the IGMP Query. |
| Bandwidth Control | Supports by-port Egress/Ingress rate control |
| Quality of Service (QoS) | Referred as Class of Service (CoS) by the IEEE 802.1P standard
Four queues per port
Packet transmission schedule using Weighted Round Robin (WRR)
User-defined weight
Classification of packet priority can be based on either a VLAN tag on packet or a user-defined port priority. |
| Port Security | Limit number of MAC addresses learned per port static MAC addresses stay in the filtering table. |
| Internetworking Protocol | Bridging : 802.1D Spanning Tree
IP Multicast : IGMP Snooping
IP Multicast Packet Filtering
Maximum of 256 active VLANs and IP multicast sessions |
| Network Management | One RS-232 serial port as local control console
Telnet remote control console
SNMP agent : MIB-2 (RFC 1213)
Bridge MIB (RFC 1493)
RMON MIB (RFC 1757)-statistics
Ethernet-like MIB (RFC 1643)
Web browser support based on HTTP Server and CGI parser TFTP software-upgrade capability. |

Note: Any specification is subject to change without notice.

Appendix B

Default Account

| Account | Password (Default) | Password Change | Create , Modify & Delete Account | Set | Read |
|----------|--------------------|------------------------|----------------------------------|-----|------|
| admin | admin | Yes | Yes | Yes | Yes |
| operator | operator | Yes
(Only operator) | No | Yes | Yes |
| guest | guest | Yes
(Only guest) | No | No | Yes |

| Classify | Number of user |
|-------------------------|----------------|
| Telnet | 3 |
| Web UI + Telnet | 5 |
| Web UI + Telnet + RS232 | 6 |

Appendix C

Console Cable Specifications

The DB-9 cable is used for connecting a terminal or terminal emulator to the Managed Switch's RJ-45 console port to access the command-line interface.

The table below shows the pin assignments for the DB-9 cable.

| Function | Mnemonic | Pin |
|---------------|----------|-----|
| Receive Data | RxD | 2 |
| Transmit Data | TxD | 3 |
| Signal Ground | GND | 5 |

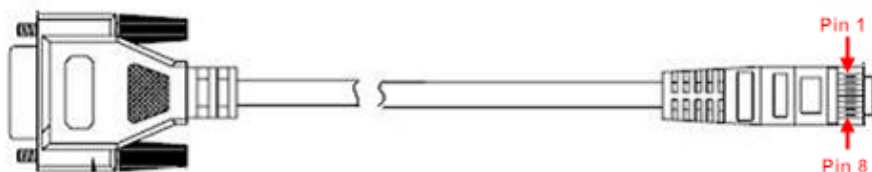


Fig. Console Cable

3 Pin Console Cable

| DB-9 | | | RJ-45 |
|------|---|-------|-------|
| RxD | 2 | ----- | 3 TxD |
| TxD | 3 | ----- | 6 RxD |
| GND | 5 | ----- | 5 GND |

